US 20160283941A1

(19) **United States**

(12) **Patent Application Publication**

Andrade

(10) **Pub. No.: US 2016/0283941 A1**

(43) **Pub. Date: Sep. 29, 2016**

(54) **SYSTEMS AND METHODS FOR PERSONAL IDENTIFICATION AND VERIFICATION**

(71) Applicant: **BLACK GOLD COIN, INC.**, Las Vegas, NV (US)

(72) Inventor: **Marcus Andrade**, Fernley, NV (US)

(21) Appl. No.: **14/940,142**

(22) Filed: **Nov. 12, 2015**

(30) **Foreign Application Priority Data**

Mar. 27, 2015 (EP) 15161502

Publication Classification

(51) **Int. Cl.**

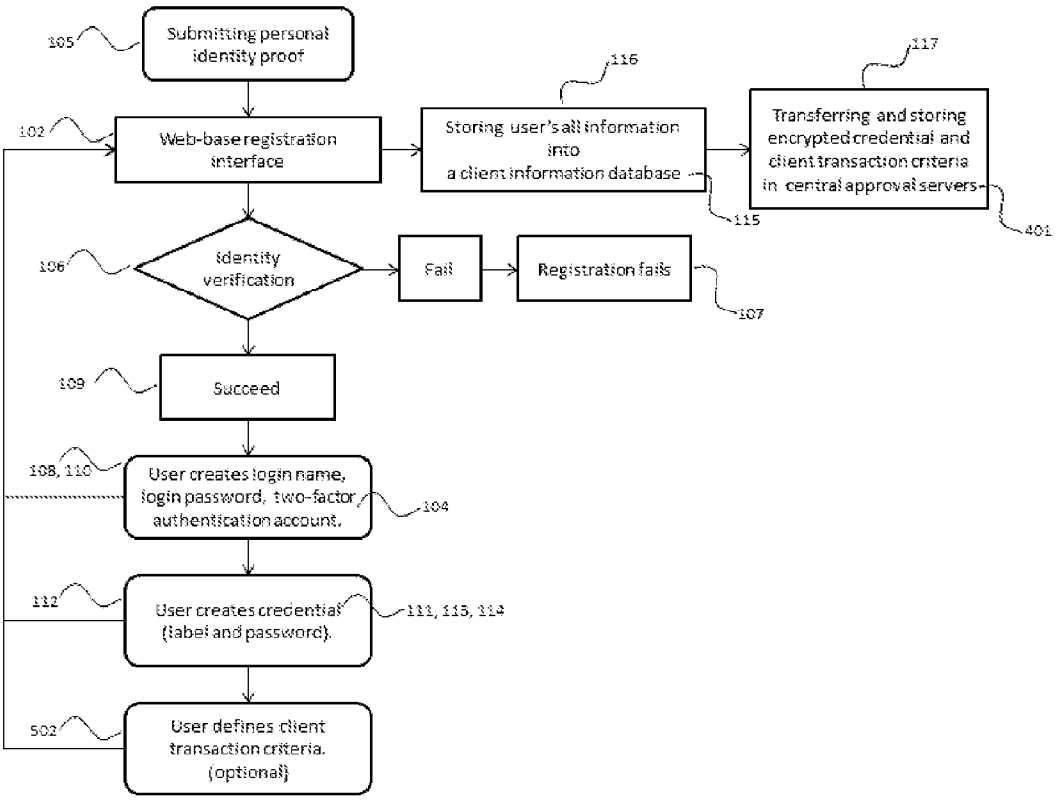
G06Q 20/40	(2006.01)
G06Q 20/36	(2006.01)
H04L 9/06	(2006.01)
G06Q 20/38	(2006.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/4014*** (2013.01); ***G06Q 20/405*** (2013.01); ***G06Q 20/3829*** (2013.01); ***G06Q 20/36*** (2013.01); ***H04L 9/0643*** (2013.01); *G06Q 2220/00* (2013.01)

(57) **ABSTRACT**

A personal/client identification and verification process, pseudonymous system and transaction network for monitoring and restricting transactions of cryptography-based electronic money. The present invention—"legal identity-linked credential authentication protocol" is a protocol providing a practical solution for the issues related to cryptocurrency theft, KYC and AML, while maintaining user privacy.



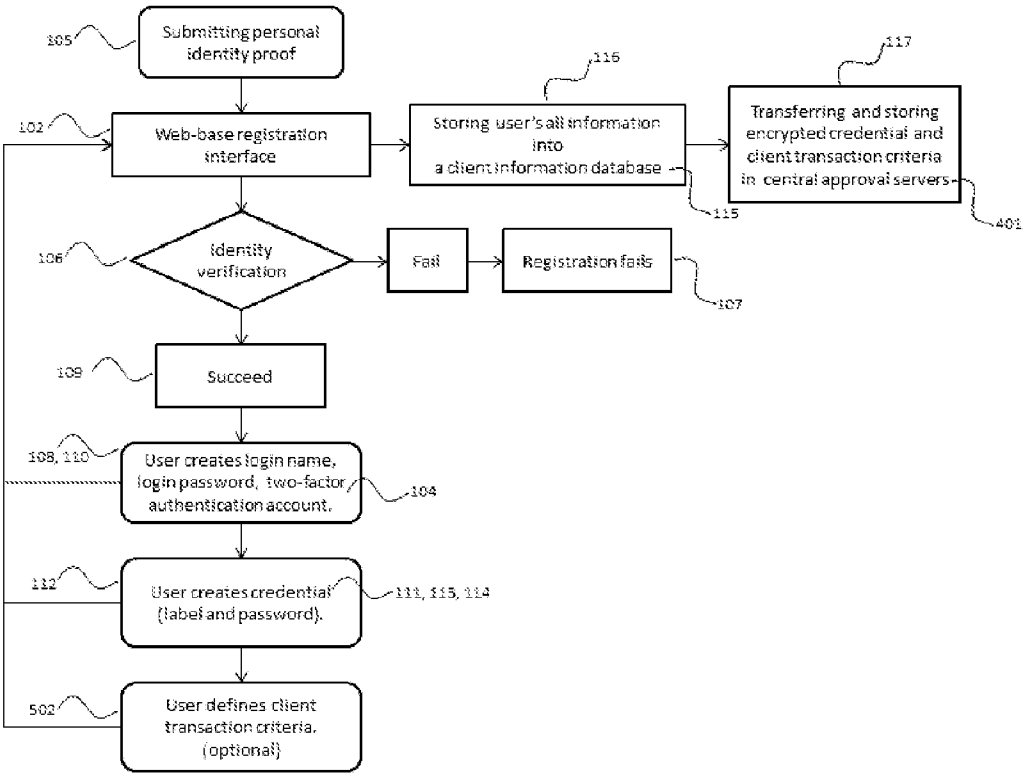

105
Submitting personal identity proof
102
Web-base registration interface
116
Storing user's all information into a client information database
117
Transferring and storing encrypted credential and client transaction criteria in central approval servers
115
401
106
Identity verification
Fail
Registration fails
107
109
Succeed
108, 110
User creates login name, login password, two-factor authentication account.
104
112
User creates credential (label and password).
111, 115, 114
502
User defines client transaction criteria. (optional)

Fig. 1

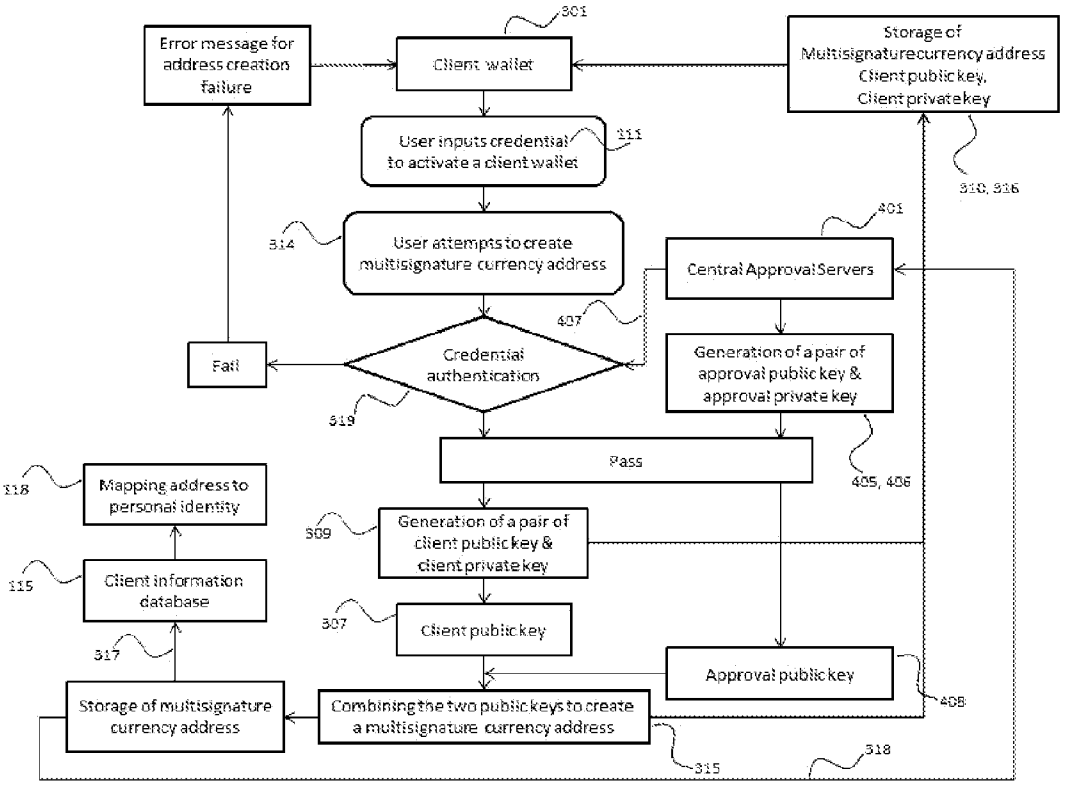

Error message for address creation failure
Client wallet
301
Storage of Multisignaturecurrency address Client public key, Client private key
User inputs credential to activate a client wallet
311
310, 316
User attempts to create multisignature currency address
314
401
Central Approval Servers
407
Fail
Credential authentication
319
Generation of a pair of approval public key & approval private key
Pass
405, 406
Mapping address to personal identity
318
Generation of a pair of client public key & client private key
309
Client information database
115
Client public key
307
Approval public key
317
408
Storage of multisignature currency address
Combining the two public keys to create a multisignature currency address
315
318

Fig. 2

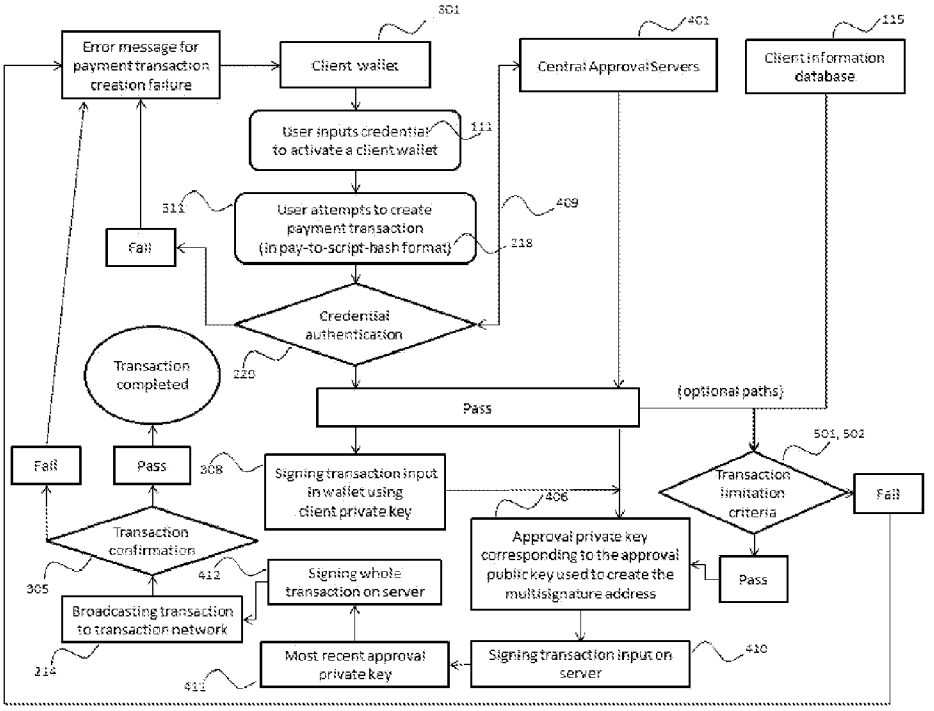

Error message for payment transaction creation failure
Client wallet
Central Approval Servers
Client information database
User inputs credential to activate a client wallet
User attempts to create payment transaction (in pay-to-script-hash format)
Fail
Credential authentication
Transaction completed
Pass
(optional paths)
Fail
Pass
Signing transaction input in wallet using client private key
Transaction limitation criteria
Fail
Transaction confirmation
Approval private key corresponding to the approval public key used to create the multisignature address
Pass
Signing whole transaction on server
Broadcasting transaction to transaction network
Most recent approval private key
Signing transaction input on server
401
115
111
311
409
218
220
501, 502
308
406
305
412
214
411
410

Fig. 3

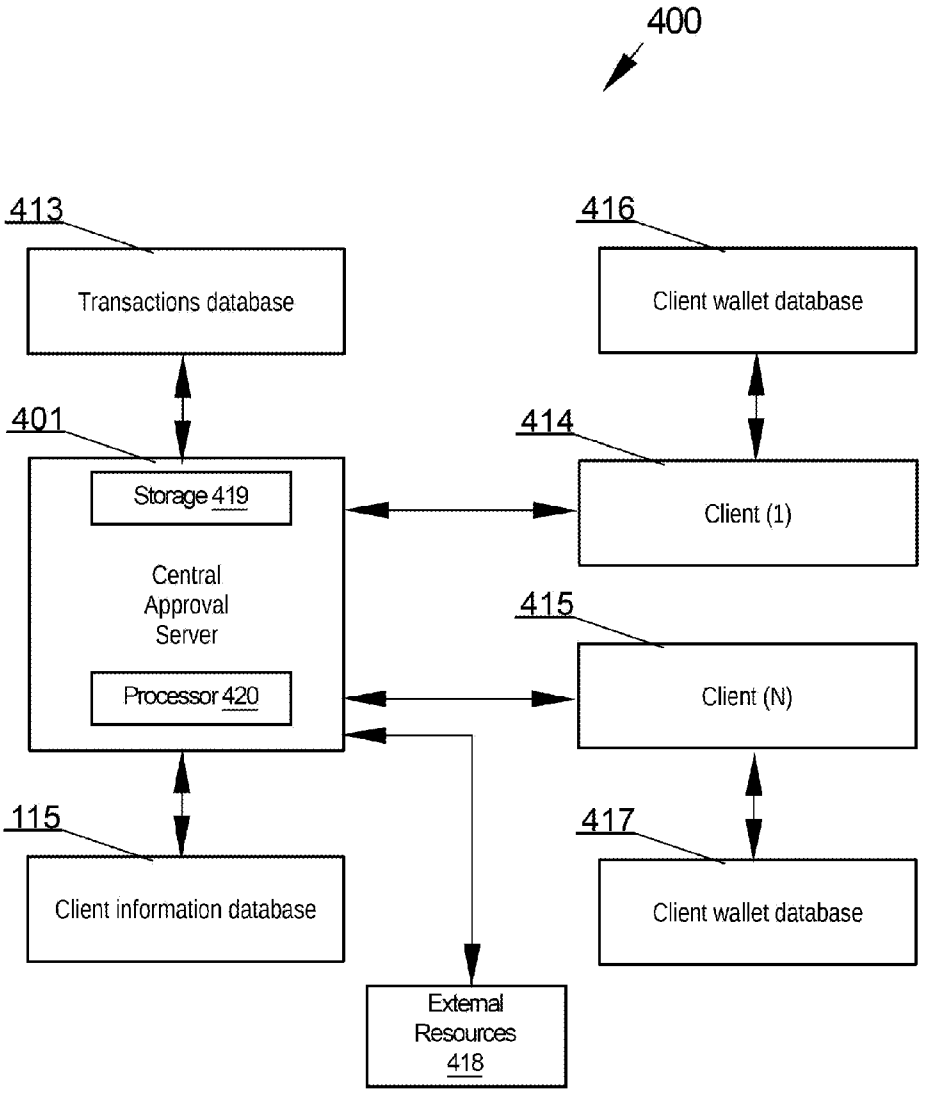

400
413
Transactions database
416
Client wallet database
401
414
Storage 419
Client (1)
Central
Approval
Server
415
Processor 420
Client (N)
115
417
Client information database
Client wallet database
External
Resources
418

Fig. 4

SYSTEMS AND METHODS FOR PERSONAL IDENTIFICATION AND VERIFICATION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the priority benefit of European Patent Application No. EP15161502.8 filed on Mar. 27, 2015 and entitled "A System And A Method For Personal Identification And Verification," which is incorporated herein by reference.

FIELD OF THE DISCLOSURE

[0002] The present invention relates to a system and method for personal identification and verification. In particular the present invention relates to personal/client identification and verification process, pseudonymous system and transaction network for monitoring and restricting transactions of cryptography-based electronic money—legal identity-linked credential authentication protocol.

BACKGROUND

[0003] Prior art defines digital currency or digital money. It is an internet based medium of exchange (i.e., distinct from physical, such as banknotes and coins) that exhibits properties similar to physical currencies, however, allows for instantaneous transactions and borderless transfer-of-ownership.

[0004] Both virtual currencies and cryptocurrencies are types of digital currencies, but the converse is incorrect. Like traditional money these currencies may be used to buy physical goods and services. Digital currencies such as bitcoin are known as "decentralized digital currencies," meaning that there is no central point of control over the money supply. (see Wikipedia)

[0005] Bitcoin is the first cryptographic-based electronic money, which was invented in 2008. It is also referred as the first cryptocurrency. Bitcoin is not only virtual money, but also a payment system composed of a decentralized peer-to-peer transaction network for recording and verifying the money transactions.

[0006] Bitcoins (i.e., units of Bitcoin) are not stored in individual owners' client wallets, but their ownerships are recorded in a public ledger of all Bitcoin transactions, i.e., blockchain, by using Bitcoin addresses of the owners. A Bitcoin address is a 160-bit hash of the public portion of a public/private Elliptic Curve Digital Signature Algorithm (ECDSA) key pair. The private key for each Bitcoin address is stored in the client wallet of the address owner.

[0007] Moreover, all client wallets are connected with each other through the Internet and form nodes of a transaction network to relay and verify the transactions. Using public/private-key cryptography, one can "sign" (i.e., use his/her private key) to send an amount of bitcoins recorded at his/her Bitcoin address to another Bitcoin address, and in the transaction network anyone who knows his/her public key can verify whether the signature is valid.

[0008] Since the appearance of Bitcoin, there have been different cryptographic-based electronic currencies being created and collectively called alternative cryptocurrencies. Among them, some are modified forms of Bitcoin using different cryptographic hash algorithms (e.g., Litecoin) and/or having additional functions (e.g., CinniCoin), while some are created using different signature technologies (e.g., CryptoNote).

[0009] By design, Bitcoin is pseudonymous, while all alternative cryptocurrencies are either pseudonymous or anonymous. For anonymous cryptocurrency, it can be easily applied to money laundering activities because all senders and receivers in money transactions are not traceable. For pseudonymous cryptocurrency, an academic study (Meiklejohn S, et al. University of California, San Diego, 2013) showed that evidence of interactions between institutes could be identified by analyzing the pattern of involvements of Bitcoin addresses in empirical purchasing of goods and services.

[0010] This approach may be able to identify illegal activities at institution level, but still not able to narrow down to a single person level. A recent academic study (Koshy P, et al. Pennsylvania State University, 2014) has shown that it is possible to map a Bitcoin address to an IP address. However, this approach is only applicable to less than 10% of the Bitcoin addresses. Therefore, it is generally believed that Bitcoin and other alternative cryptocurrencies can be used for illegal activities such as money laundering (Bryans D, Indiana Law Journal, 89 (1):441, 2014).

[0011] The pseudonymous/anonymous property also makes Bitcoin and alternative cryptocurrencies become attractive targets for hackers and thieves. For example, in February 2014, the Mt. Gox company, which was the world largest bitcoin exchange company at that time, was filed for bankruptcy protection because the company was being hacked continuously, resulting in loss of 850,000 bitcoins (worth about US$480 million).

[0012] In January 2015, the Slovenian Bitcoin exchange Bitstamp, which was the world's third largest bitcoin exchange at that time, was hacked, and less than 19,000 BTC (worth about US$5 million) was stolen. Although the hackers/thieves must transfer the stolen bitcoins to their Bitcoin addresses, the identities of most of these hackers and thieves remain unknown.

[0013] Therefore, there are needed Anti-Theft Solutions for Bitcoin. The ownerships of bitcoins are being protected by private keys, which are stored in users' wallet. Private keys can be created from a passphrase. For example, Brainwallet is a website that provides a tool to generate a Bitcoin address and its private key from the sha256 of a passphrase. Using a password dictionary, one could analyze the Bitcoin blockchain and search for active Bitcoin addresses created from typical passwords, and steal the bitcoins from these addresses using the corresponding private keys.

[0014] One simple anti-theft solution is to avoid using Bitcoin addresses generated from typical passphrases. For other Bitcoin addresses, hackers can hack the computers or servers of Bitcoin owners to look for files containing the private key records. Once these files are discovered, bitcoins stored at the corresponding addresses can be easily transferred to another address. The simple solution for this is to keep such files in a cold storage (i.e., a device which is not connected to the Internet), or even not to create such files.

[0015] Another way to steal bitcoins is to steal the main wallet data file (i.e., wallet.dat file) in a Bitcoin wallet, which is installed in a computer or server connected to the Internet. Robert Lipovsky (2013) reported an online banking trojan that can steal the wallet.dat files. Private keys are stored in the wallet.dat files and are protected with passphrases. Once the main wallet data file is stolen, the protection passphrase can be cracked by dictionary-based guessing, permutations of dictionary words or pure brute force.

[0016] One example of solutions for such stolen Bitcoin wallets is presented in a patent application publication of CN103927656 (A) entitled "Bitcoin terminal wallet with embedded, fixed collecting address and Bitcoin payment method of Bitcoin terminal wallet".

[0017] One simple solution, to the above, is to store bitcoins at a multisignature address that require two private keys for spending the bitcoins. One private key is stored in computing device (e.g. local computer), while another key is stored in a separate computing device (e.g. smart phone, remote server), creating two-factor authentication for transactions. Such solution is not yet available until the present invention.

[0018] Another solution is to make all Bitcoin senders and receivers identifiable. The legal identities of the thefts or hackers can then be uncovered from revealing the legal identities of owners of the Bitcoin addresses receiving the stolen bitcoins. Such solution is not yet available until the present invention.

[0019] Currently Anti-Money Laundering (AML) solutions for Bitcoin are highly demandable. For bitcoin service providing companies to meet U.S. (FinCEN) and worldwide regulations in AML, the current approach is a combined use of know-your-customer (KYC) and transaction monitoring. To make this possible, all traders/customers must provide their legal identities and subjected to verification. However, this approach suffers from two major problems. First, this approach is mainly adopted by companies providing legitimate services. Therefore, AML activities involving bitcoins can still happen worldwide. Second, companies usually have their own customer registration and identity verification systems.

[0020] This not only leads to redundancy in resources and high business running cost, but also creates annoyance for bitcoin users. Being an honest bitcoin user, one may need to repeatedly provide identity documents to different bitcoin service providing companies for identity verification before using their services.

[0021] On 25 Feb. 2015, Bank of England launched its One Bank Research Agenda—an ambitious and wide-ranging framework to transform the way research is done at the Bank. According to this discussion paper, Bank of England is investigating whether central banks should themselves make use of the Bitcoin's blockchain technology to issue their own digital currencies. Bank of England has stated that issues related to KYC and AML have to be addressed, and should investigate how digital identity management could be achieved while balancing privacy considerations.

[0022] Taking into account the foregoing, it would be advantageous to design a personal/client identification and verification process, pseudonymous system and transaction network for monitoring and restricting transactions of cryptography-based electronic money, that would obviate at least some of the aforementioned disadvantages.

[0023] The present invention—"legal identity-linked credential authentication protocol" is the first protocol providing a practical solution for the issues related to cryptocurrency theft, KYC and AML, while maintaining user privacy.

[0024] Last but not least, the present invention can be adopted or modified by the central banks or other financial institutions, in order to issue their own digital currencies that are supported by a ledger payment system, but also regulated by a central governing body. The ledger can be private or open to the public. Such digital currencies can hence inherit advantages of the existing banking system and advantages of cryptography-based electronic money.

SUMMARY

[0025] The invention presented herein can be summarized by the following clauses.

[0026] 1. A method for personal/client identification and verification for transactions involving cryptography-based electronic money, the method being executed by a computational server (**101**) comprising at least one computer program functioning as a registration interface (**102**), and the method being characterized in that it comprises the steps of:

[0027] providing access to one or more potential or existing currency users (**103**);

[0028] providing a registration interface (**102**) for one or more potential currency users to register a user account requiring authentication (**104**);

[0029] requesting the submission of documents for proof of legal identity of a registrant (**105**);

[0030] verifying the legal identity of the registrant (**106**);

[0031] rejecting an account creation for registrants failing in legal identity verification (**107**);

[0032] creating a personal/client account (**108**) for individual successful registrants (**109**) with successful verification of legal identity (**110**);

[0033] allowing a successful registrant (**109**) to create a credential (**111**) that comprises an associated authentication (**112**);

[0034] storing (**116**) all the submitted information in a client information database (**115**);

[0035] sending (**117**) the credential to central approval servers (**401**); and

[0036] mapping and storing (**118**) multisignature currency address(es), credential and legal identity of individual registrants.

[0037] 2. The method according to clause 1 characterized in that the authentication for accessing a personal/client account is effected by means of a password protection, two factor authentication or multiple factor authentication.

[0038] 3. The method according to clause 1 characterized in that it further comprises a step of encrypting the credentials (**114**).

[0039] 4. The method according to clause 1 characterized in that the credential is a digital, electronic or hardware item which can be used as an authentication mechanism to identify oneself. For example, it can be a unique pair of digital codes (e.g., name and password); it can be a unique product key for activing a client wallet software; and it can be a constantly changing token (e.g. a unique 7-digit code) which is tied to a physical device that is owned by the user, such as a cellphone or a personalized secure key generating device.

[0040] 5. A method for creating a cryptography-based electronic money (CBEM) (**201**) and its associated transaction network (**202**), the method being executed by a network of computer programs functioning as nodes, and the method being characterized in that it comprises the steps of:

[0041] installing a node (**203**), which can be a stand-alone computer program or a functional module of a client wallet (**111**), in one or more client computers and/or servers (**204**);

[0042] connecting all nodes to form relay nodes (**205**) of a peer-to-peer network through a data transmission network (**206**);

[0043] controlling the method for creating at least one unit of the CBEM (**207**); protecting the ownerships of at least one unit of the CBEM by public/private-key cryptography (**208**);

[0044] recording ownerships of at least one unit of the CBEM into a ledger of all transactions (e.g. block-chain) (**209**) using the owners' currency addresses (**313**) (**210**);

[0045] verifying ownerships of at least one unit of the CBEM (**211**);

[0046] restricting only valid registered users (**109**) to generate one or more valid currency addresses (**313**) to receive at least one unit of the CBEM by verifying the submitted credential (**111**) with one of the central approval servers (**401**) (**212**);

[0047] recording transactions of at least one unit of the CBEM into the ledger (**209**) (**213**);

[0048] verifying transactions of at least one unit of the CBEM (**214**);

[0049] controlling the method for transacting at least one unit of the CBEM (**215**);

[0050] incorporating the transaction rules into the programing code of at least one nodes (**216**);

[0051] restricting at least one transaction approval rule (**217**), comprising at least one of: requisition of a valid credential (**111**) from the sender, requisition of one or more approval private keys (**406**) from one of the central approval servers (**401**);

[0052] allowing only creation of multisignature transactions in pay-to-script-hash format or any other compatible format (**218**);

[0053] allowing only creation of multisignature transactions each requiring at least two private keys as signatures (**219**);

[0054] allowing only creation of multisignature transactions in the presence of a valid credential (**111**) (**220**);

[0055] restricting one of these private keys (**219**) to be an approval private key (**406**) from one of the central approval servers (**221**);

[0056] restricting the rest of the private keys (**219**) to be client private keys (**222**), which are encrypted and stored in the client wallet(s) (**301**) (**223**);

[0057] sending all transaction requests from the client wallets (**301**) to one of the central approval servers (**401**) to obtain the approval private key for signing the transactions (**224**); and

[0058] rejecting all transactions missing any one of the required private keys (**219**); (**225**).

[0059] 6. A method for personal/client identification and verification for transactions involving cryptography-based electronic money, the method being executed by a computer program functioning as a client device of a user, and the method being characterized in that it comprises the steps of:

[0060] installing a computer program of a client device to function as a client wallet (**301**) in at least one computer or computational server (**302**);

[0061] serving as one of the relay nodes (**205**) for relaying information of all CBEM units (e.g., coins) being generated in the transaction network (**202**) (**303**); serving as one of the relay nodes (**205**) for relaying all transaction information in the transaction network (**202**) (**304**);

[0062] serving as one of the relay nodes to verify and confirm all transactions that are broadcasted to the transaction network (**202**) (**305**);

[0063] generating new coins through contributing to recording any new transaction information into the ledger of all transactions (e.g. the blockchain) (**209**) (**306**);

[0064] generating one or more pairs of cryptographic client public key (**307**) and client private key (**308**) for receiving and sending coins (**309**);

[0065] storing the client public-private key pairs (items **307**, **308**) of one or more currency addresses generated by the currency users (**310**);

[0066] serving as a client wallet for the currency users to receive and send coins; (**311**);

[0067] serving as an client wallet to communicate between one of the central approval servers (**401**) and registered currency users (**109**) (**312**);

[0068] only generating (**314**) currency addresses which are multisignature addresses (**313**);

[0069] generating one of more multisignature addresses (**313**) from the client public key (**307**) and the approval public key (**405**) (**315**);

[0070] only storing one or more multisignature addresses (**313**) in the client wallet (**301**) for sending and receiving coins (**316**);

[0071] sending one of more multisignature addresses (**313**) to the client information database (**401**) for storage and mapping to legal identity of the owner of the address(es) (**317**);

[0072] sending the generated valid multisignature addresses (**313**) to the central approval servers (**401**) for storage (**318**);

[0073] submitting a credential (**111**) of a valid registered users (**109**) to one of the central approval servers for obtaining approval to generate one or more valid currency multisignature addresses (**313**) (**319**);

[0074] submitting a credential (**111**) of a valid registered users (**109**) to one of the central approval servers for obtaining approval to create one or more valid transactions (items **218**, **219**, **220**, **221**, **223**) to send coins to one or more currency addresses (**320**);

[0075] allowing only creation of transactions that use multisignature addresses (**313**) for both sending and receiving the coins (**321**); and

[0076] recording unspent coins (if there is any) into the blockchain at the currency address from where the coins have just been sent (**322**).

[0077] 7. A method for personal/client identification and verification for transactions involving cryptography-based electronic money, the method being executed by a computer program in a computational server functioning as a central approval server (**401**), and the method being characterized in that it comprises the steps of:

[0078] communicating (**407**) with a client wallet (**301**) to generate one or more valid multisignature currency addresses (**313**) in the presence of a valid credential;

[0079] providing (**408**) approval public key (**405**) to the currency wallet to create one or more multisignature addresses (**313**),

[0080] communicating (**409**) with the client wallet (**301**) to generate one or more valid transactions (**218**, **219**, **220**, **221**, **223**) to send coins to one or more currency address in the presence of a valid credential;

[0081] providing (**410**) approval private key (**406**), which are corresponding to the approval public key (**405**) used in creation of the multisignature address (**313**), to sign transaction input for one or more valid transactions (**218**, **219**, **220**, **221**, **223**);

[0082] providing the most recent private key (**411**) to sign the whole transaction for one or more valid transactions (**412**); and

[0083] storing (**414**) transaction information in a transactions database (**413**).

[0084] 8. The method according to clause 7, characterized in that the most recent approval private key (**411**) is the approval private key corresponding to the approval public key (**405**) used in creation of the multisignature address (**313**) or another approval private key.

[0085] 9. The method according to clause 7 characterized in that the step of storing (**414**) transaction information in a transactions database (**413**) includes storing a transaction ID, sender's currency address, receiver's currency address, amount of coins being transacted, transaction time and IP addresses of the sender and the receiver's client wallets.

[0086] 10. The method according to clause 7, characterized in that the method further comprises a step of verifying the transaction against one or more transaction criteria (**501**, **502**) at the central approval server (**401**).

[0087] 11. The method according to clause 7, characterized in that the one or more transaction criteria (**501**, **502**) include criteria predefined by a central governing body (**601**) and/or the registrant.

[0088] 12. The method according to clause 7, characterized in that the method further comprises a step of tracing legal identities of the sender and receiver by mapping their currency addresses in the transaction database and the client information database when needed.

[0089] 13. A method for personal/client identification and verification for transactions involving cryptography-based electronic money, the method being executed by a set of computer programs functioning as devices of a central governing body and a client device of a user, the method being characterized in that it comprises the steps of:

[0090] receiving credentials, of a registrant, comprising at least two factor authentication credentials defining a multisignature;

[0091] verifying legal identity of the registrant;

[0092] creating a personal/client account (**108**) for an individual successful registrant (**109**) with successful verification of legal identity (**110**) whereas the personal/client account facilitates mapping and storing the multisignature of a currency address and legal identity of individual registrants (**118**);

[0093] providing a registrant wallet comprising at least one unit of electronic money;

[0094] recording ownerships of the at least one unit of electronic money into a transactions database (**413**) using the registrants' currency address (**313**);

[0095] creating a multisignature transaction, in a pay-to-script-hash format or any other compatible format (**218**), each requiring at least two private keys as approval signatures (**219**);

[0096] restricting one of these private keys (**219**) to be an approval private key (**406**) from one of central approval servers (**221**);

[0097] restricting the rest of the private keys (**219**) to be the registrant's private keys (**222**), which are stored in the client wallet (**301**, **223**);

[0098] sending the transaction request from the client wallet (**301**) to at least one of the central approval servers (**401**) in order to obtain the approval private key for signing the transaction (**224**); and

[0099] broadcasting the approved transaction messages to all relay nodes in a transaction network (**214**).

[0100] 14. A system for personal/client identification and verification for transactions involving cryptography-based electronic money, the system comprising:

[0101] a central approval server (**401**) configured to execute the method according to clause 7 in order to process client registration requests, client cryptocurrency addresses, cryptocurrency transactions;

[0102] a client information database (**404**) communicatively coupled to the central approval server (**401**);

[0103] transactions database (**413**) communicatively coupled to the central approval server (**401**);

[0104] at least one client device (**414**, **415**) provided with a registrant wallet (**416**, **417**) comprising at least one unit of electronic money;

[0105] wherein the at least one client device (**414**, **415**) is configured to execute the method according to clause 13.

[0106] 15. A computer program comprising program code means for performing all the steps of the computer-implemented method according to clause 1, clause 5, clause 6, clause 7 and clause 13 when said program is run on a computer or computational server.

[0107] 16. A computer readable medium storing computer-executable instructions performing all the steps of the computer-implemented method according to clause 1, clause 5, clause 6, clause 7 and clause 13 when executed on a computer or computational server.

[0108] 17. The method of Clause 7, wherein the pair of approval public Key (**405**) and approval private key (**406**) can be changed manually or automatically in a regular period to avoid leakage of the approval public key and the approval private key to the public. After changing to a new pair of approval key, the old approval private key will be used for signing the transaction input (**410**), and the new approval private key will used for signing the whole transaction (i.e., all transaction's data) (**412**).

[0109] 18. The methods of clause 5, clause 6 and clause 7, wherein any currency addresses that are not generated through the submission of a valid credential to one of the central approval servers (**401**) are not valid, and are not able to receive any coins.

[0110] 19. The method of clause 10, wherein the transaction network (**202**) can be modified to reject any transactions that do not the meet the central transaction cri-

teria (**501**) or client transaction criteria (**502**) stored in one of the central approval servers (**401**).

[0111] 20. The method of clause 19, wherein the client transaction criteria (**502**) can be defined by a valid registered user to limit his/her own transactions.

[0112] 21. The method of clause 19, wherein the transaction criteria (**501**) can be defined by a central governing body (**601**) to stop suspicious transactions that is likely to be involved in illegal activities, such as money laundering.

[0113] 22. The method of clause 5, wherein individual transactions can be monitored with a defined rules to identify, record and report suspicious transactions that is likely to be involved in illegal activities, such as money laundering.

[0114] 23. The method of clause 5, wherein legal identities of owners of individual currency addresses are stored in the client information database. For those transactions suspected of illegal activities (clause 22), identities of their associated senders and receivers will be extracted from the client information database by tracing with the currency addresses of the senders and receivers. Subsequently, the suspicious activities and the associated client information will be reported to government agencies with respect to the regulations and laws in the associated countries.

[0115] 24. The methods of clause 1 and clause 5, wherein legal identities of owners for individual currency addresses are stored in the client information database. This fulfills the "know-your-customer" regulatory requirement. This allows the system to be used as a payment system for commercial activities.

[0116] 25. The methods of clause 1 and clause 5, wherein legal identities of owners for individual currency addresses are stored in the client information database. However, such information is not accessible to the public, in order to maintain the pseudonymous property of the cryptography-based electronic money (**201**) and its transaction network (**202**).

[0117] 26. The methods of clause 1 and clause 5, wherein a user can change his/her credential (**111**) to stop coins being transferred out from a stolen main data file (e.g., wallet.dat file) of his/her currency wallet (**301**).

[0118] 27. The methods of clause 1, clause 5, clause 6 and clause 12, wherein (i) legal identities of owners for individual currency addresses are stored in the client information database, (ii) any currency addresses that are not generated through the submission of a valid credential to one of the central approval servers (**401**) are not valid, and are not able to receive any coins (clause 18), and (iii) only valid registered users have a valid credential (**112**). When coins are stolen from someone, the theft(s) or the hacker(s) can be easily traced by retrieving legal identity(s) of the receiver(s) from the client information database according to the currency address(es) of the receiver(s). Therefore, the implementation of the methods of clause 1, clause 6 and clause 7 prevents a cryptocurrency from being stolen.

[0119] 28. The methods of clause 5, clause 6 and clause 12, wherein the amount of coins own by a valid registered user are completely and easily traceable and trackable by the central governing body (**601**) through analyzing the transaction records in the transactions database (**413**). Besides the capability of linking individual currency addresses to their owners, this unique property is contributed by recording unspent coins (if there is any) at the currency address from where the coins have just been sent/spent (**322**). This unique property allows applications of our system to financial and banking activities, particularly those required third-party auditing.

[0120] 29. The methods of Clause 20 and Clause 21, wherein, provide a practical solution for the issues related to cryptocurrency theft, KYC and AML, while maintaining user privacy.

[0121] 30. The systems of Clause 20 and Clause 21, wherein, can be adopted or modified by the central banks or other financial institutions to issue their own digital currencies that are supported by a distributed ledger payment system, but also regulated by a central governing body.

[0122] Further, there is disclosed a method involving a system for creating a new cryptography-based electronic money or cryptocurrency with the traceable legal identities of senders and receivers in all money transaction. The method may be performed in a system comprising:

[0123] 1. At least one server and at least one web-based registration interface, wherein the at least one server performs at least some, or all, of the following functions:

[0124] Providing access to one or more potential or existing currency users;

[0125] Providing an online interface for one or more potential currency users to register a user account with password protection, two factor authentication or multiple factor authentication;

[0126] Requesting the submission of documents for proof of the legal identity of a registrant;

[0127] Handling the verification of the legal identity of the registrant;

[0128] Rejection of an account creation for registrants failing in legal identity verification;

[0129] Creating of a personal/client account for individual successful registrants with successful verification of legal identity;

[0130] Allowing a successful registrant to create a credential that comprises a label and a password;

[0131] Allowing a successful registrant to change the credential and contact information;

[0132] Encrypting the credential;

[0133] Storing all the submitted information, particularly the legal identity and the encrypted credential, in a client information database;

[0134] Sending the encrypted credential, which is newly generated or changed, to central approval servers;

[0135] Mapping and storing multisignature currency address(es), credential and legal identity of individual registrants.

[0136] One cryptography-based electronic money and its associated transaction network, wherein it performs at least some, or all of the following basic functions and unique functions:

[0137] 1. Basic functions—common to those of all other cryptography-based electronic money

[0138] Providing client wallet software to public;

[0139] Connecting computers or servers through the client wallets;

[0140] Using the connected computers or servers to form relay nodes of a transaction network;

[0141] Generating a predefined amount of money units (coins) at a predefined speed;

[0142] Protecting the ownerships of the coins by public/private-key cryptography;

[0143] Recording the ownerships of the coins into a ledger of all transactions (e.g. blockchain) using the owners' currency addresses;

[0144] Distributing the ledger of all transactions (e.g. blockchain) and its updates to people who are connected to the transaction network through the client wallet;

[0145] Allowing a private key owner to send an amount of coins only without exceeding an amount of coins recorded at the corresponding currency address after reduction of the required transaction fee;

[0146] Broadcasting all new transaction messages to all relay nodes in the transaction network;

[0147] Verifying all new transaction messages at individual relay nodes;

[0148] Recording the transaction information (including but not limited to sender currency address, receiver currency address, amount of coins being transacted, transaction fee, transaction time) into the ledger of all transactions (e.g., the blockchain);

[0149] 2. Unique functions

[0150] Restricting only valid registered users to generate one or more valid currency addresses to receive the coins by verifying the submitted credential with one of the central approval servers;

[0151] Allowing only creation of multisignature transactions in pay-to-script-hash format or any other compatible format;

[0152] Allowing only creation of multisignature transactions each requiring at least two private keys as signatures;

[0153] Allowing only creation of multisignature transactions in the presence of a valid credential;

[0154] Restricting one of these private keys to be an approval private key from one of the central approval servers;

[0155] Restricting the rest of the private keys to be client private keys, which are encrypted and stored in the client wallet(s);

[0156] Sending all transaction requests from the client wallets to one of the central approval servers to obtain the approval private key for signing the transactions;

[0157] Rejecting all transactions missing any one of the required private keys;

[0158] Restricting transaction approval rules (including but not limited to requisition of a valid credential from the sender, requisition of one or more approval private keys from one of the central approval servers for signing transaction input and for signing whole transaction) for individual transactions by using a "pay-to-script-hash" script or any other compatible script that is built inside the source of the electronic money as the only script for transaction creation;

[0159] At least one computer or server for running client wallet software, wherein the at least one client wallet performs at least some, or all of the following basic functions and unique functions:

[0160] 1. Basic functions—common to those of all other cryptography-based electronic money

[0161] Serving as one of the relay nodes for relaying all transaction information in the transaction network;

[0162] Serving as one of the relay nodes to verify and confirm all transactions that are broadcasted to the transaction network;

[0163] Generating new coins through contributing to recording any new transaction information into the ledger of all transactions (e.g. the blockchain);

[0164] Generating one or more pairs of cryptographic client public key and client private key for receiving and sending coins;

[0165] Storing the client public-private key pairs of one or more currency addresses generated by the currency users;

[0166] Serving as a client wallet for the currency users to receive and send coins;

[0167] 2. Unique functions

[0168] Serving as an client wallet to communicate between one of the central approval servers and registered currency users;

[0169] Only generating currency addresses which are multisignature addresses;

[0170] Generating one of more multisignature addresses from the client public key and the approval public key;

[0171] Only storing one or more multisignature addresses in the client wallet for sending and receiving coins;

[0172] Sending one of more multisignature addresses to the client information database for storage and mapping to legal identity of the owner of the address (es);

[0173] Sending the generated valid multisignature addresses to the central approval servers for storage;

[0174] Submitting a credential of a valid registered users to one of the central approval servers for obtaining approval to generate one or more valid currency multisignature addresses;

[0175] Submitting a credential of a valid registered users to one of the central approval servers for obtaining approval to create one or more valid transactions to send coins to one or more currency addresses;

[0176] Allowing only creation of transactions that use multisignature addresses for both sending and receiving the coins

[0177] Recording unspent coins (if there is any) into the blockchain at the currency address from where the coins have just been sent;

[0178] At least one central approval server, wherein the at least one central approval server performs at least some, or all, of the following functions:

[0179] 1. Retrieving new or updated credentials and their associated currency addresses from the client information database;

[0180] 2. Storing and updating users' credentials and their associated currency addresses in the central approval database;

[0181] 3. Generating, changing, encrypting and storing one or more pairs of approval public key and approval private key.

[0182] 4. Communicating with the client wallet to generate one or more valid multisignature currency addresses in the presence of a valid credential;

[0183] 5. Providing approval public key to the currency wallet to create one or more multisignature addresses,

[0184] 6. Communicating with the client wallet to generate one or more valid transactions to send coins to one or more currency address in the presence of a valid credential;

[0185] 7. Providing approval private key, which are corresponding to the approval public key used in creation of the multisignature address, to sign transaction input for one or more valid transactions.

[0186] 8. Providing another approval private key, which can be the approval private key used in item **410** or the most recent approval private key, to sign the whole transaction for one or more valid transactions.

[0187] 9. Storing all transaction information (including but not limited to transaction ID, sender currency address, receiver currency address, amount of coins being transacted, transaction fee, transaction time and IP addresses of sender and receiver's client wallets) in a transaction database.

[0188] Further, there is disclosed a method for personal/client identification and verification for transactions involving cryptography-based electronic money, the method comprising at least some, or all, of the steps of:

[0189] 1. Verifying legal identity of a registrant;

[0190] 2. creating a personal/client account, protected by at least two-factor authentication, for an individual successful registrant with successful verification of legal identity whereas the personal/client account facilitates mapping and storing individual registrants' legal identity and currency address(es) with the personal/client account;

[0191] 3. receiving a credential, of an individual successful registrant, defining identity of the registrant, ownership of a currency address and sender identity of a transaction;

[0192] 4. storing the registrant's legal identity and credential in one or more central approval servers;

[0193] 5. providing a registrant wallet for sending and receiving at least one unit of electronic money;

[0194] 6. recording ownership of at least one unit of electronic money into a ledger of all transactions (e.g. blockchain) using the registrant's currency address(es);

[0195] 7. receiving and verifying a credential, which is submitted from a registrant wallet under a request for generation of a currency address, at a central approval server;

[0196] 8. approving the creation of a multisignature address as a valid currency address belonging to the registrant, by providing an approval public key from the central approval server to the registrant wallet;

[0197] 9. generating a valid currency address for receiving at least one unit of electronic money by combing the registrant's public key and the central approval server's approval public key at the registrant wallet;

[0198] 10. storing and mapping the registrant's legal identity, credential, one or more valid currency addresses in a client information database;

[0199] 11. creating a transaction, in a "pay-to-script-hash" format or any other compatible format, each requiring at least two private keys as signatures at the registrant wallet;

[0200] 12. restricting at least one of these private keys to be an approval private key from one of central approval servers;

[0201] 13. restricting the rest of the private keys to be the registrants' private keys, which are stored in the client wallets;

[0202] 14. restricting transaction approval rules (including but not limited to requisition of a valid credential from the sender, requisition of one or more approval private keys from one of the central approval servers for signing transaction input and for signing whole transaction) for individual transactions by using a "pay-to-script-hash" script or any other compatible script that is built inside the source of the electronic money as the only script for transaction creation;

[0203] 15. receiving and verifying a credential, which is submitted from a registrant wallet under a request for creation of a transaction, at a central approval server;

[0204] 16. verifying the transaction against one or more transaction criteria (including but not limited to those are predefined by the central governing body and/or the registrant) at the central approval server;

[0205] 17. approving the execution of the transaction by signing the transaction with one or more private keys at the registrant wallet(s) and by signing the transaction with one or more the approval private keys at the central approval server;

[0206] 18. recording the transaction message in the ledger of all transactions (e.g. blockchain);

[0207] 19. storing the transaction information (including but not limited to transaction ID, sender and receiver's cryptocurrency addresses, amount of money transacted, time of transaction and IP addresses of sender and receiver's client wallets) in a transaction database;

[0208] 20. broadcasting the signed transaction message to all relay nodes in a transaction network for confirmation;

[0209] 21. tracing legal identities of the sender and receiver by mapping their currency addresses in the transaction database and the client information database when needed.

[0210] The systems and methods described herein may be modified to require two or more approval private keys from one or more independent central governing bodies for approving the transactions. Such modified electronic money and its associated payment network may have a higher degree of regulation and governance.

[0211] The systems and methods described herein may be modified to use single-signature addresses which are only signed by a single user or multisignature addresses which are signed by two or more users for receiving and sending electronic money without requiring any approval private key from the central governing body for approving the transactions. However, such modified electronic money and its associated payment network may be more susceptible to hacking to override the regulation by the central governing body.

[0212] The systems and methods described herein may be modified to use a single-signature addresses which are only signed by a central governing body or multisignature addresses which are signed by two or more central governing

bodies for receiving and sending electronic money without requiring any private key from a user for approving the transactions. However, users may have less protection on ownership of their electronic money. Validity of such modified electronic money and its associated payment network may depend on the trust and honesty of the central governing body(ies).

[0213] The systems and methods described above may have at least some or all of the following preferable features.

[0214] Preferably, the pair of approval public Key and approval private key can be changed manually or automatically in a regular period to avoid leakage of the approval public key and the approval private key to the public. After changing to a new pair of approval key, the old approval private key will be used for signing the transaction input, and the new approval private key will used for signing the whole transaction (i.e., all transaction's data).

[0215] Preferably, any currency addresses that are not generated through the submission of a valid credential to one of the central approval servers are not valid, and are not able to receive any coins.

[0216] Preferably, the transaction network can be modified to reject any transactions that do not the meet the central transaction criteria stored in one of the central approval servers.

[0217] Preferably, the client transaction criteria can be defined by a valid registered user to limit his/her own transactions.

[0218] Preferably, the transaction criteria can be defined by a central governing body to stop suspicious transactions that is likely to be involved in illegal activities, such as money laundering.

[0219] Preferably, individual transactions can be monitored with a defined rules to identify, record and report suspicious transactions that is likely to be involved in illegal activities, such as money laundering.

[0220] Preferably, legal identities of owners of individual currency addresses are stored in the client information database. For those transactions suspected of illegal activities, identities of their associated senders and receivers will be extracted from the client information database by tracing with the currency addresses of the senders and receivers. Subsequently, the suspicious activities and the associated client information will be reported to government agencies with respect to the regulations and laws in the associated countries.

[0221] Preferably, legal identities of owners for individual currency addresses are stored in the client information database. This fulfills the "know-your-customer" regulatory requirement. This allows the system to be used as a payment system for commercial activities.

[0222] Preferably, legal identities of owners for individual currency addresses are stored in the client information database. However, such information is not accessible to the public, in order to maintain the pseudonymous property of the cryptography-based electronic money and its transaction network.

[0223] Preferably, a user can change his/her credential to stop coins being transferred out from a stolen main data file (e.g., wallet.dat file) of his/her currency wallet. Preferably, (i) legal identities of owners for individual currency addresses are stored in the client information database, (ii) any currency addresses that are not generated through the submission of a valid credential to one of the central approval servers are not valid, and are not able to receive any coins, and only valid registered users have a valid credential. When coins are stolen from someone, the theft(s) or the hacker(s) can be easily traced by retrieving legal identity(s) of the receiver(s) from the client information database. Therefore, the implementation of the system prevents a cryptocurrency from being stolen.

[0224] Preferably, the amount of coins own by a valid registered user are completely and easily traceable and trackable by the central governing body through analyzing the transaction records in the transaction database. Besides the capability of linking individual currency addresses to their owners, this unique property is contributed by recording unspent coins (if there is any) at the currency address from where the coins have just been sent/spent. This unique property allows applications of our system to financial and banking activities, particularly those required third-party auditing.

[0225] Preferably, the systems provide a practical solution for the issues related to cryptocurrency theft, KYC and AML, while maintaining user privacy.

[0226] Preferably, the systems can be adopted or modified by the central banks or other financial institutions to issue their own digital currencies that are supported by a distributed ledger payment system, but also regulated by a central governing body.

BRIEF DESCRIPTION OF THE DRAWINGS

[0227] These and other objects of the invention presented herein, are accomplished by providing a system and method for personal/client identification and verification. Further details and features of the present invention, its nature and various advantages will become more apparent from the following detailed description of the preferred embodiments shown in a drawing, in which:

[0228] FIG. **1** presents a registration and database system for capturing, verifying and storing legal identity of a new user for a cryptography-based electronic money;

[0229] FIG. **2** depicts a legal identity-linked credential authentication system for generation of a multisignature currency address for receiving and sending a cryptography-based electronic money;

[0230] FIG. **3** shows a legal identity-linked credential authentication system and the two-party signature scheme for generation of a payment transaction of an amount of coins which are owned by a user and recorded at a multisignature address;

[0231] FIG. **4** presents a diagram of a system according to the present invention.

NOTATION AND NOMENCLATURE

[0232] Some portions of the detailed description which follows are presented in terms of data processing procedures, steps or other symbolic representations of operations on data bits that can be performed on computer memory. Therefore, a computer executes such logical steps thus requiring physical manipulations of physical quantities.

[0233] Usually these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in a computer system. For reasons of common usage, these signals are referred to as bits, packets, messages, values, elements, symbols, characters, terms, numbers, or the like.

[0234] Additionally, all of these and similar terms are to be associated with the appropriate physical quantities and are

merely convenient labels applied to these quantities. Terms such as "processing" or "creating" or "transferring" or "executing" or "determining" or "detecting" or "obtaining" or "selecting" or "calculating" or "generating" or the like, refer to the action and processes of a computer system that manipulates and transforms data represented as physical (electronic) quantities within the computer's registers and memories into other data similarly represented as physical quantities within the memories or registers or other such information storage.

[0235] A computer-readable (storage) medium, such as referred to herein, typically may be non-transitory and/or comprise a non-transitory device. In this context, a non-transitory storage medium may include a device that may be tangible, meaning that the device has a concrete physical form, although the device may change its physical state. Thus, for example, non-transitory refers to a device remaining tangible despite a change in state.

[0236] As utilized herein, the term "example" means serving as a non-limiting example, instance, or illustration. As utilized herein, the terms "for example" and "e.g." introduce a list of one or more non-limiting examples, instances, or illustrations.

DESCRIPTION OF EMBODIMENTS

[0237] The present invention relates to technical fields of cryptographic-based electronic money (CBEM), such as alternative cryptocurrency, and transaction systems. More specifically, the present invention relates to a method and system for creating of a new CBEM and its associated payment system that allows disclosure of the legal identities of senders and receivers in all money transactions, while maintaining the pseudonymous property of the CBEM.

[0238] The present invention allows inclusions of additional modules for monitoring all transactions and identifying those potentially related to illegal activities, and for including criteria, which are defined by a central governing body or CBEM users, to regulate or limit transactions.

[0239] As a result, the present invention provides a practical solution for the issues related to cryptocurrency theft, KYC and AML, while maintaining user privacy. Moreover, the present invention can be adopted or modified by the central banks or other financial institutions to issue their own digital currencies that are supported by a distributed ledger payment system, but also regulated by a central governing body.

[0240] To this end, the present invention involves an integration of three major processes, including (i) legal identity verification, (ii) credential authentication and (iii) a two-party signature scheme. Embodiments of the present invention may provide systems and methods for creation of a CBEM and its associated payment system that allows a central governing body to reveal legal identities of senders and receivers in any money transactions, while maintaining the pseudonymous property of the CBEM.

[0241] The credential authentication mechanism of the present invention allows a user to change the credential to stop coins being transferred out from a stolen wallet. Last and not least, as senders and receivers of all transactions can be revealed, the theft(s) or the hacker(s) who has stolen the coins can be easily traced by retrieving legal identity(s) of the receiver(s) from the client information database. As a result, the embodiments of the present invention can prevent CBEM coins from being stolen.

[0242] To be able to reveal legal identities of senders and receivers of all transactions of a CBEM, it requires the following two key elements:

[0243] 1. legal identities of all receivers and senders of a CBEM;

[0244] 2. prohibition of anonymous people to receive and send coins of a CBEM;

[0245] These two key elements can be obtained by allowing only registered users with a verified legal identity to receive and send a CBEM. For capturing and verification of legal identities, a web-based registration interface is created for individual registrants to submit information to provide and prove his/her legal identity, and only those people with a successfully verified legal identity are accepted as valid users. They can then receive and send the CBEM. However, the major difficulty is how to prohibit anonymous people to receive and send coins of a CBEM, particularly open-source CBEM.

[0246] CBEMs, such as Bitcoin, are designed to be a decentralized payment system. Their computer programming codes are expected to be available for perusal by anyone at the open source online community. When a CBEM is open source, anyone can use the source code to create his/her currency address to receive and send the coins. Therefore, the KYC registration approach can only be applied to specific service providers, but not to all the coin users.

[0247] In order to restrict the coin usage to only registered users, a new method has been developed to differentiate currency addresses generated by registered non-anonymous users (i.e., valid currency addresses) from those generated by non-registered anonymous users (i.e., invalid currency addresses), and another method has been developed to only allow those valid currency addresses to be used for receiving and sending coins.

[0248] The present invention provides a practical solution for these two tasks through an integration of three major processes, including (i) legal identity verification, (ii) credential authentication and (iii) a two-party signature scheme. Such integration requires technical changes in:

[0249] 1. modifying Bitcoin's multisignature transaction protocol;

[0250] 2. linking it to a client information database;

[0251] 3. making it as the compulsory transaction protocol, and

[0252] 4. forcing one transaction signature to be a private key from one of the central approval servers.

[0253] The embodiments of the present invention may be achieved by the following key steps:

Step 1: Setting up a computer server and a web-based interface for capturing, verification and storage of legal identities of users and for creating user-specific credentials;

Step 2: Using the web-based interface to create credentials for regulating the process of currency address generation;

Step 3: Using a multisignature approach for receiving and sending coins; and

Step 4: Enforcing pay-to-script-hash transactions regulated by specific rules.

[0254] The aforementioned steps will now be described in more details.

Step 1: Setting Up a Computer Server and a Web-Based Interface for Capturing, Verification and Storage of Legal Identities of Users and for Creating User-Specific Credentials

[0255] The step of setting up a computer server and a web-based interface (e.g. BGCwallet.com) concerns users of a CBEM (e.g. Aten Coin). In the process of registration, a person should provide document/information about his/her legal identity (e.g. passport ID number and copy of identity page of his/her passport), and go through a process to verify his/her legal identity (e.g. identity verification service from MiiCard or IDchecker). A successful registration requires a successful verification of his/her legal identity. All the provided information will be stored in a client information database.

[0256] FIG. **1** presents a registration and database system for capturing, verifying and storing legal identity of a new user for a cryptography-based electronic money.

[0257] At least one server comprising at least one web-based registration interface (**102**), performs the following functions. First, at step (**105**) there is requested, via the web-based registration interface (**102**), a submission of documents for proof of the legal identity of a registrant. Next, at step (**106**) there is handled the verification of the legal identity of the registrant. An unsuccessful verification leads to a registration fail (**107**). Alternatively, a successful registrant (**109**) is allowed to create two factor authentication or multiple factor authentication (**104**) to prevent unauthorized access to his/her registered user account and malicious attack.

[0258] Two-factor authentication is a secure way to protect online user account (**104**). It works by requiring a user to identify oneself using two different things when he/she logs into his/her online account. The first authentication thing is a pair of login name and login password created by the user; the second authentication thing is a constantly changing token (e.g. a unique 7-digit code) which is tied to a physical device that is owned by the user, such as a cellphone or a personalized secure key generating device. Then, such online user account cannot be hacked without stealing the personal physical device. Multiple-factor authentication can also be possible by requiring a user to identify oneself using three or more different things when he/she logs into his/her online account (e.g. a pair of login name and login password, a cellphone and a smart identity card).

[0259] A successful registrant (**109**) is required to create a credential (**111**) that comprises a label and a password (**112**). Naturally a successful registrant (**109**) is allowed to change the credential and contact information (**113**), all of which are preferably encrypted at step (**114**). The credential is required for a user to generate his/her multisignature wallet address (es) (FIG. **2**) for receiving coins (e.g. atencoins), and for creating transactions (FIG. **3**).

[0260] Optionally, at step **502**, there may be defined, client transaction criteria, by a valid registered user to limit his/her own transactions. For example, a user can set a criterion that limits the maximum amount of coins being sent out from his/her currency address(es) within 24 hours. This can minimize the loss of his/her coins when his/her currency wallet is being stolen or hacked.

[0261] When the above are completed, at step (**116**) there is executed storing all the submitted information, particularly the legal identity and the encrypted credential, in the client information database (**115**).

[0262] Finally, at step **117** there is executed sending of the encrypted credential, which is newly generated or changed, to central approval servers (**401**). The central approval servers execute mapping and storing multisignature currency address (es), credential and legal identity of individual registrants (**118**). For example, a multisignature currency address is a unique string of 34 characters composed of numerical numbers, small and large alphabet letters (e.g. Aj8xFozUjo3GoNvi95kABpTjO2qQReZo5P); person identity is composed of (i) a full legal name printed on the user's national identity card or passport, (ii) national identity card/passport number and (iii) date of birth.

Step 2: Using the Web-Based Interface to Create Credentials for Regulating the Process of Currency Address Generation

[0263] Using the web-based interface, only a valid registered user (**106**, **109**) can generate a credential (**111**) (FIG. **1**, **112**), which is required for generating his/her multisignature address(es) (as shown in FIG. **2**) for receiving and sending coins (e.g. atencoins) (as shown in FIG. **3**). The use of credentials prohibits non-registered, anonymous users to generate any valid multisignature addresses to receive and send coins in the system. In other words, all valid currency addresses, for sending or receiving coins of a CBEM, are linked to real people with known, legal identities.

Step 3: Using a Multisignature Approach for Receiving and Sending Coins

[0264] By design, one approval public key from one of the central approval servers and at least one client public key are required to generate valid multisignature addresses for receiving and sending coins (FIG. **2**). Before one can use the client wallet (**301**) to generate an address to receive coins, he/she must have input his/her credential (**111**) into the client wallet. In the process of address generation, the client wallet will first submit the credential to one of the central approval servers (**401**) through an electronic/digital data transmission network (e.g. the Internet) for validation (**407**).

[0265] After checking the credential is valid, i.e., successful matching to a valid and active credential in the database of the central approval servers (**319**, **401**, **407**), the central approval server will provide the approval public key (**408**) to the client wallet through the electronic/digital data transmission network. If the credential is found to be invalid or inactive, the central approval server will return a failure message to the client wallet. After receiving the approval public key, the client wallet will proceed to generate a multisignature address (**315**).

[0266] After receiving the failure message, the client wallet will stop to the process of multisignature address generation. In the presence of the approval public key, the client wallet generates (**309**) a pair of client public key (**307**) and private key (**308**) and stores (**310**) in the client wallet, and subsequently combines the approval public key (**405**) and the client public key (**307**) to create a multisignature address (**315**), which hence is closely linked to the approval private key and the client private key. The multisignature address is stored and displayed in the client wallet (**316**). The user can use the multisignature address to receive coins of a CBEM (e.g. atencoins).

[0267] The presence of the approval public key in each multisignature address dictates that all transactions have to obtain both the approval signature (i.e., the approval private

key (**406**)) from one of the central approval servers and the client signature (i.e., the client private key (**308**)) for conferring validity.

[0268] Using this control system, only valid registered users can generate multisignature addresses. These addresses can then be used to make transactions that need to be countersigned by one of the central approval servers.

[0269] FIG. **2** depicts a legal identity-linked credential authentication system for generation of a multisignature currency address for receiving and sending a cryptography-based electronic money.

[0270] The process starts from step (**301**) with providing client wallet, which is a network resource preferably accessible as a software. Next, the input user credentials, from step (**111**), are applied in order to activate a client's wallet. Subsequently, at step (**314**), a user attempts to create a currency address wherein the system only generates currency addresses which are multisignature addresses.

[0271] Next, at step (**319**), there is executed submitting a credential, of valid registered users, to one of the central approval servers (**401**) for obtaining approval to generate one or more valid currency multisignature addresses.

[0272] In case of a failure of approval, an appropriate error message may be generated. Otherwise, in case of approval, there is executed, at step (**309**), generating one or more pairs of cryptographic client public key (**307**) and client private key (**308**) for receiving and sending coins. These client public key and client private key are stored and associated with the client's wallet (**310**). In case of approval, there is also executed, at step **408**, providing an approval public key (**405**), which is mathematically linked to an approval private key (**406**), from the central approval server to the client wallet.

[0273] Further, at step (**315**), there is executed generating one of more multisignature addresses from the client public key(s) (**307**) and the approval public key(s) (**405**). The generated multisignature currency address is stored and associated with the client's wallet (**316**).

[0274] Subsequently, at step (**317**), there is executed sending one of more multisignature addresses to the client information database (**115**), for storage and mapping to legal identity of the owner of the address(es) (**118**).

Step 4: Enforcing Pay-to-Script-Hash Transactions Regulated by Specific Rules

[0275] Bitcoin developers have currently created two different methods for creating and approving Bitcoin transactions using different scriptSig/scriptPubKey pairs. The two methods are pay-to-pubkey-hash and pay-to-script-hash.

[0276] The pay-to-pubkey-hash is the most commonly used method in daily Bitcoin transactions. In a pay-to-pubkey-hash transaction, a Bitcoin address is a 160-bit hash of the public portion of a public/private Elliptic Curve Digital Signature Algorithm (ECDSA) key pair, and a Bitcoin sender provides a Bitcoin address in scriptPubKey. In a pay-to-pubkey hash transaction, a sender transfers bitcoins directly to an owner of a public key.

[0277] In order to initiate a pay-to-pubkey hash transaction, the sender needs to provide a public key of which bitcoins are stored at the corresponding Bitcoin address and the corresponding signature (i.e., a paired private key), as well as a Bitcoin address for receiving the bitcoins. The receiving Bitcoin address is directly linked its corresponding pubic key and signature. When redeeming coins that have been sent to the Bitcoin address, the recipient provides both the signature and the public key. The script verifies that the provided public key does hash to the hash in scriptPubKey, and then it also checks the signature against the public key.

[0278] Addresses associated with pay-to-script transactions are hashes of scripts instead of a public key hash. To spend bitcoins through pay-to-script-hash, the process requires provision of a script matching the script hash and data which makes the script evaluate to true. In other words, one has to provide an input (i.e., an answer) to the script in question that the script accepts, and the transaction proceeds. If the input is invalid and the script will not be accepted, resulting in stoppage of the transaction.

[0279] Using pay-to-script-hash, one can send bitcoins to an address that is secured in various unusual ways without knowing anything about the details of how the security is set up. For example, the recipient might need the signatures of several people to receive bitcoins stored at a particular Bitcoin address, or a password might be required, or the requirements could be completely unique. For Bitcoin and all other current cryptocurrencies developed on the basis of the Bitcoin technology, pay-to-script-hash is not compulsory.

[0280] The pay-to-pubkey-hash is the standard method in Bitcoin transactions as well as in the transactions for all other current cryptocurrencies based on the Bitcoin technology. The pay-to-script-hash function is built into client wallet software of a cryptocurrency. A cryptocurrency owner can use the client wallet software to choose to use pay-to-pubkey-hash or pay-to-script-hash to create transactions.

[0281] According to the present invention, only pay-to-script-hash transactions are allowed in the CBEM transaction network. In contrast to Bitcoin and all other current cryptocurrencies based on the Bitcoin technology, this restriction is implemented inside the source codes of the CBEM, instead of only inside the source code of the client wallet software. In such way, a CBEM developer can enforce specific rules in all transactions, and this allows an implementation of a legal identity-linked credential authentication system to control all transactions. The legal identity-linked credential authentication system involves the use of user-specific credentials and multisignature addresses for receiving and sending the CBEM.

[0282] In the legal identity-linked credential authentication system, only multisignature addresses are used in the pay-to-script-hash transactions for receiving and sending the CBEM. Each client multisignature address is linked to a script that includes a client pubic key (that is generated from the client wallet) (**307**) and an approval public key (that is generated from one of the central approval server) (**405**) for create and signing transactions. Hence, every pay-to-script-hash transactions require at least a client private key (**308**) and an approval private key (**406**) to make the transaction valid.

[0283] The script for pay-to-script-hash transactions is implemented inside the source codes of the CBEM, instead of only inside the client wallets. This allows the script to enforce the requirement of one or more approval private keys (**406**) from one or more central approval servers to initializing and signing all transactions. Because provision of the approval private keys can be regulated through the central approval servers, no one can create any pay-to-pubkey-hash or pay-to-script-hash transaction that can bypass the requirements, regulations and/or rules that are predefined at the central approval servers.

[0284] FIG. **3** shows a legal identity-linked credential authentication system and the two-party signature scheme for

generation of a payment transaction of an amount of coins which are owned by a user and recorded at a multisignature address.

[0285] To create a pay-to-script-hash transaction (**218**), a client's wallet (**301**) requires a signature (i.e., an approval private key) (**406**) from a one of the central approval servers (**401**) to get permission. This request is sent with an API call to the central approval servers for authentication (**220**). In case of a failure of authentication, an appropriate error message may be generated.

[0286] If the credential submitted by the client wallet to the central approval servers (**401**) is valid (**220**, **409**) and that requested transaction is not considered as suspicious according to predefined criteria (**501**, **502**), it gets the signature from the client wallet (i.e., the client private key) (**308**) and the signatures (i.e., the approval private key(s)) (**406**, **411**) from one of the central approval servers to approve the transaction (**410**, **412**).

[0287] The script of a pay-to-script hash can be modified to require more than one client public key and/or approval private key, resulting in payment transactions requiring more than one signature from one or more clients (either senders or receivers) and/or from one or more approval agencies in order to proceed a transaction. Furthermore, to increase the security, two different approval private keys can be used for signing transaction input (**410**) and for signing whole transaction (**412**).

[0288] The present invention enforces all transactions requiring at least one approval private key from a central approval server as a signature in order to proceed a transaction. Moreover, the provision of approval private keys require a successfully validation of a valid credential provided by the sender. Because all valid credentials are linked to individual client wallet addresses and owned by registered users, of whom legal identities have been verified and stored in the client information database (FIG. **2**). In such way, only a registered user with his/her legal identity stored in the database can transfer any coins from his/her wallet addresses to other wallet addresses upon submission of a valid credential.

[0289] The credential provides a link for a central governing body owning the central approval servers and the client information database to uncover the legal identity of a CBEM sender or receiver when necessary. Because information of legal identity is not required in the whole process of a pay-to-script-hash transaction, the sender and receiver remains pseudonymous.

[0290] A central approval server may reject any transactions that do not the meet central transaction criteria (**501**) stored in at least one of the central approval servers (**401**). In particular, individual transactions can be monitored with predefined rules to identify, record and report suspicious transactions that is likely to be involved in illegal activities, such as money laundering. Any suspicious transactions and identities of the associated senders and receivers can be reported to the relevant government agencies for further action. The invention hence provides a practical solution for the current KYC/AML incompliance issues for Bitcoin and various alternative currencies.

[0291] Optionally, at step **502**, there may be defined, client transaction criteria, by a valid registered user to limit his/her own transactions. For example, a user can set a criterion that limits the maximum amount of coins being sent out from his/her currency address(es) within 24 hours. This can minimize the loss of his/her coins when his/her currency wallet is being stolen or hacked.

[0292] The transaction is then broadcasted to the network of nodes (**214**) for confirmation (**305**). After a transaction is generated, it is sent to transaction network for processing and has to be included in a block of the blockchain before becoming legitimate. Nodes accept the block only if all transactions in it are valid (i.e., properly signed) and not already spent. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

[0293] The process of implementing a transaction in a newly created block is called a transaction confirmation. Inclusion in one block is considered as one confirmation. When there are confirmations equal to or more than a predefined number (e.g. 6 in the case of Bitcoin, 10 in the case of Aten Coin), the transaction is considered confirmed. In the Bitcoin technology, this feature is introduced in order to protect the system form repeated spending of the same coins (i.e., double-spending).

[0294] The unique functions of the arrangement presented in FIG. **1**-FIG. **3** are:

- **[0295]** Allowing only creation of multisignature addresses (**313**) as valid currency addresses; (**314**)
- **[0296]** Allowing only creation of transactions that use multisignature addresses (**313**) for both sending and receiving the coins; (**321**)
- **[0297]** Allowing only creation of transactions in pay-to-script-hash format or any other compatible format (**218**); (**311**) Allowing only creation of transactions each requiring at least two private keys as signatures; (**308**, **406**)
- **[0298]** Restricting one of these private keys (**308**, **406**) to be an approval private key (**406**) from one of the central approval servers (**401**);
- **[0299]** Restricting the rest of the private keys (**308**, **406**) to be client private keys (**308**), which are encrypted and stored in the client wallet(s) (**301**);
- **[0300]** Restricting only valid registered users (**109**) to create valid credentials (**111**); (**112**)
- **[0301]** Restricting only users who have a valid credential (**111**) to generate one or more valid multisignature currency addresses (**313**) to receive the coins by verifying the submitted credential (**111**) through one of the central approval servers (**401**); (**319**, **407**)
- **[0302]** Restricting only users who have a valid credential (**111**), one or more valid multisignature currency addresses (**313**) and the corresponding client private keys (**308**, **309**) to create one or more valid transactions; (**220**, **320**, **409**)
- **[0303]** Restricting only users who have a valid credential (**111**) to receive one or more approval private keys (**406**, **411**) from one of the central approval servers (**401**) for signing one or more transactions (**410**, **412**) by verifying (**220**, **320**, **409**) the submitted credential (**111**) through one of the central approval servers (**401**);
- **[0304]** Restricting only users who have received one or more approval private keys (**406**, **411**) from one of the central approval servers (**401**) to create valid transactions by verifying (**220**, **320**, **409**) the submitted credential (**111**) through one of the central approval servers (**401**), and hence restricting only users who have a valid credential (**111**) to create valid transactions;

[0305] Linking individual credentials (**111**, **112**, **113**, **114**) to users' legal identities (**105**); (FIG. **1**)

[0306] Using individual credentials (FIG. **1**, **111**) to trace their owners' legal identities (**105**); (**116**)

[0307] Linking individual multisignature addresses (**313**, **314**) to users' credentials (**111**); (FIG. **2**)

[0308] Using individual multisignature addresses (**313**) to trace (**118**) credentials (**111**) of their owners (FIG. **2**), and hence using the credentials (**111**) to trace (**116**) legal identities (**105**) of the owners (FIG. **1**);

[0309] Using individual transactions to trace multisignature addresses (**313**) of senders and receivers (FIG. **3**), subsequently using the multisignature addresses (**313**) to trace (**118**) credentials (**111**) of the senders and receivers (FIG. **2**), and finally using the credentials (FIG. **1**, **111**) to trace (**116**) legal identities (**105**) of the senders and receivers;

[0310] Allowing tracing and tracking (**116**) legal identities of senders (FIG. **1**, **105**) and receivers in all valid transactions (FIG. **3**) because only users who have a valid credential (**111**) can create valid multisignature addresses (FIG. **2**) and create valid transactions (FIG. **3**).

[0311] In some implementations, the methods described in connection with FIG. **1**, FIG. **2**, and/or FIG. **3** may be implemented in one or more processing devices (e.g., a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information). The one or more processing devices may include one or more devices executing some or all of the operations of the method in response to instructions stored electronically on an electronic storage medium. The one or more processing devices may include one or more devices configured through hardware, firmware, and/or software to be specifically designed for execution of one or more of the operations of the method(s) illustrated in FIG. **1**, FIG. **2**, and/or FIG. **3**.

[0312] FIG. **4** presents a diagram of the system according to the present invention. The system is a client-server arrangement wherein the server is one or more central approval servers. The diagram illustrates an exemplary computer network ("system **400**") in which one or more implementations of the present invention may be realized. In some implementations, system **400** may include one or more servers **401**. The server(s) **401** may be configured to communicate with one or more client computing platform(s) **414**/**415** according to a client/server architecture. The users may access system **400** via client computing platform(s) **414**/**415**. The server(s) **401** and client computing platform(s) **414**/**415** may be configured to execute machine-readable instructions.

[0313] In some implementations, the server(s) **401**, client computing platform(s) **414**/**415**, and/or external resource(s) **418** may be operatively linked via one or more electronic communication links. For example, such electronic communication links may be established, at least in part, via a network such as the Internet and/or other networks. It will be appreciated that this is not intended to be limiting, and that the scope of this disclosure includes implementations in which server(s) **401**, client computing platform(s) **414**/**415**, and/or external resource(s) **418** may be operatively linked via some other communication media.

[0314] A given client computing platform **414**/**415** may include one or more processors configured to execute machine-readable instructions. The machine-readable instructions may be configured to enable an expert or user associated with the given client computing platform **414**/**415** to interface with system **400** and/or external resource(s) **418**, and/or provide other functionality attributed herein to client computing platform(s) **414**/**415**. By way of non-limiting example, the given client computing platform **414**/**415** may include one or more of a desktop computer, a laptop computer, a handheld computer, a tablet computing platform, a NetBook, a Smartphone, a gaming console, and/or other computing platforms.

[0315] External resource(s) **418** may include sources of information, external entities participating with system **400**, and/or other resource(s). In some implementations, some or all of the functionality attributed herein to external resource (s) **418** may be provided by resource(s) included in system **400**.

[0316] Server(s) **401** and/or client computing platform(s) **414**/**415** may include electronic storage **419**, one or more processors **420**, and/or other components. Server(s) **401** may include communication lines, or ports to enable the exchange of information with a network and/or other computing platforms. Illustration of server(s) **401** in FIG. **1** is not intended to be limiting. Server(s) **401** may include a plurality of hardware, software, and/or firmware components operating together to provide the functionality attributed herein to server(s) **401**. For example, server(s) **401** may be implemented by a cloud of computing platforms operating together as server (s) **401**.

[0317] Electronic storage **419** may comprise non-transitory storage media that electronically stores information. The electronic storage media of electronic storage **419** may include one or both of system storage that is provided integrally (i.e., substantially non-removable) with server(s) **401** and/or removable storage that is removably connectable to server(s) **401** via, for example, a port (e.g., a USB port, a firewire port, etc.) or a drive (e.g., a disk drive, etc.). Electronic storage **419** may include one or more of optically readable storage media (e.g., optical disks, etc.), magnetically readable storage media (e.g., magnetic tape, magnetic hard drive, floppy drive, etc.), electrical charge-based storage media (e.g., EEPROM, RAM, etc.), solid-state storage media (e.g., flash drive, etc.), and/or other electronically readable storage media. Electronic storage **419** may include one or more virtual storage resource(s) (e.g., cloud storage, a virtual private network, and/or other virtual storage resource(s)). Electronic storage **419** may store software algorithms, information determined by processor **420**, information received from server(s) **401**, information received from client computing platform(s) **414**/**415**, and/or other information that enables server(s) **401** to function as described herein.

[0318] Processor **420** may be configured to provide information processing capabilities in server(s) **401**. As such, processor **420** may include one or more of a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information. Although processor **420** is shown in FIG. **1** as a single entity, this is for illustrative purposes only. In some implementations, processor **420** may include a plurality of processing units. These processing units may be physically located within the same device, or processor **420** may represent processing functionality of a plurality of devices operating in coordination. Processor **420** may be configured to machine-readable instructions and/or compo-

nents of machine-readable instructions by software; hardware; firmware; some combination of software, hardware, and/or firmware; and/or other mechanisms for configuring processing capabilities on processor **420**. As used herein, the term "component" may refer to any component or set of components that perform the functionality attributed to the component. This may include one or more physical processors during execution of processor readable instructions, the processor readable instructions, circuitry, hardware, storage media, or any other components.

[0319] The client **414**/**415** and the server **401** may comprise data processing resources that may be realized using dedicated components or custom made FPGA or ASIC circuits. These computing resources are suitable to store and execute software implementing steps of the method according to the present invention.

[0320] The central approval server (**401**) processes client registration requests (FIG. **1**), client cryptocurrency addresses (FIG. **2**) client account update requests as well as cryptocurrency transactions (FIG. **3**). The central approval server (**401**) thus cooperates with a client information database (**404**) (e.g. User X: legal name, date of birthday, home address, contact address, credential, cryptocurrency address, transaction criteria) as well as with a transactions database (**413**) (e.g. Transaction Y: transaction ID, sender and receiver's cryptocurrency addresses, amount of coins transacted, time of transaction and IP addresses of sender and receiver's client wallets).

[0321] Legal identities of owners for individual currency addresses are stored in the client information database (FIG. **1**, **115**). This fulfills the "know-your-customer" regulatory requirement and allows the system to be used as a payment system for commercial activities. However, such information is not accessible to the public, in order to maintain the pseudonymous property of the CBEM and its transaction network.

[0322] When coins are stolen from someone, the theft(s) or the hacker(s) can be easily traced by retrieving legal identity (s) of the receiver(s) from the client information database (**115**). Therefore, the implementation of the system prevents coins of the CBEM from being stolen.

[0323] Because of the pseudonymous or anonymous nature of Bitcoin and alternative cryptocurrencies based on the Bitcoin technology, coin balance of individual coin owners is not traceable by only analyzing the public transaction records stored in the blockchain. Furthermore, by design, when one spends only part of the coins recorded at a specific currency address, the amount of unspent coins is recorded at a newly generated currency address. Through analysis of the blockchain, it is computation intensive for a third party to track where a received sum of coins has been finally transacted to and recorded at what addresses.

[0324] With the present invention, an amount of coins owned by a valid registered user is completely traceable and trackable by the central governing body through analyzing the transaction records in the transactions database (**413**). Besides the capability of linking individual currency addresses to their owners, this unique property of the present system is contributed by recording unspent coins (if there is any) at the currency address from where the coins have just been sent/spent. In other words, the amount of coins recorded at a currency address will become zero only after all of the coins, which were previously sent to that address, have been sent/spent (**322**). This unique property not only simplifies a third party process for tracing and tracking the ownership transfers of cryptocurrency coins through analyzing the transaction records in the blockchain, but also allows applications of the system to financial and banking activities, particularly those required third-party auditing.

[0325] The central approval server (**401**) communicates with one or more clients (**414**, **415**) implementing client wallets (**416**, **417**).

[0326] A user of a wallet requests a transaction, which must be validated by one or more central approval servers (**401**). Therefore the clients are connected with the servers (**401**) via a suitable bidirectional communication link such as GSM, UMTS, DSL.

[0327] The invention may include means to identify and stop any suspicious or unauthorized transactions automatically. Moreover, this invention prevents a CBEM from (i) being used for money laundering and (ii) being stolen. The present invention hence allows the CBEM and its transaction network to comply with AML and (KYC) policies and regulations. For example, GlobalVision Systems' PATRIOT OFFICER, an advanced rule-based intelligent BSA/AML/ATF system, can be applied to effectively automate the BSA/AML/ATF workflow by monitoring, screening, detecting, alerting, investigating and analyzing suspicious activities of all transactions.

[0328] The invention provides a useful outcome, which is improved security and traceability of transactions. This result is also concrete and tangible since statistical measurements show improved security and fewer attempts of CBEM stealing. Therefore, the invention provides a useful, concrete and tangible result. The machine or transformation test is fulfilled by the fact that the improved security achieved by means of the present invention requires requiring generations of multisignature addresses and pay-to-script-hash transactions and their specific modifications, implementations and applications thereby transforming data associated with cryptocurrencies. Due to a specific implementation scheme the idea is not abstract.

[0329] It can be easily recognized, by one skilled in the art, that the aforementioned method for personal/client identification and verification may be performed and/or controlled by one or more computer programs. Such computer programs are typically executed by utilizing the computing resources in a computing device. Applications are stored on a non-transitory medium. An example of a non-transitory medium is a non-volatile memory, for example a flash memory while an example of a volatile memory is RAM. The computer instructions are executed by a processor. These memories are exemplary recording media for storing computer programs comprising computer-executable instructions performing all the steps of the computer-implemented method according the technical concept presented herein.

[0330] While the invention presented herein has been depicted, described, and has been defined with reference to particular preferred embodiments, such references and examples of implementation in the foregoing specification do not imply any limitation on the invention. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader scope of the technical concept. The presented preferred embodiments are exemplary only, and are not exhaustive of the scope of the technical concept presented herein.

[0331] Accordingly, the scope of protection is not limited to the preferred embodiments described in the specification, but is only limited by the claims that follow.

What is claimed is:

1. A method for personal/client identification and verification for transactions involving cryptography-based electronic money, the method being executed by a computational server (**101**) configured to operate a computer program functioning as a registration interface (**102**), and the method being characterized in that it comprises the steps of:

providing access to one or more potential or existing currency users (**103**);

providing a registration interface (**102**) for one or more potential currency users to register a user account requiring authentication (**104**);

requesting the submission of documents for proof of the legal identity of a registrant (**105**);

verifying the legal identity of the registrant (**106**);

rejecting an account creation for registrants failing in legal identity verification (**107**);

creating a personal/client account (**108**) for individual successful registrants (**109**) with successful verification of legal identity (**110**);

allowing a successful registrant (**109**) to create a credential (**111**) that comprises an associated authentication (**112**);

storing (**116**) all the submitted information in a client information database (**115**);

sending (**117**) the credential to central approval servers (**401**); and

mapping and storing (**118**) multisignature currency address(es), credential and legal identity of individual registrants.

2. The method of claim **1**, wherein legal identities of owners for individual currency addresses are stored in the client information database.

3. The methods of claim **1**, wherein legal identities of owners for individual currency addresses are stored in the client information database, wherein such information is not accessible to the public, in order to maintain the pseudonymous property of the cryptography-based electronic money (**201**) and its transaction network (**202**).

4. The methods of claim **1**, wherein a user can change user's credential (**111**) to stop coins being transferred out from a stolen main data file of user's currency wallet (**301**).

5. The methods of claim **1**, wherein (i) legal identities of owners for individual currency addresses are stored in the client information database, (ii) any currency addresses that are not generated through the submission of a valid credential to one of the central approval servers (**401**) are not valid, and are not able to receive any coins, and (iii) only valid registered users have a valid credential (**112**).

6. The method according to claim **1** characterized in that the authentication is effected by means of a password protection, two factor authentication or multiple factor authentication.

7. The method according to claim **1** characterized in that it further comprises a step of encrypting the credentials (**114**).

8. The method according to claim **1** characterized in that the credential is a digital, electronic or hardware item which can be used as an authentication mechanism to identify oneself, preferably at least one of: unique pair of digital codes, a unique product key for activing a client wallet software, a constantly changing token which is tied to a physical device that is owned by the user, such as a cellphone or a personalized secure key generating device.

9. A method for creating a cryptography-based electronic money (CBEM) (**201**) and its associated transaction network (**202**), the method being executed by a network of computer programs functioning as nodes (**203**), and the method being characterized in that it comprises the steps of:

installing a node (**203**), which can be a stand-alone computer program or a functional module of a client wallet (**111**), in one or more client computers and/or servers (**204**);

connecting all nodes to form relay nodes of a peer-to-peer network (**205**) through a data transmission network (**206**);

controlling the method for creating at least one unit of the CBEM (**207**);

protecting the ownerships of at least one unit of the CBEM by public/private-key cryptography (**208**);

recording ownerships of at least one unit of the CBEM into a ledger (**209**) using the owners' currency addresses (**313**) (**210**);

verifying ownerships of at least one unit of the CBEM (**211**);

restricting only valid registered users (**109**) to generate one or more valid currency addresses (**313**) to receive at least one unit of the CBEM by verifying the submitted credential (**111**) with one of the central approval servers (**401**) (**212**);

recording transactions of at least one unit of the CBEM into the ledger (**209**) (**213**);

verifying transactions of at least one unit of the CBEM (**214**);

controlling the method for transacting at least one unit of the CBEM (**215**);

incorporating the transaction rules into the programing code of at least one nodes (**216**);

restricting at least one transaction approval rule (**217**), comprising at least one of: requisition of a valid credential (**111**) from the sender, requisition of one or more approval private keys (**406**) from one of the central approval servers (**401**);

allowing only creation of multisignature transactions in pay-to-script-hash format or any other compatible format (**218**);

allowing only creation of multisignature transactions each requiring at least two private keys as signatures (**219**);

allowing only creation of multisignature transactions in the presence of a valid credential (**111**) (**220**);

restricting one of these private keys (**219**) to be an approval private key (**406**) from one of the central approval servers (**221**);

restricting the rest of the private keys (**219**) to be client private keys (**222**), which are encrypted and stored in the client wallet(s) (**301**) (**223**);

sending all transaction requests from the client wallets (**301**) to one of the central approval servers (**401**) to obtain the approval private key for signing the transactions (**224**); and

rejecting all transactions missing any one of the required private keys (**219**).

10. The method of claim **9**, wherein any currency addresses that are not generated through the submission of a valid credential to one of the central approval servers (**401**) are not valid, and are not able to receive any coins.

11. The method of claim **9**, wherein individual transactions can be monitored with a defined rules to identify, record and report suspicious transactions that is likely to be involved in illegal activities, such as money laundering.

12. The method of claim 9, wherein legal identities of owners of individual currency addresses are stored in the client information database. For those transactions suspected of illegal activities (claim 11), identities of their associated senders and receivers will be extracted from the client information database by tracing with the currency addresses of the senders and receivers. Subsequently, the suspicious activities and the associated client information will be reported to government agencies with respect to the regulations and laws in the associated countries.

13. The method of claim 9, wherein the amount of coins own by a valid registered user are completely and easily traceable and trackable by the central governing body (601) through analyzing the transaction records in the transactions database (413). Besides the capability of linking individual currency addresses to their owners, this unique property is contributed by recording unspent coins (if there is any) at the currency address from where the coins have just been sent/spent (322). This unique property allows applications of our system to financial and banking activities, particularly those required third-party auditing.

14. A method for personal/client identification and verification for transactions involving cryptography-based electronic money, the method being executed by a computer program functioning as a client device of a user, and the method being characterized in that it comprises the steps of:

installing a computer program of a client device to function as a client wallet (301) in at least one computer or computational server (302);

serving as one of the relay nodes (205) for relaying information of all CBEM units being generated in the transaction network (202) (303);

serving as one of the relay nodes (205) for relaying all transaction information in the transaction network (202) (304);

serving as one of the relay nodes to verify and confirm all transactions that are broadcasted to the transaction network (202) (305);

generating new coins through contributing to recording any new transaction information into the ledger of all transactions (209) (306);

generating one or more pairs of cryptographic client public key (307) and client private key (308) for receiving and sending coins (309);

storing the client public-private key pairs (items 307, 308) of one or more currency addresses generated by the currency users (310);

serving as a client wallet for the currency users to receive and send coins; (311);

serving as an client wallet to communicate between one of the central approval servers (401) and registered currency users (109) (312);

only generating (314) currency addresses which are multisignature addresses (313);

generating one of more multisignature addresses (313) from the client public key (307) and the approval public key (405) (315);

only storing one or more multisignature addresses (313) in the client wallet (301) for sending and receiving coins (316);

sending one of more multisignature addresses (313) to the client information database (401) for storage and mapping to legal identity of the owner of the address(es) (317);

sending the generated valid multisignature addresses (313) to the central approval servers (401) for storage (318);

submitting a credential (111) of a valid registered users (109) to one of the central approval servers for obtaining approval to generate one or more valid currency multisignature addresses (313) (319);

submitting a credential (111) of a valid registered users (109) to one of the central approval servers for obtaining approval to create one or more valid transactions (items 218, 219, 220, 221, 223) to send coins to one or more currency addresses (320);

allowing only creation of transactions that use multisignature addresses (313) for both sending and receiving the coins (321); and

recording unspent coins (if there is any) into the blockchain at the currency address from where the coins have just been sent (322).

15. A method for personal/client identification and verification for transactions involving cryptography-based electronic money, the method being executed by a computer program in a computational server functioning as a central approval server (401), and the method being characterized in that it comprises the steps of:

communicating (407) with a client wallet (301) to generate one or more valid multisignature currency addresses (313) in the presence of a valid credential;

providing (408) approval public key (405) to the currency wallet to create one or more multisignature addresses (313);

communicating (409) with the client wallet (301) to generate one or more valid transactions (218, 219, 220, 221, 223) to send coins to one or more currency address in the presence of a valid credential;

providing (410) approval private key (406), which are corresponding to the approval public key (405) used in creation of the multisignature address (313), to sign transaction input for one or more valid transactions (218, 219, 220, 221, 223);

providing the most recent private key (411) to sign the whole transaction for one or more valid transactions (412); and

storing (414) transaction information in a transactions database (413).

16. The method of claim 15, wherein the pair of approval public Key (405) and approval private key (406) can be changed manually or automatically in a regular period to avoid leakage of the approval public key and the approval private key to the public. After changing to a new pair of approval key, the old approval private key will be used for signing the transaction input (410), and the new approval private key being used for signing the whole transaction (412).

17. The method according to claim 15, characterized in that the most recent approval private key (411) is the approval private key corresponding to the approval public key (405) used in creation of the multisignature address (313) or another approval private key.

18. The method according to claim 15 characterized in that the step of storing (414) transaction information in a transactions database (413) includes storing a transaction ID, sender's currency address, receiver's currency address, amount of coins being transacted, transaction time and IP addresses of the sender and the receiver's client wallets.

19. The method according to claim **15**, characterized in that the method further comprises a step of verifying the transaction against one or more transaction criteria (**501**, **502**) at the central approval server (**401**).

20. The method of claim **19**, wherein the transaction network (**202**) can be modified to reject any transactions that do not the meet the central transaction criteria (**501**) stored in one of the central approval servers (**401**).

21. The method of claim **20**, wherein the client transaction criteria (**502**) can be defined by a valid registered user to limit his/her own transactions.

22. The method of claim **21**, wherein, provide a practical solution for the issues related to cryptocurrency theft, KYC and AML, while maintaining user privacy.

23. The method of claim **21**, which can be adopted or modified by the central banks or other financial institutions to issue their own digital currencies that are supported by a distributed ledger payment system, but also regulated by a central governing body.

24. The method of claim **20**, wherein the transaction criteria (**501**) can be defined by a central governing body (**601**) to stop suspicious transactions that is likely to be involved in illegal activities, such as money laundering.

25. The method according to claim **15**, characterized in that the one or more transaction criteria (**501**, **502**) include criteria predefined by a central governing body (**601**) and/or the registrant.

26. The method according to claim **15**, characterized in that the method further comprises a step of tracing legal identities of the sender and receiver by mapping their currency addresses in the transaction database and the client information database when needed.

27. A method for personal/client identification and verification for transactions involving cryptography-based electronic money, the method being executed by a set of computer programs functioning as devices of a central governing body and a client device of a user, the method being characterized in that it comprises the steps of:

receiving credentials, of a registrant, comprising at least two factor authentication credentials defining a multisignature;

verifying legal identity of the registrant;

creating a personal/client account (**108**) for an individual successful registrant (**109**) with successful verification of legal identity (**110**) whereas the personal/client account facilitates mapping and storing the multisignature of a currency address and legal identity of individual registrants (**118**);

providing a registrant wallet comprising at least one unit of electronic money;

recording ownerships of the at least one unit of electronic money into a transactions database (**413**) using the registrants' currency address (**313**);

creating a multisignature transaction, in a pay-to-script-hash format or any other compatible format (**218**), each requiring at least two private keys as approval signatures (**219**);

restricting one of these private keys (**219**) to be an approval private key (**406**) from one of central approval servers (**221**);

restricting the rest of the private keys (**219**) to be the registrant's private keys (**222**), which are stored in the client wallet (**301**, **223**);

sending the transaction request from the client wallet (**301**) to at least one of the central approval servers (**401**) in order to obtain the approval private key for signing the transaction (**224**); and

broadcasting the approved transaction messages to all relay nodes in a transaction network (**214**).

28. A system for personal/client identification and verification for transactions involving cryptography-based electronic money, the system comprising:

a central approval server (**401**) configured to execute the method according to claim **15** in order to process client registration requests, client cryptocurrency addresses, cryptocurrency transactions;

wherein:

the central approval server (**401**) is communicatively coupled to a client information database (**404**);

the central approval server (**401**) is communicatively coupled to a transactions database (**413**); and

the central approval server (**401**) is configured to communicate with at least one client device (**414**, **415**) provided with a registrant wallet (**416**, **417**) comprising at least one unit of electronic money, the at least one client device (**414**, **415**) being configured to execute the method according to claim **27**.

29. A non-transitory machine-readable storage medium having instructions embodied thereon, the instructions being executable to cause one or more processors to perform all the steps of the computer-implemented method according to one of claim **1**, claim **9**, claim **14**, claim **15**, or claim **27**.

* * * * *