(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 December 2021 (30.12.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/260743 A1

(51) International Patent Classification:
G06Q 20/06 (2012.01) *G06Q 20/36* (2012.01)

(21) International Application Number:
PCT/IS2021/050009

(22) International Filing Date:
25 June 2021 (25.06.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
IS 050308 25 June 2020 (25.06.2020) IS

(71) Applicant: **MONERIUM EHF.** [IS/IS]; Laekjargotu 2, IS-101 Reykjavik (IS).

(72) Inventors: **GUDJONSSON, Arni**; Skolabraut 4, IS-170 Seltjarnarnes (IS). **KRISTJANSSON, Gisli**; Manatuni 13, IS-105 Reykjavik (IS).

(74) Agent: **ARNASON FAKTOR**; Gudridarstig 2-4, IS-113 Reykjavik (IS).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*
— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

WO 2021/260743 A1

(54) Title: SYSTEM AND METHOD FOR AUTOMATED SECURE AND VERIFIED DATA TRANSFER

(57) Abstract: The present invention relates to a system and a method for automated and secure data transfer such as for transactions including but not limited to payment transactions. The invention provides a system that comprises at least one node which is configured to provide node data. The system further comprises a data-processing component, which is configured to automatically generate a node profile based on at least the node data. Furthermore, a transferring module is configured to initiate a transaction process based on the node profile. The transferring module can provide access to and/or controlling of an entity, such as a physical entity. The node profile may comprise a unique identifier (UID), which can/may comprise a blockchain address.

System and method for automated secure and verified data transfer

Field

The invention relates to a system and a method for facilitating automated secure and verified data transfer, specifically through the use of distributed and/or decentralized networks.

Background

Nowadays, secure data transfer becomes more and more important, particularly in case the data being transferred needs high security, such as data enabling access to and/or controlling of a machine, a gate, asset transfer etc.

Payment systems in particular are any systems used to settle financial transactions through the transfer of monetary value. This includes the entities, instruments, people, rules, procedures, standards, and technologies that make its exchange possible. Nowadays, the so-called "idea of private money" which is embodied through a phenomenon of electronic currency (for example, e-money) exchange becomes increasingly popular. Electronic currency (e-money) began a new era in economics. Electronic money (e-money) is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer. The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions. E-money products can be hardware-based or software-based, depending on the technology used to store the monetary value. There have been extensive developments in the field of circulating e-money.

For example, US20170372278A1 discloses a payment system based on use of a blockchain-based electronic currency substantiated by a reserve of assets, as well are methods for issuance and circulation of the aforementioned electronic currency and methods for maintaining a reserve of assets that substantiate the aforementioned electronic currency in the disclosed payment system. In one exemplary aspect, the system comprises a management module, executable by a computer processor, configured to create and manage one or more wallets of electronic currency for a system operator and a plurality of clients, execute electronic currency payment transactions by transferring electronic currency between one or more wallets of the system operator and/or a plurality of clients and recording information about the executed transactions in a private blockchain-based settlement network, manage information about the reserve of assets substantiating the electronic currency and control in real-time purchase or sale of assets on an external market in an amount required to fully substantiate the issued electronic

currency at each moment of time; and an issuance centre, executable by a computer processor, configured to receive in real-time information from the management module concerning an amount of the reserve of assets substantiating the electronic currency, perform centralized generation and controlled issuance of the electronic currency into circulation, wherein the generation of all the electronic currency is performed in a single block by creating this block in a blockchain using a mining operation that generates a maximum possible amount of the electronic currency, and wherein the generated electronic currency is issued into circulation in an amount equal to or less than the amount of the reserve of assets substantiating it, when the amount of the reserve of assets reaches a threshold amount, calculate, by the computer processor, in real-time, an amount of assets to be sold or purchased on the external market in order to fully substantiate the issued electronic currency based on a set of mathematical functions that account for distributions of moments of time of receiving from the clients orders for purchasing or selling of electronic currency using a fiat currency and size of the received orders, and transmit to the management module an order to purchase or sell the calculated amount of assets, on the external market, to maintain a sufficient amount of reserve to fully substantiate the electronic currency at each moment of time.

US20200027089A1 relates to a method includes acquiring, at a node server, blockchain data for a blockchain address on a blockchain network. The blockchain data includes a plurality of transactions for the blockchain address. The method includes generating a local node trust score for the blockchain address based on the blockchain data. The local node trust score indicates a likelihood that the blockchain address is involved in fraudulent activity. The method includes receiving, from a plurality of remote servers, a plurality of additional local trust scores for the blockchain address. The method includes determining a consensus trust score based on the local node trust score and the plurality of additional local trust scores. Additionally, the method includes monitoring a ledger on the blockchain network for a contract trust request that specifies the blockchain address and sending, to the blockchain network, the consensus trust score for the blockchain address specified in the contract trust request.

US20190303920A1 discloses a transaction system and process using a token smart contract is disclosed. The system may receive a transfer notification comprising a user public blockchain address, a merchant public blockchain address, and a transaction amount. The system may retrieve a transaction account identifier and a merchant identifier based on the user public blockchain address and the merchant public blockchain address. The system may adjust a transaction account balance associated with the user identifier based on the transaction amount. The system may credit a merchant account based on the transaction amount.

As established, sending money via the Internet is not new - but it is still cumbersome, slow and expensive. Systems and methods facilitating secure and verified transmission automatically between systems such as established conventional banking systems and blockchain networks and independent nodes would be very useful.

Summary

In light of the above, it is an object of the present invention to overcome or at least alleviate the shortcomings of the prior art. More particularly, it is an object of the present invention to provide a system and a method for facilitating automated and secure data transactions such as but not limited to payment transactions, as well as transaction and transmission of other intangible goods and digital objects such as but not limited to tickets (e.g. airline tickets, event tickets etc), shares, titles, certificates, etc.

In a first embodiment a system is provided. The system comprises at least one node. The node may be configured to provide node data. The system further comprises a data-processing component. The data processing component is configured to automatically generate a node profile based on at least the node data. Furthermore, the system comprises at least one transferring module. The transferring module is configured to initiate a transaction process based on the node profile. In the context herein the transferring module may also be referred to as "a transaction platform" or "a service provider platform" and these terms are interchangeable as used.

According to the system and the method in accordance with the present invention, the data transaction can comprise and/or trigger the access to and/or controlling of an entity, such as a physical entity, such as a machine, a gate, such as an airport gate in case of the issuance of an airline ticket. The system is further useful for the issuing of airline tickets and has the advantage that the ticket itself can be securely and readily transmitted forward from a node (participating user) or returned, if the airline allows such. Other type of tickets, such as tickets to sporting events and concerts, are often issued to specified users only, to prevent hoarding and black-market sales. Such tickets may be issued to a user in a system or platform of registered users in accordance with the present invention, where verified user names and user UIDs allow safe issuing and transmission of tickets to specified users. Thus, the system and method if the invention is further useful for management of other intangible goods such as but not limited to shares, titles, IDs, other tickets such as event tickets or documents, e.g. certificates, associated with a specified user, alternatively, associated with, or in addition to transactions with money and e-money as described herein. The user may then hold a digital wallet, where these other intangible goods are

issued to a digital wallet holding one or more blockchain addresses associated with the blockchain network, as further described herein.

The term node is used herein as generally understood in the art. Thus, a node may generally refer to an access point in a network. In some embodiments the node may comprise a computer and/or a peripheral, a cell phone, a tablet, PC or other means to access to the network by any user device. The node may be attached to a network. The node may further comprise a wearable attached to, tech togs and/or a smart electronic device that may be installed close to and/or on the surface of the skin, where they detect, analyse, and transmit information concerning e.g. ambient data and which allow in some cases immediate feedback to the wearer. The ambient data may comprise geographical data. The node may further comprise the node interface. The node interface may comprise an output interface, such as: screens or monitors configured to display visual data (e.g. displaying graphical user interfaces of the questionnaire to the user), speakers configured to communicate audio data (e.g. playing audio data to the user). The node interface can also comprise an input interface, such as, camera configured to capture visual data (e.g. capturing images and/or videos of the user), microphone configured to capture audio data (e.g. recording audio from the user), and a keyboard configured to allow the insertion of text and/or other keyboard commands (e.g. allowing the user to enter text data and/or another keyboard and mouse, touchscreen, joystick – configured to facilitate the navigation through different graphical user interfaces of the questionnaire.

It will also be understood that the term module may also refer to a computer program, and/or a device, and/or a plurality of each or both that may provide functionality for other programs, devices and/or components of the present invention. For instance, a module, such as transferring module may provide various functionalities, which may be referred to as services, such as, for example, sharing data or resources among multiple clients, or performing computation and/or storage functions. It will further be understood that a single module may serve multiple clients, and a single client may use multiple modules. Furthermore, a client process may run on the same device or may connect over a network to a server on a different device, such as a remote server or a cloud. The module may have rather primitive functions, such as just transmitting rather short information to another level of infrastructure, or can have a more sophisticated structure, such as a storing, processing and transmitting unit.

In some embodiments the data processing component can comprise at least one of a CPU (central processing unit), GPU graphical processing unit), DSP (digital signal processor), APU (accelerator processing unit), ASIC (application-specific integrated circuit), ASIP (application-specific instruction-set processor) or FPGA (field programmable gate array) or any combination thereof. Thus, in some embodiment the transferring module in the present

invention can be referred to as a processing server, which may include one or more or all of the above-mentioned functionalities.

In some embodiments the data processing component can further be generating the database using the node data. The data processing component can be configured to automatically recognize the node associated with the node data and can further generate the database based on the node. In some further embodiments the node profile may comprise the database or part thereof. The data processing component can be configured with machine learning techniques, such as deep learning techniques.

In some embodiments the node data can comprise all the data related to a user or participant.
In some embodiments input transaction data for a transfer of data is used for automatically generating a transaction order, wherein the input transaction data is formatted based on one or more standards for a data transaction. Such standard can be selected from SEPA, IBAN, BIC for financial data transfer; standardized format for airline tickets (including terms such as name, airline, seat number, fare code; IATA standardized schedules information (SSIM), NDC (New Distribution Capability) airline distribution system, etc.

In some embodiments the transferring module may comprise an application programming interface. The system may further comprise the data processing component which may be configured to extract node data from a user device. The user device may be a smart phone, app, computing device and the like. The user device may also be equipped with a digital wallet, like metamask.

In some embodiments the node profile comprises the profile of a user including the node data. The user data may be aggregated in a dataset and potentially encrypted etc., the IP address of a node, for example. In some embodiments the node profile comprises at least one unique identifier (UID). The UID can advantageously comprise a string of alphanumeric characters and/or QR code.

In some furthermore embodiments the UID may be configured to be associated with the node. The system may further be configured to authorise the at least one node to participate in a transaction process. In some furthermore embodiments the UID may be an address to a digital wallet on a blockchain network, further being the access information to a user account.

In some embodiments the data processing component may be configured to authorise the at least one node to participate in the transaction process once the node inputs the UID. The UID may comprise a blockchain address.

In some embodiments the UID may comprise at least one of public key and private key. In some embodiments the node may comprise the at least one node profile. The node

profile may further comprise a plurality of UID, wherein each UID may be configured to be unique to the node.

In some further embodiments the transferring module may comprise an e-money issuer. Further, the data processing component may be configured to extract node data from the user device, wherein the user device comprises a digital wallet.

In some embodiments the transferring module may comprise an e-money generator. Further, the transferring module may comprise an e-money remover. Furthermore, the transferring module may be configured to generate a balance value based on transaction data. The balance value may comprise the quantity of e-money.

In some embodiments the balance value may comprise a monetary value in any monetary unit(s), such as euro, GBP, USD, etc. The transferring module may further be configured to generate transaction data associated with each UID.

In some embodiments the transferring module may further be configured to associate at least one balance value to the at least one node profile. Furthermore, the transferring module may comprise a token generator.

In some embodiments the system may comprise a node interface. The node interface may comprise a computing device, such as a smart phone, laptop and the like. The node interface may further comprise an output interface and/or an input interface.

In some embodiments the node interface can be configured to extract node data from at least one node. Further, the data processing component can be configured to enable a data exchange between the node interface and the node profile.

In some further embodiments the at least one node profile can comprise a shared ledger. The system can further be configured to associate at least one transaction protocol to the node profile. In such embodiments the transaction protocol may be stored on a distributed ledger.

In some embodiments the transaction protocol can be configured to automatically self-execute and/or execute and/or control and/or document and/or store the at least one transaction event. The transaction protocol can further comprise at least one smart contract. The transaction protocol can be configured to facilitate the update of the distributed ledger and/or grouped operations and/or transferring operations with one or more command instructions.

In some embodiments the transferring module can be configured to associate at least one transaction protocol to the node profile. The system can comprise at least one of at least one and a plurality of datastore. The datastore may comprise a blockchain network, such as Ethereum.

In some embodiments the datastore comprises blockchain-based distributed computing platform. The transaction protocol may be configured to be stored in the datastore.

In some further embodiments the node profile may be configured to be stored in the datastore. In some embodiments the system may further comprise an account generator. The account generator may comprise a computing unit. The data processing component may comprise the account generator.

In some embodiments the account generator may be configured to automatically generate a node account based on node profile. The node account may comprise a proxy bank account. The proxy bank account can further be configured to be stored on a memory component. The memory component can comprise comprises a volatile or non-volatile memory, such as a random-access memory (RAM), Dynamic RAM (DRAM), Synchronous Dynamic RAM (SDRAM), static RAM (SRAM), Flash Memory, Magneto-resistive RAM (MRAM), Ferroelectric RAM (F-RAM), or Parameter RAM (P-RAM). Preferably the proxy bank account is stored on the transferring module.

In some further embodiments the data processing component may comprise the memory component. The node account may also be configured to be stored in the datastore. The datastore may comprise a blockchain network. The datastore may comprise a shared ledger, for example, the Ethereum mainnet, and network participants, which are computers or nodes where the ledger is stored, updated, and maintained using the blockchain technology.

In some embodiments the node account may be configured to participate in the transaction process. In some further embodiments wherein, the system may comprise a master account. The data processing component may be configured to exchange data with the master account. In some further embodiments the master account may comprise a virtual bank account.

In some embodiments the node account may be configured to participate in the transaction process using at least one of the existing financial entity. The system may further be configured to enable bilateral data exchange between at least one user device and a node.

In some embodiments the transferring module may be configured to connect the at least one user device to participate in the transaction process. In some further embodiments the transferring module may be configured to associate the at least one node profile with the at least one user device.

In some embodiments the transferring module may be configured to associate the at least one node with the at least one user device. The system may further be configured to associate the at least one node profile with the at least one connected user device, such as a digital wallet.

In some further embodiments the system may be advantageously configured enable a transaction request from the at least one node to the at least one financial entity. The transaction request may comprise an operational command to initiate the transaction process.

In some embodiments the system may be configured to enable the transaction process from the at least one node to the at least one financial entity using the transferring module. The financial entity typically refers to a conventional authorised bank or other authorised financial institution that operates according to conventional recognised bank protocols.

In some embodiments the system may further be configured to enable the transaction process from the node to the datastore. The system may further be configured to enable the transaction process from the node to the at least one node profile stored in the datastore.

In some embodiments the system may further be configured to enable the transaction process from the node to the at least one UID. The system may be further configured to enable the transaction process from the node to the at least one transaction protocol stored on the at least one of datastore.

In some further embodiments the transferring module may be configured to enable the at least one transaction process from the financial entity to the node profile. The transferring module may be configured to enable the at least one transaction process from the financial entity/institution to the proxy bank account.

In some furthermore embodiments the transferring module may be configured to automatically detect the balance value associated in the transaction process. The transferring module may be configured to transfer the balance value from the proxy bank account to the master account.

In some embodiments the transferring module may be configured to automatically associate the balance value based on the transaction process to the respective UID.

In some embodiments the transferring module may be configured to automatically associate the balance value based on the transaction process to the respective UID with the same monetary units. In some further embodiments the e-money generator may be configured to associate a positive value to the respective UID. The positive value may comprise a positive balance value.

In some embodiments the system may be configured to enable the at least one transaction process from the at least one UID to the financial entity. The system may further be configured to enable at least one transaction process from the at least one node profile to the financial entity/institution.

In some embodiments the e-money remover may be configured to automatically deduct/subtract/remove the value from the proxy bank account. The transferring module may be configured to instruct the master bank to enable the transaction to the financial entity.

In some embodiments wherein the system may be configured to enable the at least one transaction process between the at least two UIDs. The system may further be configured to enable the at least one transaction process between the at least two node profiles.

In some embodiments the system may be configured to enable the at least one transaction process from the at least one financial entity to the at least one datastore. The system may be configured to enable the at least one transaction process between the at least two datastores.

In some embodiments the system may be configured to enable the at least one transaction process from the at least one UID to the at least one datastore. In some embodiments the system may be configured to enable the at least one transaction process from the at least one smart contract to the at least one datastore.

In another embodiment a computer implemented method is disclosed. The system may be configured to perform any of the method steps according to any of the relevant method embodiment.

Below, **system embodiments** will be discussed. These embodiments are abbreviated by the letter "S" followed by a number. Whenever reference is herein made to "system embodiments", these embodiments are meant.

S1. A system, wherein the system comprises:

i. at least one node, configured to provide node data;

ii. a data-processing component, wherein the data processing component is configured to automatically generate a node profile based on at least the node data; and

iii. at least one transferring module configured to initiate a transaction process based on the node profile.

S2. The system according to the preceding embodiment wherein the data processing component is configured to extract node data from a user device.

S3. The system according to any of the preceding embodiments wherein the transaction process comprises the access to and/or controlling of an entity.

S4. The system according to any of the preceding embodiments wherein the transaction process comprises the access to and/or controlling of a machine.

S5. The system according to any of the preceding embodiments wherein the transaction process comprises the access to and/or controlling of a gate such as an airport gate.

S6. The system according to any of the preceding embodiments wherein the node profile comprises at least one unique identifier (UID).

S7. The system according to the preceding embodiment wherein the UID comprises a string of alphanumeric characters and/or QR code.

S8. The system according to any of the preceding embodiments wherein the UID is configured to be associated with the node.

S9. The system according to any of the preceding embodiments wherein the system is configured to authorise the at least one node to participate in a transaction process.

S10. The system according to the preceding embodiment wherein the data processing component is configured to authorise the at least one node to participate in the transaction process once the node inputs the UID.

S11. The system according to any of the preceding embodiments wherein the UID comprises at least one of public key and private key.

S12. The system according to any of the preceding embodiments wherein the node comprises the at least one node profile.

S13. The system according to any of the preceding embodiments wherein the node profile comprises a plurality of UID, wherein each UID is configured to be unique to the node.

S14. The system according to any of the preceding embodiments wherein the transferring module comprises an e-money issuer.

S15. The system according to any of the preceding embodiments wherein the data processing component is configured to extract node data from the user device, wherein the user device comprises a digital wallet.

S16. The system according to any of the preceding embodiments wherein the transferring module comprises an e-money generator.

S17. The system according to any of the preceding embodiments wherein the transferring module comprises an e-money remover.

S18. The system according to any of the preceding embodiments wherein the transferring module is configured to generate a balance value based on transaction data.

S19. The system according to any of the preceding embodiments wherein the balance value comprises a monetary value in any monetary unit(s).

S20. The system according to any of the preceding embodiments wherein the transferring module is configured to generate transaction data associated with each UID.

S21. The system according to any of the preceding embodiments wherein the transferring module is further configured to associate at least one balance value to the at least one node profile.

S22. The system according to any of the preceding embodiments wherein the transferring module further comprises a token generator.

S23. The system according to any of the preceding embodiments wherein the system further comprises a node interface.

S24. The system according to any of the preceding embodiments wherein the node interface is configured to extract node data from at least one node.

S25. The system according to any of the preceding embodiments wherein the data processing component is further configured to enable a data exchange between the node interface and the node profile.

S26. The system according to any of the preceding embodiments wherein the at least one node profile comprises a shared ledger.

S27. The system according to any of the preceding embodiments wherein the system further comprises at least one transaction protocol.

S28. The system according to any of the preceding embodiments wherein the system is further configured to associate the at least one transaction protocol to the node profile.

S29. The system according to the preceding embodiment wherein the transaction protocol is configured to automatically self-execute and/or control and/or document and/or store the at least one transaction event.

S30. The system according to the preceding embodiment wherein the transaction protocol comprises at least one smart contract.

S31. The system according to any of the preceding embodiments wherein the transferring module is configured to associate the at least one transaction protocol to the node profile.

S32. The system according to any of the preceding embodiments wherein the system comprises at least one of at least one and a plurality of datastore.

S33. The system according to the preceding embodiment wherein the datastore comprises blockchain-based distributed computing platform.

S34. The system according to any of the preceding embodiments wherein the transaction protocol is configured to be stored in the datastore.

S35. The system according to any of the preceding embodiments wherein the node profile is configured to be stored in the datastore.

S36. The system according to any of the preceding embodiments wherein the system further comprises an account generator.

S37. The system according to any of the preceding embodiments wherein the data processing component comprises the account generator.

S38. The system according to any of the preceding embodiments wherein the account generator is configured to generate a node account based on node profile.

S39. The system according to any of the preceding embodiments wherein the node account comprises a proxy bank account.

S40. The system according to any of the preceding embodiments wherein the proxy bank account is configured to be stored on a memory component.

S41. The system according to any of the preceding embodiments wherein the data processing component comprises the memory component.

S42. The system according to any of the preceding embodiments wherein the node account is configured to be stored in the datastore.

S43. The system according to any of the preceding embodiments wherein the node account is configured to participate in the transaction process.

S44. The system according to any of the preceding embodiments wherein the system comprises a master account.

S45. The system according to any of the preceding embodiments wherein the data processing component is configured to exchange data with the master account.

S46. The system according to any of the preceding embodiments wherein the master account comprises a virtual bank account.

S47. The system according to any of the preceding embodiments wherein the node account is configured to participate in the transaction process using at least one of the existing financial entity.

S48. The system according to any of the preceding embodiments wherein the system is further configured to enable bilateral data exchange between at least one user device and a node.

S49. The system according to any of the preceding embodiments wherein the transferring module is configured to connect the at least one user device to participate in the transaction process.

S50. The system according to any of the preceding embodiments wherein the transferring module is configured to associate the at least one node profile with the at least one user device.

S51. The system according to any of the preceding embodiments wherein the transferring module is configured to associate the at least one node with the at least one user device.

S52. The system according to any of the preceding embodiments wherein the system is configured to associate the at least one node profile with the at least one connected user device, such as a digital wallet.

S53. The system according to any of the preceding embodiments wherein the system is configured to enable a transaction request from the at least one node to the at least one financial entity.

S54. The system according to any of the preceding embodiments wherein the system is configured to enable the transaction process from the at least one node to the at least one financial entity using the transferring module.

S55. The system according to any of the preceding embodiments wherein the system is further configured to enable the transaction process from the node to the datastore.

S56. The system according to any of the preceding embodiments wherein the system is further configured to enable the transaction process from the node to the at least one node profile stored in the datastore.

S57. The system according to any of the preceding embodiments wherein the system is further configured to enable the transaction process from the node to the at least one UID.

S58. The system according to any of the preceding embodiments wherein the system is further configured to enable the transaction process from the node to the at least one transaction protocol stored on the at least one of datastore.

S59. The system according to any of the preceding embodiments wherein the transferring module is configured to enable the at least one transaction process from the financial entity to the node profile.

S60. The system according to any of the preceding embodiments wherein the transferring module is configured to enable the at least one transaction process from the financial entity to the proxy bank account.

S61. The system according to any of the preceding embodiments wherein the transferring module is configured to automatically detect the balance value associated in the transaction process.

S62. The system according to any of the preceding embodiments wherein the transferring module is further configured to transfer the balance value from the proxy bank account to the master account.

S63. The system according to any of the preceding embodiments wherein the transferring module is configured to automatically associate the balance value based on the transaction process to the respective UID.

S64. The system according to any of the preceding embodiments wherein the transferring module is configured to automatically associate the balance value based on the transaction process to the respective UID with the same monetary units.

S65. The system according to any of the preceding embodiments wherein the e-money generator is configured to associate a positive value to the respective UID.

S66. The system according to any of the preceding embodiments wherein the system is configured to enable the at least one transaction process from the at least one UID to the financial entity.

S67. The system according to any of the preceding embodiments wherein the system is configured to enable at least one transaction process from the at least one node profile to the financial entity.

S68. The system according to any of the preceding embodiments wherein the e-money remover is configured to automatically deduct the value from the proxy bank account.

S69. The system according to any of the preceding embodiments wherein the transferring module is configured to instruct the master bank to enable the transaction to the financial entity.

S70. The system according to any of the preceding embodiments wherein the system is configured to enable the at least one transaction process between the at least two UIDs.

S71. The system according to any of the preceding embodiments wherein the system is configured to enable the at least one transaction process between the at least two node profiles.

S72. The system according to any of the preceding embodiments wherein the system is configured to enable the at least one transaction process from the at least one financial entity to the at least one datastore.

S73. The system according to any of the preceding embodiments wherein the system is configured to enable the at least one transaction process between the at least two datastores.

S74. The system according to any of the preceding embodiments wherein the system is configured to enable the at least one transaction process from the at least one UID to the at least one datastore.

S75. The system according to any of the preceding embodiments wherein the system is configured to enable the at least one transaction process from the at least one smart contract to the at least one datastore.

Below, **method embodiments** will be discussed. These embodiments are abbreviated by the letter "M" followed by a number. Whenever reference is herein made to "method embodiments", these embodiments are meant.

M1. A computer-implemented method, comprising the steps of:

i. authorizing at least one node to participate in a transaction process; and

ii. enabling the transaction process between at least two participants using at least one transferring module.

M2. The method according to any of the preceding embodiments wherein the method comprises the step of carrying out the method on the system according to any of the preceding system embodiments.

M3. The method according to any of the preceding embodiments wherein the method comprises automatically generating a node profile based on at least a portion of node data.

M4. The method according to any of the preceding embodiments wherein the method comprises automatically generating a node profile based on at least a portion of node data by a data processing component.

M5. The method according to any of the preceding embodiments wherein the method comprises automatically initiating the transaction process, preferably based on the node profile.

M6. The method according to any of the preceding embodiments wherein the method comprises automatically initiating the transaction process by the transferring module.

M7. The method according to any of the preceding embodiments wherein the method comprises extracting node data from at least the user device.

M8. The method according to any of the preceding embodiments wherein the method comprises associating at least one unique identifier (UID) with the node profile.

M9. The method according to any of the preceding embodiments wherein the method comprises associating each node with the at least one UID.

M10. The method according to the preceding embodiment wherein the participant comprises at least one of node profile and UID and datastore and transaction protocol and financial entity and proxy bank account and user device and master account.

M11. The method according to any of the preceding embodiments wherein the method comprises authorizing the at least one node to participate in a transaction process.

M12. The method according to any of the preceding embodiments wherein the method comprises authorizing the at least one node to participate in the transaction process using data processing component.

M13. The method according to any of the preceding embodiments wherein the method comprises authorizing the at least one node to participate in the transaction process using the node input and/or the UID.

M14. The method according to any of the preceding embodiments wherein the node input comprises UID, wherein the UID comprises at least one of public key and/or private key.

M15. The method according to any of the preceding embodiments wherein the method comprises associating a plurality of UID to the node profile, wherein each UID is configured to be unique to the node.

M16. The method according to any of the preceding embodiments wherein the method further comprises providing an e-money issuer.

M17. The method according to any of the preceding embodiments wherein the method comprises providing the transferring module an e-money issuer.

M18. The method according to any of the preceding embodiments wherein the method comprises extracting node data from the user device, wherein the user device comprises a digital wallet.

M19. The method according to any of the preceding embodiments wherein the method comprises providing an e-money generator.

M20. The method according to any of the preceding embodiments wherein the method comprises providing the transferring module with the e-money generator.

M21. The method according to any of the preceding embodiments wherein the method comprises providing an e-money remover.

M22. The method according to any of the preceding embodiments wherein the method comprises providing the transferring module with the e-money remover.

M23. The method according to any of the preceding embodiments wherein the method further comprises generating a balance value.

M24. The method according to any of the preceding embodiments wherein the method comprises generating the balance value based on transaction data.

M25. The method according to any of the preceding embodiments wherein the method comprises generating the balance value by the transferring module.

M26. The method according to any of the preceding embodiments wherein the method comprises generating the balance value using the transaction protocol.

M27. The method according to any of the preceding embodiments wherein the method comprises generating transaction data associated with the at least one UID.

M28. The method according to any of the preceding embodiments wherein the method comprises generating transferring module associated with the UID using the transferring module.

M29. The method according to any of the preceding embodiments wherein the method further comprises associating the at least one balance value with the at least one node profile.

M30. The method according to any of the preceding embodiments wherein the method comprises associating the at least one balance value with the at least one node profile using the transferring module.

M31. The method according to any of the preceding embodiments wherein the method further comprises providing a token generator.

M32. The method according to any of the preceding embodiments wherein the method comprises providing the token generator to the transferring module.

M33. The method according to any of the preceding embodiments wherein the method comprises providing a node interface.

M34. The method according to any of the preceding embodiments wherein the method comprises automatically extracting node data from the at least one node.

M35. The method according to any of the preceding embodiments wherein the method comprises enabling a data exchange between the node interface and the node profile.

M36. The method according to any of the preceding embodiments wherein the method comprises enabling the data exchange between the node interface and the node profile using the data processing component.

M37. The method according to any of the preceding embodiments wherein the method comprises providing at least one shared ledger.

M38. The method according to the preceding embodiment wherein the method comprises providing the at least one shared ledger to the at least one node profile.

M39. The method according to any of the preceding embodiments wherein the method comprises associating the at least one transaction protocol to the at least one node profile.

M40. The method according to any of the preceding embodiments wherein the method comprises automatically self-executing at least one transaction event.

M41. The method according to any of the preceding embodiments wherein the method comprises automatically executing [is this different from self-executing?] the at least one transaction event.

M42. The method according to any of the preceding embodiments wherein the method comprises automatically documenting the at least one transaction event.

M43. The method according to any of the preceding embodiments wherein the method comprises automatically storing the at least one transaction event.

M44. The method according to any of the preceding embodiments wherein the method comprises providing the transaction event, wherein the transaction event comprises transaction process.

M45. The method according to any of the preceding embodiments wherein the method comprises providing the transaction protocol, wherein the transaction protocol comprises at least one smart contract.

M46. The method according to any of the preceding embodiments wherein the method comprises associating the at least one transaction protocol to the node profile.

M47. The method according to any of the preceding embodiments wherein the method comprises associating the at least one transaction protocol to the node profile using the transferring module.

M48. The method according to any of the preceding embodiments wherein the method comprises providing at least one of at least one and a plurality [don't understand] of datastore.

M49. The method according to any of the preceding embodiments wherein the datastore comprises blockchain-based distributed computing platform.

M50. The method according to any of the preceding embodiments wherein the method comprises storing the at least one transaction protocol on the at least one datastore.

M51. The method according to any of the preceding embodiments wherein method comprises storing the at least one node profile on the datastore.

M52. The method according to any of the preceding embodiments wherein method comprises storing the at least one node data on the datastore.

M53. The method according to any of the preceding embodiments wherein the method further comprises providing an account generator.

M54. The method according to any of the preceding embodiments wherein the method comprises providing the data processing component with the account generator.

M55. The method according to any of the preceding embodiments wherein the method comprises generating a node account based on node profile.

M56. The method according to any of the preceding embodiments wherein the method comprises generating a node account based on node profile using the account generator.

M57. The method according to any of the preceding embodiments wherein the node account comprises a proxy bank account.

M58. The method according to any of the preceding embodiments wherein the method comprises storing the proxy bank account in a memory component.

M59. The method according to any of the preceding embodiments wherein the method comprises providing the data processing component with the memory component.

M60. The method according to any of the preceding embodiments wherein the method comprises storing the node account.

M61. The method according to any of the preceding embodiments wherein the method comprises storing the node account in the datastore.

M62. The method according to any of the preceding embodiments wherein method comprises facilitating the node account to participate in the transaction process.

M63. The method according to any of the preceding embodiments wherein method comprises automatically participating the node account in the transaction process

M64. The method according to any of the preceding embodiments wherein the method comprises providing a master account.

M65. The method according to any of the preceding embodiments wherein the method comprises exchanging data between the master account and the data processing component.

M66. The method according to any of the preceding embodiments wherein the master account comprises a virtual bank account.

M67. The method according to any of the preceding embodiments wherein the method comprises facilitating the at least one node account to participate in the transaction process.

M68. The method according to any of the preceding embodiments wherein the method comprises facilitating the at least one node account to participate in the transaction process using at least one financial entity.

M69. The method according to any of the preceding embodiments wherein the method further comprises enabling bilateral data exchange between the at least one user device and the at least one node.

M70. The method according to any of the preceding embodiments wherein the method comprises connecting the at least one user device to participate in the transaction process.

M71. The method according to any of the preceding embodiments wherein the method comprises connecting the at least one user device to participate in the transaction process using the transferring module.

M72. The method according to any of the preceding embodiments wherein the method comprises associating the at least one node profile with the at least one connected user device, such as a digital wallet.

M73. The method according to any of the preceding embodiments wherein the method comprises enabling at least one transaction request from the at least one node to the at least one financial entity.

M74. The method according to any of the preceding embodiments wherein the method comprises enabling the transaction process from the at least one node to the at least one financial entity.

M75. The method according to any of the preceding embodiments wherein the method comprises enabling the transaction process from the at least one node to the at least one financial entity using the transferring module.

M76. The method according to any of the preceding embodiments wherein the method further comprises enabling the transaction process from the node to the datastore.

M77. The method according to any of the preceding embodiments wherein the method comprises enabling the transaction process from the node to the at least one node profile stored in the datastore.

M78. The method according to any of the preceding embodiments wherein the method comprises enabling the transaction process from the node to the at least one node profile stored in the transferring module.

M79. The method according to any of the preceding embodiments wherein the method comprises enabling the transaction process from the node to the at least one UID.

M80. The method according to any of the preceding embodiments wherein the method comprises enabling the transaction process from the node to the at least one transaction protocol stored on the at least one of datastore.

M81. The method according to any of the preceding embodiments wherein the method comprises enabling the at least one transaction process from the financial entity to the node profile.

M82. The method according to any of the preceding embodiments wherein the method comprises enabling the at least one transaction process from the financial entity to the node profile using the transferring module.

M83. The method according to any of the preceding embodiments wherein the method comprises enabling the at least one transaction process from the financial entity to the proxy bank account.

M84. The method according to any of the preceding embodiments wherein the method comprises enabling the at least one transaction process from the financial entity to the proxy bank account using the transferring module.

M85. The method according to any of the preceding embodiments wherein the method comprises automatically detecting the balance value associated in the transaction process.

M86. The method according to any of the preceding embodiments wherein the method comprises automatically detecting the balance value associated in the transaction process using the transferring module.

M87. The method according to any of the preceding embodiments wherein the method comprises transferring the balance value from the proxy bank account to a master account.

M88. The method according to any of the preceding embodiments wherein the method comprises transferring the balance value from the proxy bank account to a master account using the transferring module.

M89. The method according to any of the preceding embodiments wherein the method comprises automatically transferring the balance value from the proxy bank account to a master account.

M90. The method according to any of the preceding embodiments wherein the method comprises automatically transferring the balance value from the proxy bank account to a master account using the transferring module.

M91. The method according to any of the preceding embodiments wherein the method comprises automatically associating the balance value based on the transaction process to the respective UID.

M92. The method according to any of the preceding embodiments wherein the method comprises automatically associating the balance value based on the transaction process to the respective UID using the transferring module.

M93. The method according to any of the preceding embodiments wherein the method comprises automatically associating associate the balance value based on the transaction process to the respective UID with the same monetary units.

M94. The method according to any of the preceding embodiments wherein the method comprises automatically associating associate the balance value based on the transaction process to the respective UID with the same monetary units using the transferring module.

M95. The method according to any of the preceding embodiments wherein the method comprises automatically associating a positive value to the respective UID.

M96. The method according to any of the preceding embodiments wherein the method comprises automatically associating a positive value to the respective UID using the e-money generator.

M97. The method according to any of the preceding embodiments wherein the method comprises enabling the at least one transaction process from the at least one UID to the financial entity.

M98. The method according to any of the preceding embodiments wherein the method comprises enabling at least one transaction process from the at least one node profile to the financial entity.

M99. The method according to any of the preceding embodiments wherein the method comprises automatically deducting the balance value from the proxy bank account.

M100. The method according to any of the preceding embodiments wherein the method comprises automatically deducting the balance value from the proxy bank account using the e-money remover.

M101. The method according to any of the preceding embodiments wherein the method comprises automatically instructing the master bank to enable the transaction to the financial entity.

M102. The method according to any of the preceding embodiments wherein the method comprises automatically instructing the master bank to enable the transaction to the financial entity using the transferring module.

M103. The method according to any of the preceding embodiments wherein the method comprises automatically enabling the at least one transaction process between the at least two UIDs.

M104. The method according to any of the preceding embodiments wherein the method comprises automatically enabling the at least one transaction process between the at least two node profiles.

M105. The method according to any of the preceding embodiments wherein the method comprises automatically enabling the at least one transaction process from the at least one financial entity to the at least one datastore.

M106. The method according to any of the preceding embodiments wherein the method comprises automatically enabling the at least one transaction process between the at least two datastores.

M107. The method according to any of the preceding embodiments wherein the method comprises automatically enabling the at least one transaction process from the at least one UID to the at least one datastore.

M108. The method according to any of the preceding embodiments wherein the method comprises automatically enabling the at least one transaction process from the at least one transaction protocol to the at least one datastore.

Below, **program embodiments** will be discussed. These embodiments are abbreviated by the letter "P" followed by a number. Whenever reference is herein made to "program embodiments", these embodiments are meant.

P1. A computer program product comprising instructions, which, when the program is executed by an end user interface device, causes an end user device to perform the method steps according to any method embodiment, which have to be executed on the user interface device, wherein the end user device is according to any system embodiment that comprises a user interface device that is compatible to said method embodiment.

P2. A computer program product comprising instructions, which, when the program is executed by a combination of a data processing component and an end user device, cause the end user device and the data processing component to perform the method steps according to any method embodiment, which have to be executed on the data processing component and the end user device, wherein the end user device and the data processing system is according to any system embodiment that comprises a data processing component and/or the end user device that is compatible to said method embodiment.

P3. A computer program product comprising instructions, which, when the program is executed by a data processing component, cause the data processing component to perform the method steps according to any method embodiment, which have to be executed on the data processing component, wherein the data processing component is according to any system embodiment that comprises a data processing component that is compatible to said method embodiment.

Brief description of the embodiments

Fig. 1 schematically shows an exemplary embodiment according to the present invention.

Fig. 2 schematically shows an exemplary embodiment according to the present invention

Detailed description of the embodiments

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

Fig. 1 shows an exemplary embodiment according to the present invention. One embodiment of transaction process **a** from a financial entity 1 to an UID 3 is shown, via the proxy bank account 2. The UID 3 can comprise a blockchain address. The public blockchain address can receive and hold digital assets such as cryptocurrency or e-money. The corresponding private key, known only to the owner, can be used to sign transactions for the public address, including transfers of assets to other addresses. For example, for a private key: 60cf347dbc59d31c1358c8e5cf5e45b822ab85b79cb32a9f3d98184779a9efc2, the public address can be: 0xA21D0cf8A9a5eED856B92A341a61cE0c1C74d4c2.

The proxy bank account 2 can be the digital bank account generated by an account generator which is part of the system of the invention. The proxy bank account can be used to receive and send money for a specific node profile within existing payment systems e.g. SWIFT and SEPA. The financial entity 1 can comprise an external bank account which can be using standardized protocol for bank transfers. For example, all European countries and several outside Europe use the IBAN standard for international bank accounts and bank transfers. An IBAN designation is a string of up to 34 characters, two all caps letters denoting the country, followed by two checksum numbers, which in turn is followed by a country dependent alphanumeric string designating the bank, the branch, and the account. The proxy bank account 2 can also comprise a virtual bank account hence a virtual IBAN. A virtual IBAN is an IBAN which is not a bank account but serves as a proxy for another IBAN address. Such virtual IBAN account can be used to reroute payments to a "real" IBAN and its underlying physical bank account.

The proxy bank account can hold money in a specific monetary unit, for example a regular currency, e.g. euro, for a specific UID (e.g. 0xA21D0cf8A9a5eED856B92A341a61cE0c1C74d4c2) that can be located on a specific datastore 4 (example, Ethereum mainnet).

For the transaction process **a**, money can be sent from a financial entity to the proxy bank account using existing payment systems. The payment once received by the proxy bank account and detected by the transferring module can be transferred to a master account. The master account can further communicate to the transferring module the balance value received. The e-money generator can mint the e-money and associate it to the UID 3.

In the transaction process **b**, a transaction from a UID 3 and/or an associated node profile to a financial entity 1, via proxy bank account 2 is shown. The node can be configured to generate a transaction request for a specified value of transaction. Further, the node can also be configured to select at least one proxy bank account to authorize the transaction. When the request is successful the e-money remover burns the value from the UID 3 and/or the node profile and transfers the value to the requested financial entity 1, using the existing payment systems, such as BIC, IBAN, sort codes, account numbers, etc.

In a transaction process **c**, a transaction from a UID 3 stored in a datastore 4 to a second UID 3′ stored in second datastore 4′ is shown. The datastore 4 can be made up of a shared ledger, example, the Ethereum mainnet, and network participants, which are computers or nodes where the ledger is stored, updated, and maintained using the blockchain technology. The transferring module can be configured to perform an AML (Anti Money Laundering) and/or CFT (Countering Financing of Terrorism) audits for the transaction request initiated by the node, may be at the node interface. The node interface may comprise an output interface, such as: screens or monitors configured to display visual data (e.g. displaying graphical user interfaces of the questionnaire to the user), speakers configured to communicate audio data (e.g. playing audio data to the user). The node interface can also comprise an input user interface, such as, camera configured to capture visual data (e.g. capturing images and/or videos of the user), microphone configured to capture audio data (e.g. recording audio from the user), and a keyboard configured to allow the insertion of text and/or other keyboard commands (e.g. allowing the user to enter text data and/or another keyboard and mouse, touchscreen, joystick – configured to facilitate the navigation through different graphical user interfaces of the questionnaire. After the request is successful the value is burned from the originating UID 3 and mint at the destination UID 3′. It may be noted that at least two UIDs 3, 3′ can be stored in at least two datastores 4, 4′. The datastore 4, 4′ may comprise a blockchain network.

In a transaction process **d**, a transaction from a financial entity 1 to a transaction protocol 5, via the proxy bank account 2 is shown. In such embodiments, money can be sent from the at least one financial entity 1 to the at least one proxy bank account 2, associated to the at least one node, using existing payment systems e.g. BIC, IBAN, sort codes and account numbers, etc. The payment can be then received at the proxy bank account 2 and detected by the transferring module. The transferring module can further automatically transfer the payment from the proxy bank account 2 to the at least one master account.

The transferring module can then automatically create an instructional command for the payment and perform required audits. After the request is successfully processed and approved, the transferring module will deduct balance value from the proxy bank account 2 and the e-money generator can mint the balance value to the transaction protocol 5 in the same currency as the payment with applicable metadata that is required by the transaction protocol 5.

In a transaction process **e**, a transaction from an UID 3 stored in the datastore 4 to a transaction protocol 5 stored in a second datastore 4′ is shown. The data processing component can allow the at least one node to authenticate a transaction request, using node data, such as username and password. Node profile can then be created by the data processing component. The node profile can comprise the request to send a specified amount of money from the node's UID 3 to a transaction protocol 5. After the processing and approval, the transferring module can burn the amount from the UID 3, and mint the remainder to the blockchain transaction protocol 5 in the same currency with applicable metadata that is required by the transaction protocol 5.

In Fig. 2 a second embodiment of the invention is disclosed. In a transaction process **f**, an automatic transfer of balance value 6 from the at least one UID 3 to a financial entity 1 is shown. It may be noted that the balance value 6 can comprise e-money. The balance value 6 is transferred from an originating UID 3 to a second UID 3′, on the same datastore 4, with automatic pay-out operation which can be pre-configured to transfer the balance value 6 to a financial entity 1. The transferring module can be configured to detect inbound payment to the UID 3′, and burn the corresponding balance value 6 from the UID 3. Further, the transferring module can detect that transactions completed successfully and automatically create an order to send a specified amount of money and/or balance value 6 from the proxy bank account 2 to the financial entity 1. Once the order is successfully processed and approved, the transferring module, specifically e-money remover, will transfer the balance value 6 to the requested financial entity 1 using the existing payment systems.

In a transaction process **g**, an automatic transfer of money from at least one UID 3 to a second UID 3′ on a second datastore 4′ is shown. The at least one of second and first UID 3, 3′ may comprise a blockchain address with automatic pay-out operation. The money can be transferred from an originating UID 3 to a UID 3′, on the same datastore 4, with automatic pay-out operation pre-configured to transfer the money to a UID 3′ on another datastore 4′. A UID 3 on a datastore 4 can transfer balance value 6 to UID 3′ located on the different datastore 4′. The transferring module can automatically detect once the balance value 6 is transferred to the UID 3 and burns the amount from the UID 3 on datastore 4 and mints the same balance value 6 to the UID 3' located on datastore 4'.

In a transaction process **h**, an automatic transfer of money from a UID 3 to a transaction protocol 5 on another datastore 4′ is shown. The transferring module can be configured to transfer the balance value 6 from UID 3 on datastore 4 to transaction protocol 5 on datastore 4′. The UID 3 can further be configured to automatically pay out any balance value 6 received to the at least one transaction protocol 5 located on datastore 4'. The transferring module automatically detects once balance value 6 is received for UID 3 and burns the amount from datastore 4 and mints the amount to the transaction protocol 5 on datastore 4' with any relevant metadata if applicable for the transaction protocol 5. The transferring module can deduct the balance value 6.

This, having regard to the above embodiment the invention can be exemplified in an embodiment where a method is provided for authorization and execution of a blockchain transaction, comprising:

storing, in a database of a transferring module, a plurality of user profiles, wherein each user profile includes data related to a unique user including at least one user ID, at least one user account, at least one instruction for transactions for each of the at least one user account, at least one address to a digital storage unit such as a digital wallet which is associated with a blockchain network, and at least one UID for the at least one digital storage unit;

generating, by a node (which in this embodiment can comprise a user device), a transaction order, by receiving input transaction data for a transfer of assets or other digital objects (data), wherein the transaction data includes a designation of a transaction party, which is typically a user with a user account in the database of the transaction module;

receiving the transaction order by the transferring module, wherein the order can be formatted based on one or more standards for a data transaction (such as SEPA, etc.);

identifying and verifying, by the transferring module, the designated party (user and user account stored in the transferring module database);

generating, by the transferring module, a transaction request for a blockchain transaction on a blockchain network, including selecting from the user profile an address to a digital storage unit being associated with a blockchain network;

broadcasting the blockchain transaction to the blockchain network;

where the blockchain network (nodes of the blockchain network) executes the transaction and updates the ledger to reflect the added transaction.

The transaction request for a blockchain transaction on a blockchain network may be authorized and executed based on the user profile and data from the transaction order.

The transaction request for a blockchain transaction on a blockchain network may comprise minting e-money to a blockchain network.

In some embodiments the user profile comprises information for a user account including information concerning minting any amount in a specific currency to a specific address associated with a blockchain network.

It is understood from the above that the user account can be a proxy account stored in the transferring module database.

Specifically, the transaction request for a blockchain transaction on a blockchain network may comprise burning a specified value of e-money from a blockchain network. The transaction request may further include transferring the specific value of e-money removed from a blockchain network to a user account stored on the transferring module. Advantageously, the user account can be a proxy account stored on the transferring module.

It follows that a user profile can comprise information for the proxy account including information concerning transferring any deposit in a specific currency to a second user account stored at a financial entity (bank).

The digital storage unit in the invention can thus advantageously comprise a blockchain wallet. A digital wallet / blockchain wallet used in the invention will generally and preferably store private and public key pairs of assets issued on blockchains. A random public key can be issued by any user and serves as that user's public address. Most blockchains use a shortened version of a public key as the user public address. The public address can receive and hold digital assets such as cryptocurrency or e-money, certificates, shares or other unique digital objects. A private key held by the user is used to sign transfers of assets to another public keys. The public address is derived from the private key through a series of mathematical operations.

Examples

In a more specific example of the invention the following exemplified embodiment is set forth:

Creation of User account

1. User A creates a user account with a username and password (UID) for his user account.
2. A transfer module (which in this example is a service provider platform) generates a user profile for User A.

3. The user entity as identified by the system (i.e. his identified device/peripheral or computer) can in this example be viewed as a node. The user profile comprises one or more of name, address and other required regulatory data (this would constitute at least part of node data). A digital wallet holding one or more blockchain addresses associated with a single blockchain network (data store) links the addresses to their user profile using private key.
4. The service provider platform generates e-money accounts for the blockchain address each in respective single currency as defined.
5. The service provider platform generates one or more bank account numbers and associates to one or more e-money accounts, where each bank account number may support single or multi-currency.

User-initiated transaction, User B to A

1. User B initiates a transaction by logging into an internet bank,
2. User B transfers 100 EUR from a bank account number at 3rd party bank to a proxy bank account number in the name of User A at the service provider platform (the platform representing in general the data processing component/transferring module of the invention).
3. The proxy bank account number is generated by the service provider platform to receive and send funds in EUR to and from a blockchain address (user device/e-wallet) on a blockchain network, in this example being the Ethereum main net (i.e. "data store").
4. The payment of 100 EUR received by the proxy bank account number is detected by the service provider platform (transferring module).
5. The service provider platform automatically extracts the financial transfer information of existing payment systems e.g. SEPA associated with the transfer of funds. The information comprises name of receiver, amount, currency and receiver account.
6. The service provider platform obtains information about the user profile (i.e. node data) and automatically performs audit for approval of the transfer of funds.
7. The service provider platform automatically creates a blockchain transaction request (generates a node profile) for a transaction process of minting e-money in the amount of 100 EUR to the User/Participant A's blockchain address on the Ethereum network (datastore).
8. Optionally, the service provider platform may collect/subtract fee from payment, then give go-ahead if security verification is OK.

9. The service provider platform automatically broadcasts the blockchain transaction to the blockchain network.

10. The blockchain network nodes automatically execute the transaction and update the ledger simultaneously to reflect the newly added transactions i.e. automatically mints

e-money in the amount of 100 EUR (minus eventual fee) to User A's blockchain address on the Ethereum mainnet network based on the transaction request (node profile).

11. User A's digital wallet can now read that the balance has been increased by 100 EUR for the blockchain address. User A can also transfer the e-money with the wallet to another blockchain address on the same blockchain network.

Corresponding schemes can be drawn up for the invention when implement for transactions from a blockchain account managed by the service provider of the service platform (the transferring module) to an account of the same or another user in a conventional banking institution, between two conventional accounts, but with a secure transaction through the transaction module.

User-initiated transaction, A to B

1. User A initiates a transaction by logging into service provider platform,
2. User A makes a request for a transfer of 100 EUR from User/Participant A's blockchain address on the Ethereum network (datastore) to a proxy bank account number in the name of User B at the service provider platform (the platform representing in general the data processing component/transferring module of the invention).
3. The service provider platform obtains information about the user profile(s) (i.e. node data) and automatically performs audit for approval of the transfer of funds.
4. The service provider platform automatically creates a blockchain transaction request (generates a node profile) for a transaction process of burning e-money in the amount of 100 EUR from the User/Participant A's blockchain address on the Ethereum network (datastore).
5. The service provider platform automatically broadcasts the blockchain transaction to the blockchain network.

6. The blockchain network nodes automatically execute the transaction and update the ledger simultaneously to reflect the newly added transactions i.e. automatically burns e-money in the amount of 100 EUR from User A's blockchain address on the Ethereum mainnet network based on the transaction request (node profile).

7. User A's digital wallet can now read that the balance has been reduced by 100 EUR for the blockchain address.
8. A proxy bank account number for user B has been generated by the service provider platform to receive and send funds in EUR to and from a blockchain address (user device/e-wallet) on a blockchain network, in this example being the Ethereum main net (i.e. "data store").

9. A payment of 100 EUR is received by the proxy bank account of user B is detected by the service provider platform (transferring module).

10. The service provider platform automatically creates financial transfer information of existing payment systems e.g. SEPA to associate with the transfer of funds. The information comprises name of receiver, amount, currency and receiver account.

10. Optionally, the service provider platform may collect/subtract fee from payment, then give go-ahead if security verification is OK.

11. The service provider platform transfers 100 EUR from the proxy bank account of User B at the service provider platform to a bank account number at 3rd party bank in the of name of user B.

In another specific example of the invention the following exemplified embodiment is set forth:

Creation of User account for airline tickets

1. User A creates a user account with a username and password (UID) for his user account at a service provider platform associated with one or many airlines.

2. The service provider platform (transfer module) generates a user profile for User A.

3. The user entity identified by the system (i.e. his identified device/peripheral or computer) can in this example be viewed as a node. The user profile comprises one or more of name, address and other required regulatory data (this would constitute at least part of node data). A digital wallet holding one or more blockchain addresses associated with a blockchain network (data store) links the addresses to their user profile using private key.

4. The service provider platform generates ticket accounts for the blockchain address each for a respective airline as defined.

Ticket transaction for user A on airline B.

1. User A initiates a transaction by logging into a service provider platform,

2. User A requests an airline ticket for a chosen flight from airline Y, by selecting the airline, flight number and selects a seat on the airplane. Alternatively, the selection process is managed through a booking system, which then forward a ticket order to the service provider platform

3. The service provider platform automatically extracts the airline ticket information from a standardized information provided by associated airlines.

4. The service provider platform obtains information about the passenger from the user profile (i.e. node data) and automatically performs audit for approval of the issuance of an airline ticket.

5. The service provider platform automatically creates a blockchain transaction request (generates a node profile) for a transaction process of issuing an airline ticket for the user on a selected flight of airline Y to the user's blockchain address on a blockchain network (datastore).

6. The service provider platform automatically broadcasts the blockchain transaction to the associated blockchain network.

7. The blockchain network nodes automatically execute the transaction and update the ledger simultaneously to reflect the newly added transactions i.e. issues an airline ticket for the requestd flight to User A's blockchain address on the associated blockchain network based on the transaction request (node profile).

11. User A's digital wallet can now read that a new airline ticket has beein issued for the blockchain address.

User A can also transfer the airline ticket from the wallet back to the service provider platform if he needs to change or cancel his travel, if allowed by the airline. If the ticket is transferred to the service provider platform a certain time in advance to the flight, the airline can receive back the actual digital ticket. If a return of ticket is approved by the airline the blockchain network nodes automatically execute the transaction and update the ledger simultaneously to reflect the new transactions i.e. return transmisson/cancellation of the ticket, from User A's blockchain address on the associated blockchain network based on the transaction request (node profile).

It is noted that not all the drawings carry all the reference signs. Instead, in some of the drawings, some of the reference signs have been omitted for sake of brevity and simplicity of illustration.

Reference numbers and letters appearing between parentheses in the claims, identifying features described in the embodiments and illustrated in the accompanying drawings, are provided as an aid to the reader as an exemplification of the matter claimed. The inclusion of such reference numbers and letters is not to be interpreted as placing any limitations on the scope of the claims.

The term "at least one of first option and a second option" is intended to mean the first option or the second option or the first option and the second option.

Whenever a relative term, such as "about", "substantially" or "approximately" is used in this specification, such a term should also be construed to also include the exact term. That is, e.g., "substantially straight" should be construed to also include "(exactly) straight".

Whenever steps were recited in the above or also in the appended claims, it should be noted that the order in which the steps are recited in this text may be accidental. That is, unless otherwise specified or unless clear to the skilled person, the order in which steps are recited may be accidental. That is, when the present document states, e.g., that a method comprises steps (A) and (B), this does not necessarily mean that step (A) precedes step (B), but it is also possible that step (A) is performed (at least partly) simultaneously with step (B) or that step (B) precedes step (A). Furthermore, when a step (X) is said to precede another step (Z), this does not imply that there is no step between steps (X) and (Z). That is, step (X) preceding step (Z) encompasses the situation that step (X) is performed directly before step (Z), but also the situation that (X) is performed before one or more steps (Y1), …, followed by step (Z). Corresponding considerations apply when terms like "after" or "before" are used.

Claims

1. A system, wherein the system comprises:
   i. at least one node, configured to provide node data;
   ii. a data processing component, wherein the data processing component is configured to automatically generate a node profile based on at least said node data, wherein the node profile comprises at least one unique identifier (UID) associated with the node; and
   iii. at least one transferring module configured to initiate a transaction process based on the node profile.

2. The system according to claim 1 wherein the system is configured to authorise the at least one node to participate in a transaction process.

3. The system according to any of the preceding claims, wherein the transaction process comprises the access to and/or controlling of an entity, such as a physical entity.

4. The system according to any of claims wherein the transferring module is configured to generate transaction data associated with each UID.

5. The system according to any of the preceding claims wherein the transferring module is further configured to associate at least one balance value to the at least one node profile.

6. The system according to any of the preceding claims wherein the system comprises at least one transaction protocol and is configured to associate the at least one transaction protocol to the node profile.

7. The system according to claim 6 wherein the transferring module is configured to associate the at least one transaction protocol to the node profile.

8. The system according to any of the preceding claims wherein the system further comprises at least one and/or a plurality of datastore(s), wherein the datastore comprises blockchain-based distributed computing platform.

9. The system according to any of the preceding claims wherein the system comprises a master account, wherein the system is further configured to facilitate data exchange between the data processing component and the master account.

10. The system according to any of the preceding claims wherein the transferring module is configured to associate the at least one node with at least one user device.

11. The system according to any of the preceding claims wherein the transferring module is configured to enable the at least one transaction process from a financial entity to the node profile.

12. The system according to any of the preceding claims wherein the transferring module is configured to enable the at least one transaction process from a financial entity to at least one proxy bank account and/or at least one node account.

13. The system according to any of the preceding claims wherein the system comprises an e-money generator, wherein the e-money generator is configured to associate a positive value to the respective UID.

14. A computer-implemented method, comprising the steps of:

i. authorizing at least one node to participate in a transaction process; and
ii. enabling the transaction process between at least two participants using at least one transferring module.

15. The method according to the preceding claim wherein the transaction process comprises access to and/or control of an entity, such as a physical entity.

16. The method according to the preceding claim wherein the participant comprises at least one of node profile and UID and datastore and transaction protocol and financial entity and proxy bank account and user device and master account.

17. The method according to claim 14 or 15, comprising automatically generating a node profile based on at least a portion of node data provided by or associated with said note.

18. The method according to claim 17, wherein the method comprises enabling the transaction process from the at least one node to the at least one financial entity.

19. The method according to any of the preceding two claims wherein the method comprises enabling the transaction process from the node to the at least one node profile stored in a datastore.

20. The method according to any of the preceding seven claims wherein the method comprises enabling the transaction process from the node to the at least one transaction protocol stored on the at least one transferring module.

21. The method according to any of the preceding eight claims wherein the method comprises enabling the at least one transaction process from the financial entity to the node profile.

22. The method according to any of the preceding seven claims wherein the method comprises enabling the at least one transaction process from the financial entity to the proxy bank account.

23. The method according to any of the preceding eight claims wherein the method comprises automatically detecting a balance value associated in the transaction process.

24. The method according to any of the preceding nine claims wherein the method comprises transferring the balance value from the proxy bank account to a master account.

25. The method according to any of the preceding two claims wherein the method comprises automatically associating the balance value based on the transaction process to the respective UID.

26. The method according to any of the preceding ten claims wherein the method comprises automatically enabling the at least one transaction process from the at least one transaction protocol to the at least one datastore.

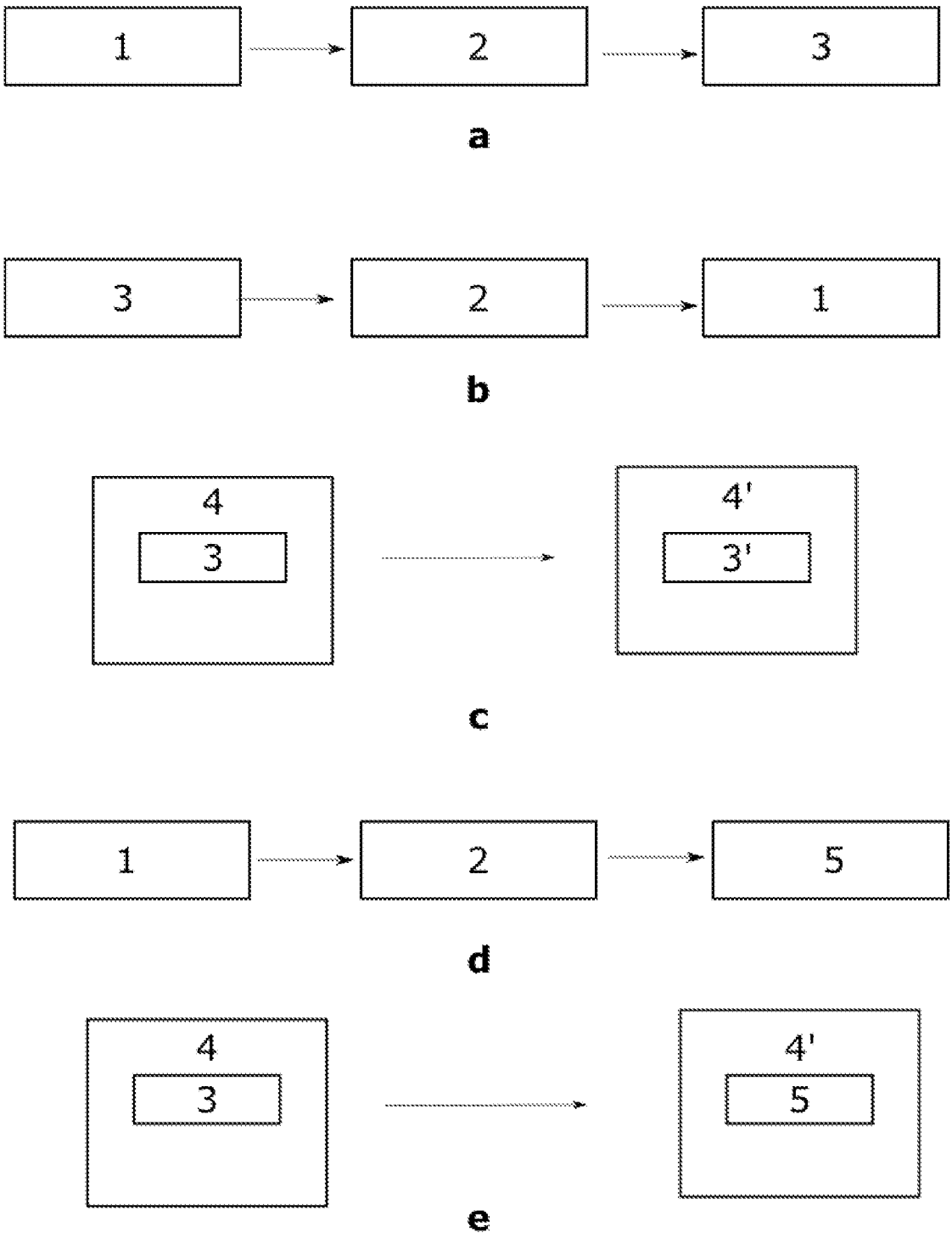


Fig. 1

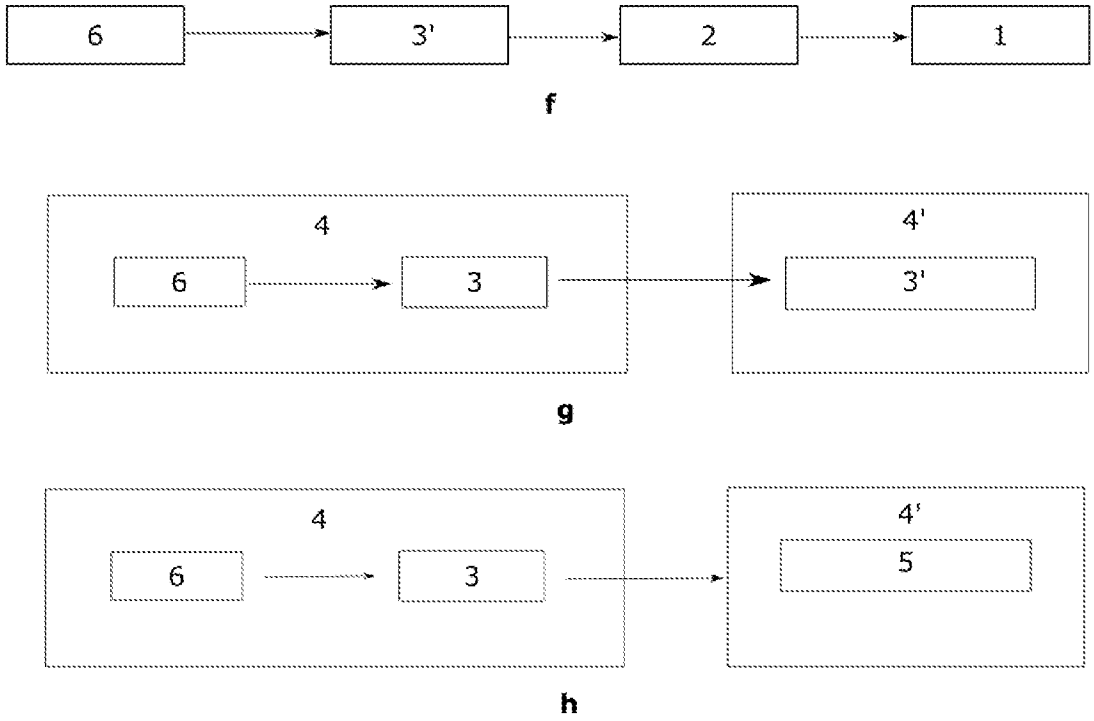


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/IS2021/050009

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/06 G06Q20/36
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/143469 A1 (STEWART STEVE [US] ET AL) 7 May 2020 (2020-05-07) abstract; figures paragraphs [0162] - [0198]	1-26

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 September 2021	01/10/2021

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Breugelmans, Jan

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IS2021/050009

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020143469 A1	07-05-2020	NONE	