BLOCKCHAIN BASED CRYPTOCURRENCY WITH REGULATORY MECHANISM

FIELD OF THE PRESENT DISCLOSURE

[0001] The present disclosure relates generally to blockchain technologies and, in particular, to a blockchain based cryptocurrency with a regulatory mechanism permitting censorship and non-fungibility of cryptocurrency for providing control to central authorities for taking action against illicit or unwanted transactions being conducted on the blockchain.

BACKGROUND

[0002] In recent times, blockchain currencies have seen increased usage over traditional fiat currencies by consumers who value anonymity and security. Currencies that use a blockchain, such as cryptographic currencies ("cryptocurrencies"), offer consumers a currency that is decentralized and relatively anonymous and secure in its use. For example, a transaction that is posted to a blockchain may not require any information regarding the sender or recipient of the currency. The blockchain enables cryptocurrency users to hold, send, and receive money online, including clearing and settlement of digital asset trading and distributed computing without having the need for central intermediaries. Therefore, the use of blockchain by cryptocurrencies like bitcoins erases the need for central authorities as well as the need to trust them.

[0003] Despite the emergence of such positive uses, the wider applications of block chain technology are challenged by some misgivings, such as suspected associations of bitcoins and other virtual currencies with money laundering activities and the like. For instance, the Financial Action Task Force (FATF) reported in 2015 on how the founders of Liberty Reserve were able to launder hundreds of millions of US dollars for six years for various criminal organizations using bitcoins. This also expanded to the abusive use of blockchain technology in shadowy trading sites such as the now defunct Silk Road. It has been argued that the primary reason blockchains are associated with cybercrime is the absence of strategic governance to set up agreed rules and to ensure compliance. The moment such governance with policies,

procedures and mechanisms and enforcement are in place, the real societal benefits of blockchains could be achieved.

[0004] However, cryptocurrency blockchains such as those developed by Satoshi Nakamoto (Bitcoin) are inherently designed and implemented to be resistant to any method of censorship. The idea behind such cryptocurrency blockchains is that a user can send money to any address and no central third party can interfere with the user's ability to send and receive money because blockchain does an end run around "trusted third parties". For example, when Wikileaks decided to use Bitcoin as a payment method after the US government shut off Wikileaks' access to payments processors, Satoshi Nakamoto urged Wikileaks to not use Bitcoin (Bitcoin Talk post dated December 05, 2010, 09:08:08 AM); however, Nakamoto could still not stop Wikileaks from using Bitcoin because Bitcoin lacked censorship abilities. This had national security implications for the United States as Wikileaks was able to continue to receive funds to publish sensitive materials that were considered detrimental to the United States.

[0005] As blockchain technology becomes embedded in the finance and financial services industries, cryptocurrencies gain prevalence, and the potential for additional blockchain applications continues to grow; industry participants are likely to face heightened regulatory scrutiny, even as the regulatory landscape shifts and evolves with the technology. With blockchain use cases and applications expanding in scope and number, regulators around the world, including major countries like US, China, Japan and India, have expressed interest in regulating blockchain to protect consumers and the market from fraud and other illegal conduct. Otherwise, as blockchains grow, they become large enough to process illicit transactions that could have severe consequences for national security, global geo-political stability and humanity's ability to control the development of advanced Artificial Intelligence.

[0006] Therefore, there is a need to find new techniques for regulating the implementation of blockchains for cryptocurrencies purposes by central authorities for blocking illicit or unwanted transactions and the like. Documents describing the closest subject matter provide for a number of more or less complicated features that fail to solve the problems described above in an efficient and economical way. None of the documents suggest the novel features of the present disclosure.

SUMMARY

[0007] The present disclosure provides a blockchain which allows implementation of regulations or censorship by creating a regulatory wallet or regulatory wallets in the blockchain, for example, a cryptocurrency blockchain. Such regulatory wallet would be part of the cryptocurrency blockchain and may be owned by a central authority who would be issued the private key to the regulatory wallet. The central authority with the private key for the regulatory wallet would have the ability to move any existing coin from the cryptocurrency blockchain into the regulatory wallet. Once a coin is in the regulatory wallet, the central authority with the private key would also have the ability to spend and/or destroy the moved coin in the regulatory wallet based on its discretion.

[0008] The present disclosure further proposes checks for the central authority, in particular in the central authority's ability to spend and/or destroy the moved coin in the regulatory wallet based on its discretion.

[0009] In the present regulatory mechanism, the regulatory wallet or wallets would be created by a hard code in the blockchain. To implement the present regulatory mechanism, an existing cryptocurrency blockchain would have to "hard fork" to create the regulatory wallet system.

[0010] The foregoing summary is illustrative only and is not intended to be in any way limiting. In addition to the illustrative aspects, embodiments, and features described above, further aspects, embodiments, and features will become apparent by reference to the drawings and the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] For a more complete understanding of example embodiments of the present disclosure, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0012] FIG. 1 illustrates a peer-to-peer network with a plurality of network connected devices connected to the peer-to-peer network in interaction with a blockchain, in accordance with one or more embodiments of the present disclosure; and

[0013] FIG. 2 illustrates a network connected device that may be utilized by a central authority to implement regulatory mechanism in the blockchain of the peer-to-peer network, in accordance with one or more embodiments of the present disclosure.

DETAILED DESCRIPTION

[0014] In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. It will be apparent, however, to one skilled in the art that the present disclosure can be practiced without these specific details. In other instances, apparatuses and methods are shown in block diagram form only in order to avoid obscuring the present disclosure.

[0015] Reference in this specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present disclosure. The appearance of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Further, the terms "a" and "an" herein do not denote a limitation of quantity, but rather denote the presence of at least one of the referenced item. Moreover, various features are described which may be exhibited by some embodiments and not by others. Similarly, various requirements are described which may be requirements for some embodiments but not for other embodiments.

[0016] The embodiments are described herein for illustrative purposes and are subject to many variations. It is understood that various omissions and substitutions of equivalents are contemplated as circumstances may suggest or render expedient, but are intended to cover the application or implementation without departing from the spirit or the scope of the present disclosure. Further, it is to be understood that the phraseology and terminology employed herein

are for the purpose of the description and should not be regarded as limiting. Any heading utilized within this description is for convenience only and has no legal or limiting effect.

[0017] The present disclosure provides a blockchain which allows implementation of regulations or censorship by creating a regulatory wallet or regulatory wallets in the blockchain, for example, a cryptocurrency blockchain. Such regulatory wallet would be part of the cryptocurrency blockchain and may be owned by a central authority who would have the private key to the regulatory wallet. The central authority with the private key for the regulatory wallet would have the ability to move any existing coin from the cryptocurrency blockchain into the regulatory wallet. Once a coin is in the regulatory wallet, the central authority with the private key would also have the ability to spend and/or destroy the moved coin in the regulatory wallet based on its discretion.

[0018] Aspects of the present disclosure will be described in the context of an exemplary system of a plurality network connected devices communicating through the medium of a peer-to-peer network system 100 (hereinafter, sometimes simply referred to as "system 100"), as shown schematically in FIG. 1. As depicted, the network system 100 is embodied within a packet switched based peer-to-peer network 101, through the interconnection of the plurality of network connected devices on a peer-to-peer network 108. A network connected device 102 may connect to the peer-to-peer network 108 through a direct connection to the packet switched network with a wired connection, or through a wireless connection by association with a wireless access point, a cellular base station, a Bluetooth connection, or other means of connection. In an embodiment of the present disclosure, the network connected device 102 may be a device controlled by the central authority as described above.

[0019] Other devices connected the peer-to-peer network 101 may include network connected devices acting as a "standard node" 104, 105 whose role is to maintain a list of other devices connected through the peer-to-peer network 101, and to forward on received network messages to those devices on the list, possibly independently, or possibly as a response to a request from another network connected device. As one skilled in the art will be aware, no individual standard node is required to have a complete list of all devices, as the process of peer-to-peer networking only requires that a union of a set of all standard nodes contains a complete list of all devices on the peer-to-peer network, and for every pair of network connected devices

there is a network route from one device to the other, possibly via a set of one or more nodes. Therefore, the only requirement to be a participant on the peer-to-peer network 101 is to establish a connection to one or more of the standard nodes on said network. Further devices connected via the peer-to-peer network 101 may include one or more network connected devices 106, 107 acting as a validator node, whose role may be to act as a standard node, and may also be to receive transaction messages from the peer-to-peer network 101, process them according to the methods and processes to be described further below, and transmitting the results of said processing back to the peer-to-peer network 101 for inclusion in a distributed ledger.

[0020] The devices described above may each be implemented through a system comprising a one or a plurality of: general purpose microprocessors, digital signal processors (DSPs), application specific instruction set processors (ASIPs), field programmable gate arrays (FPGAs), dedicated application specific integrated chips (ASICs), or other equivalent integrated or discrete logic circuitry and peripheral circuitry, connected to a tangible storage medium containing instructions which when executed effect methods and techniques described below. The techniques additionally, or alternatively, may be realized at least in part by a computer-readable communication medium or record carrier, that carries or communicates code in the form of instructions or data structures and that can be accessed, read, and/or executed by a computer.

[0021] An embodiment of the network connected device 102 is presented in FIG. 2, and is now discussed in further detail. The network connected device 102 may comprise a CPU 202 capable of executing instructions stored in a memory 204, and controlling other peripheral components through drivers 206 stored within the memory 204. Further storage 208 may be present, which may contain a cryptographically secure partition or component 210, where cryptographic keys may be securely stored. In the embodiments of the present disclosure, the cryptographically secure partition 210 is utilized to store the private keys to the regulator wallet (as discussed above) in the blockchain as implemented on the peer-to-peer network system 100. The network connected device 102 may also include an input-output (I/O) device 212 which may be implement by a user, i.e. the central authority for inputting instructions (for example, via a keyboard) and the like. It may be understood that each of the network connected device 102 may be operated by a corresponding central authority, being part of the peer-to-peer network system 100.

[0022] The network connected device 102 may connect to the packet switched network 101 through a network module 214, which may consist of a direct wired connection to the packet switched network through a cable 216. In a different embodiment of the invention, the network module 214 may contain wireless components comprising one or more wireless modules implemented in firmware or hardware, including a wireless local area network (WLAN) unit such as a Wi-Fi adapter utilizing an 802.11 protocol, a wireless wide area network (WWAN) unit such as GSM, LTE, or other cellular wireless data communication system, or a Bluetooth unit. The wireless components may provide network connectivity for the network connected device 102 to the packet switched peer-to-peer network 101 of FIG. 1. Components comprising the network connected device 102 may communicate through a bus 218, which may be implemented as a peripheral component interconnect express (PCIe) bus, a universal serial bus (USB), a universal asynchronous receiver/transmitter (UART) serial bus, a suitable advanced micro-controller bus architecture (AMBA) interface, a serial digital input output (SDIO) bus, or other equivalent interface.

[0023] The present system 100 provides a cryptocurrency blockchain 110 (schematically depicted in FIG. 1) that implements a regulatory mechanism. In the present examples, the regulatory mechanism is defined in the cryptocurrency blockchain 110 in the form of a hard code. In other examples, the regulatory mechanism may also be implemented on existing cryptocurrency blockchain. For this purpose, the existing cryptocurrency blockchain would have to implement a "hard fork" to define the regulatory mechanism therein. The present system 100 with the regulatory mechanism implements censorship on the cryptocurrency blockchain 110, making the present cryptocurrency blockchain 110 "non-fungible." This is in contrast to, for example, the 'Bitcoin' or 'Ethereum' blockchains which are "fungible" because each coin therein has the same properties as every other coin and they are perfectly exchangeable with each other without any censorship.

[0024] The regulatory mechanism is imposed by providing one or more regulatory wallets 112 (as representatively shown in FIG. 1) on the cryptocurrency blockchain 110. A central authority utilizing the network connected device 102 is issued and provided with the private key to the regulatory wallet 112. Herein, the central authority may be trusted central authority, such as a Govt. recognized institute, for example, Federal Reserve or the like. In other

examples, the central authority may be a privately owned business or corporation which may be trusted by the users of the present system 100. Such regulatory wallet 112 may be distinguished from other regular wallets 114 (as representatively shown in FIG. 1) on the cryptocurrency blockchain 110 as any coin in the regular wallets 114 could be moved therefrom to the regulatory wallet 112 based on appropriate permissions, without the need of cryptographic keys associated with those regular wallets 114. Further, the present system 100 allows the central authority to block transactions between any two regular wallets 114 based on its discretion.

[0025] The present system 100 enables the central authority utilizing the network connected device 102 with the private key to the regulatory wallet 112 to censor or block a bilateral transaction in the cryptocurrency blockchain 110, even though the central authority in itself is external party to the bilateral transaction in question as implemented on the cryptocurrency blockchain 110. Thus, the central authority would have censorship rights to restrain the ability of other parties to transact on the cryptocurrency blockchain 110. In the present embodiments, the central authority with the private key of the regulatory wallet 112 would have the ability to move any number of existing coins in the regular wallets 114 into the regulatory wallet 112 in the cryptocurrency blockchain 110. Once a coin is in the regulatory wallet 112, the central authority with the private key would also have the ability to spend and/or destroy the moved coin in the regulatory wallet 112 based on its discretion.

[0026] In one or more examples, the censorship right to, for example, stop a bilateral transaction in the cryptocurrency blockchain 110, may be based on the discretion of the central authority. Herein, the "discretion" may be defined as decision of one or more officers of the central authority. Such discretion may be provided to the central authority by government, judicial branch, legislative branch or the like. Preferably, the discretion may be applied under judicial purview to only those transactions or accounts on the cryptocurrency blockchain 110 which have shown or likely to show involvement in illegal transactions, such as money laundering. In other examples, the censorship right may be based on some predefined algorithms which are implemented on the cryptocurrency blockchain 110. Such predefined algorithms may be designed to find illicit transactions, for example transactions associated with shady accounts, transactions with unusual behavior, etc.; and may automatically block, or at least put the transaction on hold for a human officer to review based on a case-by-case basis, by exercising

the censorship rights. Further, in some examples, limits may be imposed onto the discretion of the central authority; for example, providing rights to block only a limited number of transactions on the cryptocurrency blockchain 110 and the like.

[0027] In the present examples, the central authority with the private key for the regulatory wallet 112 would more or less act as a monetary authority that could use the cryptocurrency blockchain 110 to limit or possibly mitigate any instance of illicit transactions thereon. In the present examples, the system 100 may implement several different regulatory wallets 112 on the cryptocurrency blockchain 110 which can be created for different government regulating agencies. For example, the US Department of Justice can control one regulatory wallet to implement forfeitures related to proceeds of crime; the US Treasury Executive Office for Asset Forfeiture can control another regulatory wallet to implement the Treasury Forfeiture Fund; intelligence agencies and arms of the military could control their own regulatory wallets to limit the spread of artificial intelligence activity on the blockchain or to confiscate a wartime enemy's coins. No private key for one of the regulatory wallet 112 would be able to move or spend a coin that is inside another of the regulatory wallet 112 not controlled by that regulatory wallet's own private key. That is, the US Treasury would not be able to spend a coin in the US Department of Justice's regulatory wallet, and vice-versa.

[0028] In some embodiments, the present system 100 may implement a master regulatory key which would be able to access any coin in the one or more regulatory wallets 112 in the cryptocurrency blockchain 110. A trusted central monetary authority (such as, the Federal Reserve) may be issued such master regulatory key. The trusted central monetary authority could use this master regulatory key to keep all the agencies, that have the ability to confiscate coins, under check. This function keeps peace among agencies that have access to regulatory wallet keys and assigns one agency; in this case, the trusted central monetary authority, as a supervisor for the entire system 100. Therefore, the trusted central monetary authority could use this master regulatory key to keep the present system 100 functional and reputable without the delay of due process. In one implementation the master regulatory key would be designed such that it is controlled by a "one-time pad," as known in the art.

[0029] The present system 100 further provide remedies in case of somebody's coin was accidently or improperly added to a regulatory wallet 112. In the present implementations,

the redress would be obtainable outside of the cryptocurrency's technique; for example, via judicial review under administrative law. That is, the owner of the regular wallet 114 whose coins may have been moved into one of the regulatory wallets 112 could appeal in Civil Courts to provide evidence related to legal status of the moved coins and thereby may get relief from the Court in the form of releasing of the moved coins back into the owner's regular wallet 114. In such case, the Court may direct either the concerned central authority of the regulatory wallet 112 to take the action for releasing of the moved coins, or may direct the trusted central monetary authority to use its master regulatory key for taking the same action.

[0030] Alternatively, remedy from the Civil Courts may be perceived to be harmful to a cryptocurrency. That's because cryptocurrencies essentially permit a-legal non-justiciable transactions whose primary use value is their ability to by-pass legally-entrenched trusted third parties, by acting in a purely peer-to-peer manner. In an embodiment, an alternative to remedy through the civil courts that maintains the non-justiciable nature of transactions may involve that a dispute is heard by an extra-juridical tribunal that solely has the ability to request that a regulatory authority make an ex-gratia payment to the aggrieved party, providing no ability to juridically order regulatory authorities to do anything. Furthermore, the central authority may be controlled by an intelligence agency that has the ability to place the central authority outside the competent jurisdiction of the courts.

[0031] It will be appreciated that the present system 100 can be alternatively implemented with only one regulatory wallet or with many regulatory wallets without any limitations. In one implementation, the system 100 could be implemented as having one or more regulatory wallets 112 with the corresponding private keys assigned to the concerned central authorities, and no master regulatory key may be issued. In an alternate implementation, the system 100 could be implemented having regulatory wallets 112 but with no corresponding private keys issued to any central authority, but having only one master regulatory key issued and provided to the trusted central monetary authority which overlooks the entire system 100. In such second implementation, the central authorities may approach the trusted central monetary authority to take action related to blocking of any transaction or confiscating of existing coins from any regular wallet 114, if needed. In addition, each regulatory wallet, not just the central authority, can be controlled by a one-time pad, as discussed above.

[0032] The system 100 of the present disclosure can also be implemented as a "box" for an artificial intelligence (AI) bot or the like which could possibility develop as a financially involved AI on a blockchain; or, in other words, where the blockchain may be the "substrate" for AI. It may be appreciated that a blockchain is an artificial time, a "mode of irreversibility." Credentials on the blockchain are just avatars; and these avatars may be the prime assets and "identity" of such artificial intelligence. On the blockchain, AI doesn't need don't need to pass a KYC/AML check to send and receive money, to hire human labor, to accumulate capital, finance undertakings or exchange and underwrite securities. To the blockchain, an AI's avatar is indistinguishable from a human's avatar. Thus, it is entirely possible that a particular AI could take control over some vital blockchain to develop in a manner that is averse to humanity. As discussed, the present system 100 could be implemented as a "box" for such artificial intelligence. The present blockchain 110 with the regulatory wallet 112 allows humans to regulate the development of AI by controlling the number of possessed coins thereby. The regulatory wallet 112 as proposed in the present system 100 provides humans with ontological discretion to guide the evolution of AI and could be vital to save humanity from existential threat of malicious AI.

[0033] The foregoing descriptions of specific embodiments of the present disclosure have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed, and obviously many modifications and variations are possible in light of the above teaching. The exemplary embodiment was chosen and described in order to best explain the principles of the present disclosure and its practical application, to thereby enable others skilled in the art to best utilize the present disclosure and various embodiments with various modifications as are suited to the particular use contemplated.

ABSTRACT

The present disclosure provides a blockchain which allows implementation of regulations or censorship by creating a regulatory wallet or regulatory wallets in the blockchain, for example, a cryptocurrency blockchain. Such regulatory wallet would be part of the cryptocurrency blockchain and may be owned by a central authority who would have the private key to the regulatory wallet. The central authority with the private key for the regulatory wallet would have the ability to move any existing coin from the cryptocurrency blockchain into the regulatory wallet. Once a coin is in the regulatory wallet, the central authority with the private key would also have the ability to spend and/or destroy the moved coin in the regulatory wallet based on its discretion.

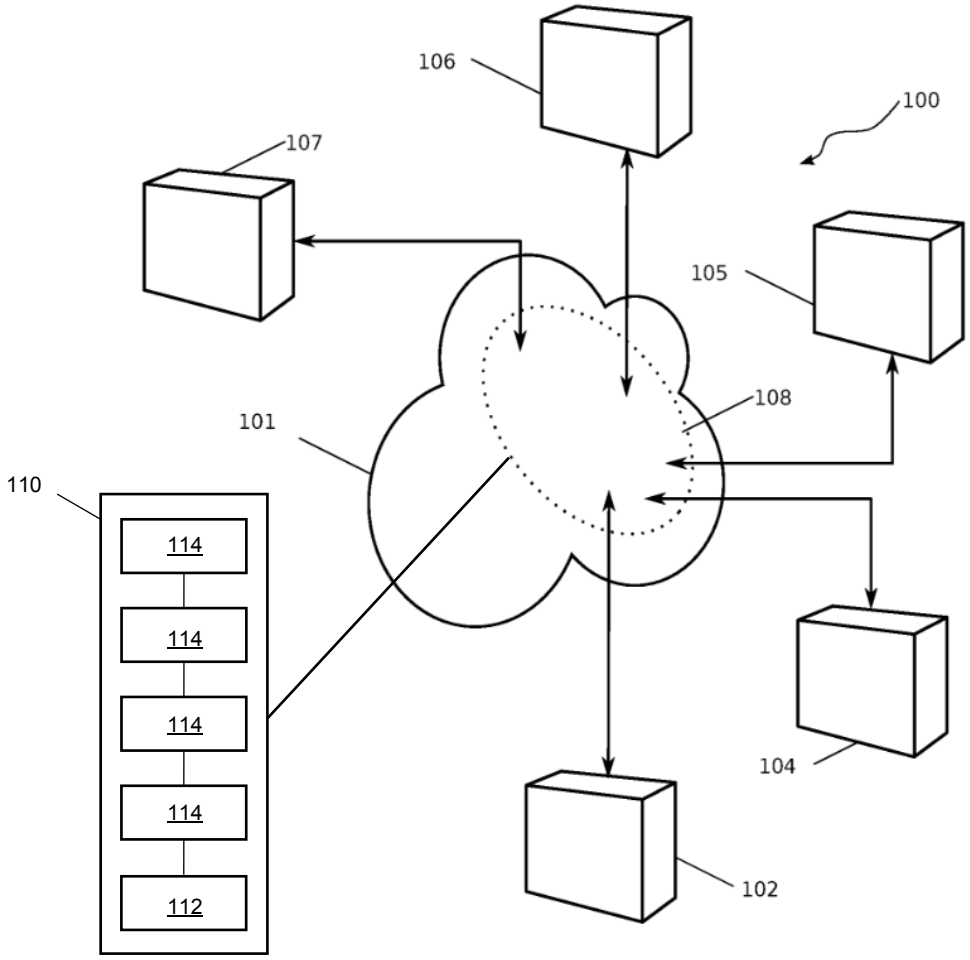

FIG. 1

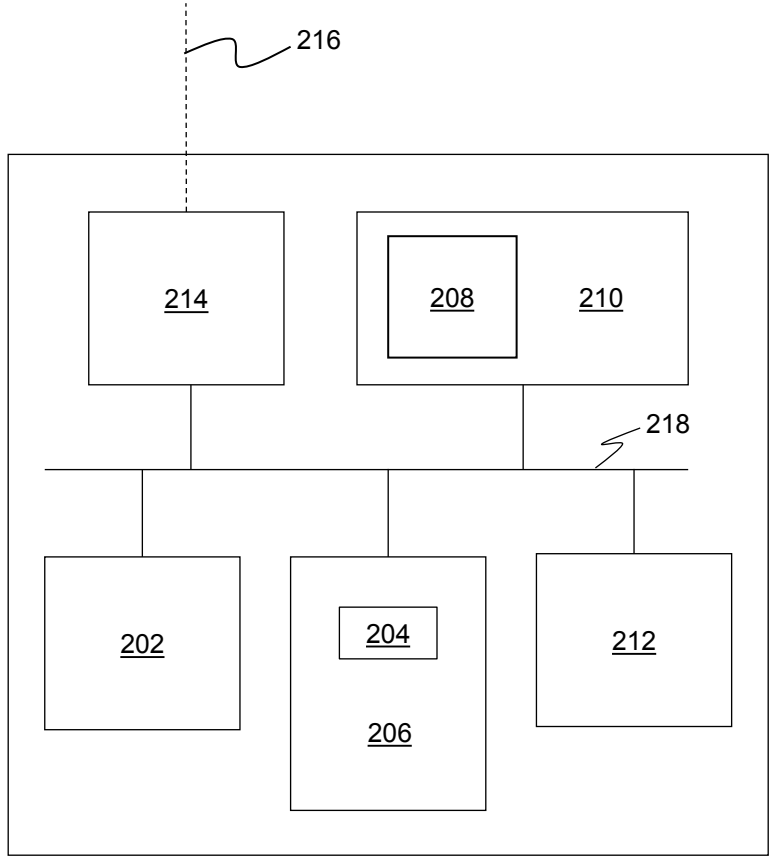

FIG. 2

PTO/SB/16 (01-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 1 of 2

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. _____

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Rami Nader	Tabello	Toronto, Canada

Additional inventors are being named on the _____ separately numbered sheets attached hereto.

TITLE OF THE INVENTION (500 characters max):

BLOCKCHAIN BASED CRYPTOCURRENCY WITH REGULATORY MECHANISM

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☒ The address corresponding to Customer Number: 154677

OR

☐ Firm or Individual Name

Address

City	State	Zip
Country	Telephone	Email

ENCLOSED APPLICATION PARTS (*check all that apply*)

☒ Application Data Sheet. See 37 CFR 1.76.
☐ CD(s), Number of CDs _____
☒ Drawing(s) *Number of Sheets* 02
☐ Other (specify) _____
☒ Specification (e.g., description of the invention) *Number of Pages* 12

Fees Due: Filing Fee of $280 ($140 for small entity) ($70 for micro entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is $400 ($200 for small entity) ($100 for micro entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant asserts small entity status. See 37 CFR 1.27.
☒ Applicant certifies micro entity status. See 37 CFR 1.29.
Applicant must attach form PTO/SB/15A or B or equivalent.
☐ A check or money order made payable to the *Director of the United States Patent and Trademark Office* is enclosed to cover the filing fee and application size fee (if applicable).
☒ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: _____.

70
TOTAL FEE AMOUNT ($)

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 10 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/16 (01-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 2 of 2

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

- [x] No.
- [ ] Yes, the invention was made by an agency of the U.S. Government. The U.S. Government agency name is: _____

_____

- [ ] Yes, the invention was made under a contract with an agency of the U.S. Government. The name of the U.S. Government agency and Government contract number are: _____

_____

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

SIGNATURE _____ DATE 2018-10-23

TYPED OR PRINTED NAME Jinggao Li REGISTRATION NO. 64450 (*if appropriate*)

TELEPHONE 203-916-7016 DOCKET NUMBER 32000.006USP

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	34170488
Application Number:	62753907
International Application Number:	
Confirmation Number:	1708
Title of Invention:	BLOCKCHAIN BASED CRYPTOCURRENCY WITH REGULATORY MECHANISM
First Named Inventor/Applicant Name:	Rami Tabello
Customer Number:	154677
Filer:	Jinggao Li
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	31-OCT-2018
Filing Date:	
Time Stamp:	23:45:04
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$70
RAM confirmation Number	110118INTEFSW23474100
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		1_32000_006USP_Provisional_Specification.pdf	209803 ecb96e1b7b22524300c2f37ae36ae03fe1af33ae	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Abstract	12	12
	Specification	1	11

Warnings:

Information:

2	Drawings-only black and white line drawings	2_32000_006USP_Drawings.pdf	80114 ded5b3feb82a9d0d1ac36558088d99e617ef70ed	no	2

Warnings:

Information:

3	Provisional Cover Sheet (SB16)	3_32000_006USP_Provisional_Application_for_Patent_Cover_Sheet.pdf	176558 c1ebe0638a78e5e8d8ea01a5188a4b5b686812cb	no	3

Warnings:

This is not a USPTO supplied Provisional Cover Sheet SB16 form.

Information:

4	Application Data Sheet	4_32000_006USP_ADS.pdf	108146 1ddc7c1e30113fb69964ca235b1303498b18598f	no	8

Warnings:

Information:

This is not an USPTO supplied ADS fillable form

5	Oath or Declaration filed	5_32000_006USP_Declaration.pdf	1069014 5e088262846654e6a9b67365ef17f63096875aaf	no	2

Warnings:					
Information:					
6	Certification of Micro Entity (Gross Income Basis)	6_32000_006USP_Micro_entity_status.pdf	111231 089d4603147cc62b69c7997d3ff01647feb3ed5d	no	2
Warnings:					
Information:					
7	Power of Attorney	7_32000_006USP_POA.pdf	2005477 84ee0085ff939669c6b94a3e8b38e771503f4eb1	no	4
Warnings:					
Information:					
8	Fee Worksheet (SB06)	8_32000_006USP_Fee_Transmittal.pdf	158518 c3e9c5a088af21f2662a6981aae99a974db1e477	no	2
Warnings:					
Information:					
9	Transmittal of New Application	9_32000_006USP_Transmittal_Form.pdf	187036 1996e2c6efb1e8083cbf35b2396d0ec6e0a3d1a1	no	2
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	29522 e5360f17d814f0a43a70ac424f2abe54b01e1620	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	4135419	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.