



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
61/990,795	05/09/2014		130	uc-lc-prov1		

CONFIRMATION NO. 8467

94276
Matthew Bogosian
215 Reservation Road
O-114
Marina, CA 93933

FILING RECEIPT



Date Mailed: 05/19/2014

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Reginald C. Middleton, New York, NY;
Matthew T. Bogosian, Marina, CA;

Applicant(s)

Reginald C. Middleton, New York, NY;
Matthew T. Bogosian, Marina, CA;

Power of Attorney:

Matthew Bogosian--69710

If Required, Foreign Filing License Granted: 05/16/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/990,795**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

SYSTEMS AND METHODS FOR LOW TRUST AND ZERO TRUST TRANSACTIONS

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

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)
Reginald C.	Middleton	New York, NY
Matthew T.	Bogosian	Marina, CA

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

TITLE OF THE INVENTION (500 characters max):

SYSTEMS AND METHODS FOR LOW TRUST AND ZERO TRUST TRANSACTIONS

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☒ The address corresponding to Customer Number: 94276

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* 12
☐ Other (specify) _____

☒ Specification (e.g., description of the invention) *Number of Pages* 60

Fees Due: Filing Fee of \$260 (\$130 for small entity) (\$65 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.
 130

☐ 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).
 TOTAL FEE AMOUNT (\$)

☒ 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: _____.

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.

Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

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.



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.

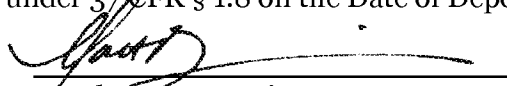
SIGNATURE /Matthew T. Bogosian/ DATE May 9, 2014
TYPED OR PRINTED NAME Matthew T. Bogosian REGISTRATION NO. 69,710
(if appropriate)
TELEPHONE +1.831.824.4442 DOCKET NUMBER uc-lc-prov1

I hereby certify that this paper or fee is being filed with the United States Patent and Trademark Office via EFS-Web under 37 CFR § 1.8 on the Date of Deposit indicated below.

Signed:

Name:

Date of Deposit:


Matthew T. Bogosian
May 9, 2014

PROVISIONAL PATENT APPLICATION

SYSTEMS AND METHODS FOR LOW TRUST AND ZERO TRUST TRANSACTIONS

COPYRIGHT STATEMENT

[1] All material in this document, including the figures, is subject to copyright protections under the laws of the United States and other countries. The owner has no objection to the reproduction of this document or its disclosure as it appears in official governmental records. All other rights are reserved.

TECHNICAL FIELD

[2] Related technical field(s) are: telecommunications, digital communications, and computer technology.

BACKGROUND ART

[3] Market efficiency tends to increase—and therefore transaction costs tend to decrease—in proportion to the degree that transacting parties trust each other. However, rent extraction tends to increase—and therefore trust decreases—in proportion to market size.¹ Efficient and productive participation in larger markets therefore requires mitigating trust issues, but that comes at a cost. That cost can often be reduced by economies of scale, but even today, there is substantial overhead from buffering against risks introduced by counterparties, intermediaries, post-delivery payment failures, guarantor failures, escrow, etc.

[4] Since the mid nineties, there has been an explosion of commercial activity where parties previously unknown to each other agree to transact using the internet as the fundamental communication medium, sometimes even across international borders. Establishing and maintaining trust between those parties has played a central role, and various crude solutions based on traditional, but inefficient methods have been attempted (e.g., electronic exchanges with expensive fees, “online” escrow and dispute resolution using third parties, various reputation systems, third party guarantors, etc.).

¹ Rose, David C. The Moral Foundation of Economic Behavior. New York: Oxford UP, 2011. Print.

[5] Among those markets where individuals interact are those which trade financial instruments (e.g., stocks, bonds, options, futures, swaps, currency exposure, etc.). With the advent of financial engineering, individuals and businesses have been able to leverage computing in financial trading, including automating the process of entering and exiting trades based on programmable conditions or algorithms. However, even with the explosion of the use of technology in this space, such technology is overwhelmingly layered on top of legacy centralized markets. Nearly all impose relatively large costs to conduct trades with counterparties. Some very high-volume exchanges sell the ability for “high value” (i.e., high-paying) customers to cut in line ahead of less savvy or less well equipped investors. Some have questioned the fairness of this practice.

[6] Further, the cost of contract enforcement in international trade can be prohibitive, and success might be very difficult to predict. In addition, a seller may wish to receive one currency, and a buyer may wish to send another. The value of one currency denominated in another can be volatile. Historically, one way that remote parties have mitigated risk is to engage the assistance of trusted intermediaries. One such mechanism is a letter of credit (L/C). L/Cs are appropriate where a seller does not know whether to trust a buyer wishing to place a large order, but does trust a bank where the buyer has established a line of credit. The buyer and bank agree that the bank will release funds from that line of credit to the seller when the seller meets certain conditions (most often transmitting evidence of shipment to the bank before a certain date). The bank provides the promise (L/C) to the seller, and the seller and buyer agree on the remaining terms of the transaction. However, payment often happens at a later date than the agreement, and exchange rates could vary between the time that the agreement was struck and the time payment is received. Only the largest of institutions have the resources necessary to properly hedge against exchange rate volatility. Additionally, the fees charged by banks for L/Cs and currency exchanges are substantial. Perversely, a high degree of trust must also be placed in the intermediary institution(s), who effectively acts as self-interested document examiners who may or may not independently verify the veracity of said documents before releasing the funds, perhaps leaving much of the risk of mistake, forgery, or fraud on the shoulders of the seller. As such, L/Cs are typically not well-suited for consumer transactions, or where transactions involve currencies whose values may vary wildly in relation to each other.

[7] So-called “cryptocurrencies”—technologies that promise tightly-controlled asset creation coupled with the ability to transfer control or ownership of those assets computationally when rigorously-defined criteria are met, with little-or-no dependency on third party intermediaries,

and with very low transaction costs compared to traditional mechanisms—are relatively new creatures. The Bitcoin protocol and progeny (Ethereum, Litecoin, etc.) are one such class of technologies that have recently enjoyed meteoric rises in popularity (and valuation).

[8] For the purposes of illustration by way of example, those particular cryptocurrencies generally operate by maintaining a whole or partial history of all verified transactions. With few exceptions beyond the scope of the invention, transactions function roughly as follows.² A transaction comprises at least one output and at least one input. The output comprises an output “script”, which comprises an ordered set of well-defined executable operations. The input comprises an input script, which comprises a second ordered set of such operations. A new (child) transaction comprises an input whose input script is combined with the output script from an existing (parent) transaction in a predictable way. Said new transaction is considered valid if others agree the combination, when evaluated, produces an anticipated state or result. A transaction output is considered “spent” if it is accepted by others as associated with a valid child transaction. A transaction output is considered “unspent” if it is not accepted as associated with any valid child transactions. The concept of “ownership” or “title” of a transaction output is determined by which entity may exercise control over said output, or, more specifically, who may create and/or expose new transactions to “spend” said output that will be accepted by others as valid.

[9] A transfer occurs when an entity produces a new child transaction that is accepted by others as valid, and whose input is associated with an output from a parent transaction. In most cases, this is a simple transfer of control to a second entity, where the new transaction’s output script is a small set of operations for which creating a corresponding input script is computationally simple for a single entity in possession of a particular asymmetric cryptography key pair, and computationally impractical for all others. In other words, it is “addressed” to an entity with access to a particular private key. Existing software abstracts these addresses and simple transactions sufficiently for laypersons to engage in them without being programmers or protocol experts.

[10] However, many more complex scripts—and therefore transactions—describing conditions under which a set of asset transfers takes place are contemplated by the set of available operations. Because the general means of describing those operations is typically

² This is an oversimplification of the Bitcoin protocol, but it is sufficient for the purposes of this disclosure. More detailed information may be found on the Bitcoin Wiki <<https://en.bitcoin.it/>>. Details regarding the Ethereum protocol may be found on the Ethereum Wiki <<https://github.com/ethereum/wiki/wiki>>.

binary or programming code³, arbitrary transactions cannot generally be created or understood by laypersons. For example, as of April 21, 2014, the Bitcoin Contracts Wiki page comprises brief instructions for several theoretical “example” transactions.⁴ In each, irrespective of role in the transaction, laypersons are unlikely able to understand—much less follow—these instructions. Fundamental steps are missing that would enable them to confidently conduct similar transactions, much less combinations of such transactions. Despite its great potential, this kind of complexity without abstraction has likely frustrated adoption of the Bitcoin protocol and progeny for anything besides “simple” payments in traditional markets.

SUMMARY OF INVENTION

[11] The invention pertains to systems and methods enabling parties with little trust or no trust in each other to enter into and enforce agreements conditioned on input from or participation of a third party, over arbitrary distances, without special technical knowledge of the underlying transfer mechanism(s), optionally affording participation of third-party mediators, substitution of transferors and transferees, term substitution, revision, or reformation, etc. Such transactions can occur reliably without involving costly third-party intermediaries who traditionally may otherwise be required for such transactions, and without traditional exposure to counterparty risk.

[12] This application explores example embodiments enabling arbitrary swaps and L/Cs. Arbitrary swaps and L/Cs are useful illustrative examples because traditionally the two are very different animals. However, the invention allows for their expression and enforcement in remarkably similar terms. As one skilled in the art will appreciate, the invention can be applied to many other agreement structures as well.

[13] In one example, Party A believes that bitcoins (BTC) will rise in notional terms when valued in New Zealand dollars (NZD) over the next few weeks. Party B believes the opposite is true, that BTC will fall when valued in NZD over a similar timeframe. Neither parties are aware of each other, but each wants to place a small bet in accordance with saidrespective beliefs. One embodiment of the invention allows those parties to discover each other, collaborate with each other to agree on concrete terms, propose transactions reflecting their agreement, and finally enforce that agreement without traditional, costly measures.

3 See, e.g., “bitcoind - How Can I Create a Multi Signature 2-of-3 Transaction?” StackExchange, 23 Mar. 2014. Web. 21 Apr. 2014. <<https://bitcoin.stackexchange.com/questions/3712/how-can-i-create-a-multi-signature-2-of-3-transaction>>.

4 Hearn, Mike. “Contracts.” Bitcoin. Bitcoin Community, 9 Apr. 2014. Web. 21 Apr. 2014. <<https://en.bitcoin.it/wiki/Contracts>>.

[14] In another example, Party A is a merchant who wishes to allow her customers to trade their BTC for her services. However, she would rather receive US dollars (USD) because she is concerned about the volatility of BTC. Party A is not concerned about whether BTC will rise or fall when valued in USD. Periodically (e.g., once per day, hour, etc., or even once per transaction where she receives BTC), she can offer to sell exposure to BTC valued in USD in proportion to the BTC she receives from her customers. In other words, she swaps her exposure to BTC in exchange for exposure to USD. Party B has fewer BTC and more USD than he wants, and desires increased exposure to BTC valued in USD. One embodiment of the invention allows Party B to find and exchange—or “swap”—exposures with Party A, allowing Party A to accept BTC in exchange for her goods or services knowing that she will be compensated by Party B if her BTC lose value against USD, in exchange for Party B being able to keep any upside if BTC gains in value against USD. Another embodiment seeks out these swaps automatically upon detection of Party A’s ownership of additional BTC.

[15] Combinations are possible. For example, Party A accepts Australian dollars (AUD), but prefers USD, and wants to hedge against volatility of AUD in USD. One embodiment of the invention allows Party A to swap exposure to USD in BTC with Party B, and simultaneously swap exposure to BTC in AUD with Party C over a similar time period, thereby synthesizing a hedge against AUD in USD. The invention is not limited such that Party B and Party C are distinct parties (they could be the same), nor is it limited such that Party A must conduct two separate trades. In addition, various embodiments of the invention allow the parties to perform these types of transactions without maintaining currency deposits or making currency purchases or exchanges.

[16] In yet another example, Party A wishes to purchase goods from Party B. The parties do not know each other well. Party B wants assurances of availability of funds from Party A, but Party A does not want to release those funds to Party B (or an assignee) until Party B has demonstrated proof of shipment (or met some other condition)

[17] In one embodiment comprising a swap, a first client and a second client participate in a series of transactions where assets from a first party and assets from a second party are committed until a combination of two of the first party, the second party, and an intermediary release them in accordance with a calculation by the intermediary based on observation of external state, such as the relative value of certain assets at a specific time.

[18] In another embodiment comprising an L/C, a first client and a second client participate

in a series of transactions where assets from a first party are committed until either the first client or an intermediary releases them based on observation of external state, such as verification of delivery to a shipper or an address.

[19] In a further embodiment, the assets may be refunded if no such observation can be made by an expiration time.

[20] In yet another embodiment, the commitment of assets may be extended pending a settlement facilitated by a mediator.

BRIEF DESCRIPTION OF THE DRAWINGS

[21] FIG. 1 depicts a typical embodiment for practicing the invention, especially for use with or comprising a distributed transfer mechanism, where the clients, transfer mechanism, facilitator, and oracle data source are distinct participants, and where the facilitator comprises the oracle.

[22] FIG. 2 depicts aspects of one embodiment pertaining to a swap comprising one or more source transactions and a commit transaction.

[23] FIG. 3 depicts aspects of one embodiment pertaining to a swap comprising a commit transaction and a refund transaction.

[24] FIGS. 4-5 depict aspects of swap embodiments comprising relatively simple disbursement transactions in a swap situation involving principal and collateral.

[25] FIGS. 6-7 depict transaction chains from various example swap embodiments where one party wishes to exit before termination, but cannot secure an agreement from the counterparty, but is able to find a party willing to stand in place of the party wishing to exit.

[26] FIG. 8 depicts aspects of one embodiment pertaining to an L/C comprising a source transaction and a commit transaction.

[27] FIG. 9 depicts aspects of one embodiment pertaining to an L/C comprising a commit transaction and an expiration transaction.

[28] FIGS. 10-11 depict aspects of L/C embodiments comprising relatively simple disbursement transactions in a situation involving principal and collateral.

[29] FIGS. 12-14 depict transaction chains from various example L/C embodiments

comprising substitutions of parties.

[30] FIGS. 15-16 depict aspects of embodiments where the agreeing parties have designated a mediator to resolve any dispute that may arise.

DESCRIPTION OF THE EMBODIMENTS

[31] The invention is not limited to the following embodiments. The description that follows is for purpose of illustration and not limitation. Other systems, methods, features and advantages will be or will become apparent to one skilled in the art upon examination of the figures and detailed description. It is intended that all such additional systems, methods, features, and advantages be included within this description, be within the scope of the inventive subject matter, and be protected by the accompanying Claims.

[32] For example, the Bitcoin protocol is often used in this application as an illustrative vehicle. However, the invention is not limited by the Bitcoin protocol specifically. Any technology making it sufficiently difficult to re-characterize ownership of assets (virtual or otherwise) unless certain rigorously-defined criteria are met may be substituted. The invention is not limited to decentralized or centralized transfer mechanisms. For example, in one embodiment transactions could be recognized (i.e., facilitated) by an authority (centralized). In another embodiment, they could be validated by election (distributed), etc.

[33] Further, while the Bitcoin protocol explicitly identifies “inputs” and “outputs” for transactions, the invention is not limited to such transfer mechanisms. Various embodiments of the invention may be practiced in any context in which ownership of an asset can be re-characterized, provided the transfer mechanism exposes the necessary features. This application uses “input” and “output” both literally (e.g., with respect to technologies like the Bitcoin protocol) as well figuratively (e.g., with other technologies such as those modeled after double-entry accounting, chain-of-title, etc.). In a more traditional model, for example, an “input” might comprise an amount of some or all of an available “balance” in an “account” under one entity’s direction or control (e.g., at a traditional bank). An output might comprise a reference to another entity’s account (e.g., an account number). In such a model, recharacterization of assets occurs when—once certain conditions are met—the balance of the first entity’s account is decremented and (preferably atomically) the balance of the second entity’s account is incremented. This is but one example of alternative transfer mechanisms with which the invention may be practiced.

[34] In addition, this application may disclose or imply aspects of the invention comprising a “display”, an “input”, a “display device”, an “input device”, or similar term. However, this invention is not limited to being practiced only by persons with common natural abilities. “Display [device]” is intended to comprise any device capable of unambiguously communicating information to a human being via any of the senses, or combinations of senses. For example, blind persons could use the device with an “audio display”, which may comprise a text-to-speech synthesizer. Alternately, a braille terminal could be used. Similarly, “input [device]” is intended to comprise any device capable of receiving information from a human being. Modernly, popular input devices comprise a keyboard, a mouse, a touch screen, etc., but could be a speech-to-text converters, sip-and-puff devices, click-and-type devices, motion or gesture recognition devices, etc. These are but a few examples. A diversity of such display and input devices are known in the art and may be used when practicing the invention, as will become apparent to one skilled in the art.

[35] In the embodiment depicted in FIG. 1, the invention comprises some or all of the depicted participants on a computer network (not depicted). The participants comprise a first client (A) typically operated for a first party (not depicted) coupled to the computer network (either persistently or intermittently), a second client (B) typically operated for a second party (not depicted) coupled to the computer network (either persistently or intermittently), a transfer mechanism accessible via the computer network, a facilitator accessible to the computer network, optionally an oracle, and optionally an oracle data source accessible by the oracle. In a typical embodiment, the computer network comprises the internet, but this is not a requirement. Other configurations are possible. For example, multiple, independent computer networks can be used for connecting any subset of the participants, including private networks, VPNs, secure tunnels, frame relays, etc. Any computer networking technology will suffice so long as it affords communication between the various participants during times consistent with the invention.

[36] In a typical embodiment, each of the first client, the second client, and the facilitator comprises a computer processor configured to perform certain steps within the scope of the invention. In some embodiments, the oracle comprises a computer processor. In other embodiments, such as those using the Ethereum protocol as the transfer mechanism, one or both of the facilitator and the oracle comprise instructions for computation which are evaluated by participants in a proof of work protocol, in which case a participant comprises a computer processor configured to evaluate the instructions for computation. In many embodiments, a

client comprises a display device and an input device for interacting with a human being, but this is not strictly necessary. In other embodiments, a client could be fully automated, requiring no human intervention. In one such embodiment, the computer processor of the first client is configured to monitor aspects of the transfer mechanism, the facilitator, the oracle, or the second client, and is configured to interact automatically with the various participants based on an observed change of state.

[37] For example, in one embodiment, the transfer mechanism comprises the Bitcoin protocol, and each of the clients, and the facilitator comprises a non-transitory data store for storing key pairs, inchoate transactions, etc. The first client is configured such that when it observes that it acquires new ownership of BTC, it initiates an offer via the facilitator to trade exposure to one asset or asset class (e.g., BTC) in exchange for exposure to another asset or asset class (e.g., USD).

[38] FIG. 1 depicts a typical embodiment for practicing the invention—especially for use with a distributed transfer mechanism—where the clients, transfer mechanism, facilitator, and oracle data source are distinct participants, and where the facilitator comprises the oracle. However, the depicted arrangement is not the only one contemplated by the invention. In an alternate embodiment, the facilitator provides some or all aspects of the transfer mechanism. In another embodiment, the facilitator comprises some or all aspects of a client. For example, part or all of a client's data store, the ability to initiate or accept offers, etc., could be “embedded” in the facilitator, thereby enabling the facilitator to operate as a client itself (e.g., one controlled by the owners of the facilitator, or on behalf of a third party who has entrusted control to the facilitator). In yet another embodiment, the facilitator is separate and distinct from the oracle. Alternately, the oracle could comprise its own data source. Many configurations are contemplated by the invention are possible, and will become apparent to one skilled in the art.

[39] FIG. 2 depicts aspects of one embodiment pertaining to a swap comprising one or more source transactions and a commit transaction. As depicted, the commit transaction comprises a first input for accepting a first amount from a first source transaction (i.e., from a first party), a second input for accepting a second amount from a second source transaction (i.e., from a second party), and one or more outputs for directing portions of those amounts to one or more other transactions (not depicted), where the first amount and second amount total an expected amount. In many cases, the first and second amounts are equivalent, but not necessarily. In some cases the amounts comprise a principal amount (P), and (optionally) a collateral amount

(C), as depicted in the various figures.

[40] In a typical embodiment, the commit transaction is configured such that some or all of the amounts available via its output(s) may only be transferred with confirmation from at least two of the first party, the second party, the facilitator, and optionally a third party (such as a mediator). In an alternate embodiment, the commit transaction is configured such that some or all of the amounts available via its outputs may only be transferred with confirmation from one of the facilitator and optionally a trusted third party, and one of the first party and the second party. In another alternate embodiment, the commit transaction is configured such that some or all of the amounts available via its outputs may only be transferred with confirmation from either the facilitator or two of the first party, the second party, and optionally a trusted third party. These are non-limiting examples. In addition to the examples presented herein, commit transactions may be configured such that outputs vest ownership in a conjunction of any number of parties, somewhat analogous to a checking account where checks must be signed by two authorized parties in order to be honored.

[41] While a first source transaction and a second source transaction are depicted in FIG. 2, this should not be construed as a limitation of the invention. Amounts may be input into the commit transaction from any number different sources. Excesses may be refunded back to respective parties, or different parties altogether. The only limitation is that the commit transaction comprises inputs totaling at least the expected amount. In some embodiments, fees (not depicted) may be imposed for directing the amounts from their respective sources to said inputs, which may require adjusting the source transactions to compensate for those fees. For example, transfer mechanisms may impose transfer fees, withdrawal fees, wire fees, etc. The Bitcoin protocol, for example, may require a “mining fee” in order to ensure timely processing of the transfer.

[42] FIG. 3 depicts aspects of one embodiment pertaining to a swap comprising a commit transaction and a refund transaction. The commit transaction comprises a first input for receiving a first principal amount (P_A), a second input for receiving a second principal amount (P_B), and a commit output. The refund transaction comprises an input for receiving an amount from the commit output, a first refund output to the first party, and a second refund output to the second party. In a typical embodiment, the refund transaction is not created until well after the commit transaction, or created such that it is only valid after a certain time in the future and only if the commit output has not yet been spent. This allows another transaction to come before

it and spend the commit output, but if no such other transaction is created, the refund transaction can put the parties back in or close to their original positions.

[43] FIGS. 4-5 depict aspects of swap embodiments comprising relatively simple disbursement transactions in a swap situation involving principal and collateral. In FIG. 4, the commit transaction comprises a first joined principal and collateral input from a first party and a second joined principal and collateral input from a second party. In FIG. 5, the commit transaction comprises a first principal (P_A) input from a first party, a first collateral (C_A) input from the first party, a second principal (P_B) input from a second party, and a second collateral (C_B) input from the second party. These are but two of many possible configurations that will become apparent to one skilled in the art. For example, a commit transaction could comprise a principal input from a first party, a collateral input from a second party (e.g., a guarantor of the first party, not depicted), and a joined principal and collateral input from a third party.

[44] In the embodiments depicted in FIGS. 4-5, each of the disbursement transactions comprises an input for receiving an amount from the commit output. In FIG. 4, the disbursement transaction comprises a first joined modified principal and collateral disbursement output to the first party, a second joined modified principal and collateral disbursement output to the second party, and an optional fee (ϕ) output to a third party. In FIG. 5, the disbursement transaction comprises a collateral disbursement output to the first party, a modified principal disbursement output to the first party, a modified collateral disbursement output to the second party, and an optional fee output to a third party. Again, these are but two of many possible configurations that will become apparent to one skilled in the art. For example, analogous to above, a disbursement transaction could comprise a modified principal disbursement output to a first party, a possibly modified (if the principal was exhausted) collateral disbursement output to a third party (e.g., a guarantor of the first party), or a joined modified principal and possibly modified (if the principal was exhausted) disbursement collateral output to a second party.

[45] In each of the embodiments depicted in FIGS. 4-5, the fee is allocated from the modified principals and is shared equally among the parties to the trade, although this is not required. It could be allocated at any stage, or multiple stages. It could be born solely or disproportionately by one party. Also, in each of the embodiments depicted in FIGS. 4-5, the calculation of the amounts for two or more disbursement outputs comprises a difference (∂), which is positive to one party, and negative to another party. The disbursement transaction in the embodiment

depicted in FIG. 5 would be characteristic, for example, of a swap in which the second principal was exhausted before the expiration of the swap, thereby requiring that an amount be allocated from the collateral. In other words, where:

$$\delta > P_B - \frac{1}{2} \varphi \quad [\text{eq. 1}]$$

[46] To illustrate by way of example how some of the various components above may be used together to facilitate various basic swap agreements, the following steps occur in one embodiment using the Bitcoin or similar protocol as the transfer mechanism, where the parties do not trust each other, and the facilitator is not fully trusted by any of the parties:

1. A first client transmits an offer to a facilitator, the offer comprising terms, the terms comprising:
 - a. a reference to a base asset;
 - b. a reference to a quote asset;
 - c. a principal amount;
 - d. an expiration time;
 - e. optionally a reference to a denominating asset;
 - f. optionally, a collateral amount; and
 - g. optionally, a result function;

Example terms:

Base: USD

Quote: AUD

Denominating: BTC

Principal: 0.5 (BTC)

Collateral: 2 × principal

$$res_{base}(b_o, q_o, b_f, q_f): \text{principal} \times \frac{b_f - b_o}{q_f - q_o}$$

Expiration: 2014-06-01T12:34:56Z

...

2. Optionally, the facilitator validates aspects of the offer (e.g., that the facilitator can interpret the terms, that the expiration time is within an acceptable range, etc.). If validation fails, the facilitator may reject the offer, optionally with an error message to the first client.
3. A second client retrieves the offer from the facilitator.
4. The first client signs a first source transaction comprising a transaction ID.
5. The second client signs a second source transaction comprising a transaction ID.
6. The second client transmits the transaction ID of the second source transaction to the first client, optionally via the facilitator, in such a way that it is associated with the offer (e.g., in the same message, via an offer ID, offer hash, etc.). In another embodiment the first client transmits the transaction ID of the first source transaction to the second client, and subsequent steps mirror the following of this embodiment.
7. One of the second client and the facilitator transmits a second public key to the first client in such a way that it is associated with the offer.
8. The first client signs a first principal input of an inchoate commit transaction for creating a complete commit transaction, the inchoate commit transaction comprising:
 - a. the first principal input for receiving a first principal amount from the first source transaction;
 - b. a second principal input for receiving a second principal amount from the second source transaction; and
 - c. a commit output comprising a commit amount and a condition requiring signatures of private keys corresponding to two of:
 - i. a first public key;

- ii. the second public key; and
- iii. a facilitator public key.

Example inchoate commit transaction:

Input:

Previous tx: **85e5...e61f**

Index: **1**

scriptSig: **efd6...ea1601 a6a6...2c2b**

Input:

Previous tx: **705d...9ce2**

Index: **0**

scriptSig: **[sig. placeholder]**

...

Output:

Value: **300000000**

scriptPubKey: **2 67c1...4a70 bf9a...f9e3 cffd...1373 3
OP_CHECKMULTISIG**

...

9. The first client transmits the inchoate commit transaction to the second client, optionally via the facilitator. Optionally, the facilitator validates aspects of the inchoate commit transaction (e.g., that inchoate commit transaction is signed by a first party, that the first principal amount and the second principal amount each satisfy the terms, etc.). If validation fails, the facilitator may reject the inchoate commit transaction, optionally with an error message to the first client. Optionally, the facilitator transmits the offer and the inchoate commit transaction to the second client.

10. Optionally, the second client verifies that the inchoate commit transaction is as expected, signed by the first party, etc.
11. The second client creates the complete commit transaction by signing the inchoate commit transaction and optionally saves a copy in non-transitory memory, the complete commit transaction comprising:
 - a. the first principal input for receiving the first principal amount from the first source transaction;
 - b. a second principal input for receiving a second principal amount from the second source transaction; and
 - c. a commit output comprising a commit amount and a condition requiring signatures of private keys corresponding to two of:
 - i. the first public key;
 - ii. the second public key; and
 - iii. the facilitator public key.

Example complete commit transaction:

ID: **6b24...b607**

Input:

Previous tx: 85e5...e61f

Index: 1

scriptSig: efd6...ea1601 a6a6...2c2b

Input:

Previous tx: 705d...9ce2

Index: 0

scriptSig: **78eb...fc4501 531f...00dd**

...

Output:

Value: 300000000

scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
OP_CHECKMULTISIG

...

12. The second client signs an inchoate refund transaction comprising:
- a. a lock time after the expiration time;
 - b. an input for receiving the commit amount from the complete commit transaction;
 - c. a first refund output comprising a first refund amount and a first condition requiring approval of the first party; and
 - d. a second refund output comprising a second refund amount and a condition requiring approval of a second party.

Example inchoate refund transaction:

Input:

Previous tx: **6b24...b607**

Index: **0**

scriptSig: **OP_0 [sig. placeholder] c255...d80301**

Output:

Value: **149995000**

scriptPubKey: **OP_DUP OP_HASH160 53a5...8974
OP_EQUALVERIFY OP_CHECKSIG**

Output:

Value: **149995000**

scriptPubKey: **OP_DUP OP_HASH160 30e6...2511**
OP_EQUALVERIFY OP_CHECKSIG

...

nLockTime: **2014-06-03T12:34:56Z**

13. The second client transmits the complete commit transaction and the inchoate refund transaction to the to the first client, optionally via the facilitator. Optionally, the facilitator validates aspects of the complete commit transaction and the inchoate refund transaction (e.g., that complete refund transaction is signed by the first party and the second party, that inchoate refund transaction is signed by the second party, that aspects of the complete commit transaction match the inchoate commit transaction, that the first refund amount of the signed complete refund transaction is not more than the first principal amount, that the second refund amount of the signed complete refund transaction is not more than the second principal amount, that the lock time is after the expiration time, etc.). If validation fails, the facilitator may reject the inchoate refund transaction or the complete commit transaction, optionally with an error message to the second client. Optionally, the facilitator transmits the complete commit transaction and the inchoate refund transaction to the first client.
14. Optionally, the first client verifies that the complete commit transaction is as expected and signed by the first party and the second party, that the inchoate refund transaction is as expected and is signed by the second party, etc.
15. Optionally, the first client saves a copy of the complete commit transaction in non-transitory memory.
16. The first client creates the complete refund transaction and saves a copy in non-transitory memory, the complete refund transaction comprising:
 - a. a lock time after the expiration time;
 - b. an input for receiving the commit amount from the complete commit transaction;
 - c. a first refund output comprising a first refund amount and a first condition

requiring approval of the first party; and

a second refund output comprising a second refund amount and a condition requiring approval of the second party.

Example complete refund transaction:

ID: **d5f8...8ab5**

Input:

Previous tx: 6b24...b607

Index: 0

scriptSig: OP_0 **b859...452c01** c255...d80301

Output:

Value: 149995000

scriptPubKey: OP_DUP OP_HASH160 53a5...8974

OP_EQUALVERIFY OP_CHECKSIG

Output:

Value: 149995000

scriptPubKey: OP_DUP OP_HASH160 30e6...2511

OP_EQUALVERIFY OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z

17. The first client transmits the complete refund transaction to the second client, optionally via the facilitator. Optionally, the facilitator validates aspects of the complete refund transaction (e.g., that complete refund transaction is signed by both the first party, that the complete refund transaction has not otherwise been modified, is consistent with the terms and the complete commit transaction, etc.). If validation fails, the facilitator may reject the complete refund transaction, optionally with an error message to the first

client. Optionally, the facilitator transmits the complete refund transaction to the second client.

18. Optionally, the second client verifies that the complete refund transaction is as expected and signed by the first party and the second party, etc.
19. After creating or receiving both the complete commit transaction and the complete refund transaction, the first client broadcasts the first source transaction.
20. After creating or receiving both the complete commit transaction and the complete refund transaction, the second client broadcasts the second source transaction.
21. After seeing that both the first source transaction and second source transaction have been broadcast, one or both of the first client the second client broadcast the complete commit transaction.
22. On or after the expiration time or at a time or upon an event as defined by the terms, and before the lock time of the complete refund transaction, the facilitator performs a calculation in accordance with the terms for determining a first disbursement amount and a second disbursement amount, optionally requesting information from an oracle for use in the calculation (e.g., the most recent price of an asset pair, the price of the asset pair at the time the offer was accepted, etc.). In one embodiment, the facilitator queries an oracle, which comprises a data source that could comprise an external data feed, internal database, another oracle, etc.

In the example embodiment, given a time t , the oracle provides the value at t of one or more of: the base asset, the quote asset, the base asset in terms of the denominating asset b_t , the quote asset in terms of the denominating asset q_t , or the base asset in terms of the quote asset (e.g., if the base asset or the quote asset is also the denominating asset).

In continuing the example above, the base asset is USD, the quote asset is AUD, and the denominating asset is BTC. b_o is the value of USD in BTC at the time the trade is initiated. b_f is the value of USD in BTC at the time the trade is completed. q_o is the value of AUD in BTC at the time the trade is initiated. q_f is the value of AUD in BTC at the time the trade is completed. The calculation the facilitator uses to compute the first disbursement amount and the second disbursement amount comprises $res_{base}(b_o, q_o, b_f,$

q_f). In typical embodiments, a party's loss is proportionate to its counterparty's gain, implying:

$$res_{quote}(b_o, q_o, b_f, q_f) = -res_{base}(b_o, q_o, b_f, q_f) \quad [\text{eq. 2}]$$

23. The facilitator signs an inchoate disbursement transaction, which comprises:
- a. an input for receiving the commit amount from the complete commit transaction;
 - b. a first disbursement output comprising the first disbursement amount and a first condition requiring approval of the first party;
 - c. a second disbursement output comprising the second disbursement amount and a condition requiring approval of the second party; and
 - d. optionally a third disbursement output comprising a fee amount and a condition requiring approval of a third party;

typically where the sum of the first disbursement amount, the second disbursement amount, and any fee amount is not more than the commit amount from the complete commit transaction.

Example inchoate disbursement transaction:

Input:

Previous tx: **6b24...b607**

Index: **0**

scriptSig: **OP_0 [sig. placeholder] ddbb...b00601**

Output:

Value: **142500736**

scriptPubKey: **OP_DUP OP_HASH160 53a5...8974**

OP_EQUALVERIFY OP_CHECKSIG

Output:

Value: **157479264**

scriptPubKey: **OP_DUP OP_HASH160 30e6...2511**
OP_EQUALVERIFY OP_CHECKSIG

Output:

Value: **10000**

scriptPubKey: **OP_DUP OP_HASH160 d377...5c8c**
OP_EQUALVERIFY OP_CHECKSIG

...

24. The facilitator transmits the inchoate disbursement transaction to both the first client and the second client, either of whom may independently verify, sign, and broadcast the disbursement transaction before the time arrives that the other can successfully broadcast the complete refund transaction.

[47] The above is but one embodiment of a transaction according to the invention. In another, equivalent or alternate steps may be used. The following describes an embodiment comprising an atypical, but illustrative arrangement:

1. A first client transmits an offer to a second client.
2. The first client transmits the offer to a facilitator.
3. The facilitator transmits to the first client a first inchoate commit transaction for creating a complete commit transaction, the first inchoate commit transaction comprising:
 - a. a first principal input for receiving a first principal amount from a first source transaction; and
 - b. a first commit output comprising a first commit amount and a condition requiring approval of two of:
 - i. a first party;
 - ii. a second party; and
 - iii. the facilitator.

4. The facilitator transmits to the second client a second inchoate commit transaction for creating a complete commit transaction, the second inchoate commit transaction comprising:
 - a. a second principal input for receiving a second principal amount from a second source transaction; and
 - b. a second commit output comprising a second commit amount and a condition requiring approval of two of:
 - i. the first party;
 - ii. the second party; and
 - iii. the facilitator.
5. The first client signs the first source transaction.
6. The first client completes and signs (e.g., with `SIGHASH_SINGLE` | `SIGHASH_ANYONECANPAY`) the first inchoate commit transaction.

Example first inchoate commit transaction:

...

Input:

Previous tx: **85e5...e61f**

Index: **1**

scriptSig: **5e7c...a11a83 ecad...d0ba**

...

Output:

Value: **150000000**

scriptPubKey: **2 67c1...4a70 bf9a...f9e3 cffd...1373 3
OP_CHECKMULTISIG**

...

7. The first client transmits the first inchoate commit transaction to the facilitator.
8. The second client signs the second source transaction.
9. The second client completes and signs (e.g., with `SIGHASH_SINGLE` | `SIGHASH_ANYONECANPAY`) the second inchoate commit transaction.

Example second inchoate commit transaction:

...

Input:

Previous tx: **705d...9ce2**

Index: **0**

scriptSig: **ade1...9dcb83 f058...878a**

...

Output:

Value: **150000000**

scriptPubKey: **2 67c1...4a70 bf9a...f9e3 cffd...1373 3
OP_CHECKMULTISIG**

...

10. The second client transmits the second inchoate commit transaction to the facilitator.
11. The facilitator creates the complete commit transaction from the first inchoate transaction and the second inchoate commit transaction, the complete commit transaction comprising:
 - a. a first principal input for receiving a first principal amount from the first source transaction; and
 - b. a first commit output comprising a first commit amount and a condition

requiring approval of two of:

- i. the first party;
 - ii. the second party; and
 - iii. the facilitator;
- c. a second principal input for receiving a second principal amount from the first source transaction; and
- d. a second commit output comprising a second commit amount and a condition requiring approval of two of:
- i. the first party;
 - ii. the second party; and
 - iii. the facilitator.

Example complete commit transaction:

ID: **11f0...8ea8**

Input:

Previous tx: **85e5...e61f**

Index: **1**

scriptSig: **5e7c...a11a83 ecad...d0ba**

Input:

Previous tx: **705d...9ce2**

Index: **0**

scriptSig: **ade1...9dcb83 f058...878a**

...

Output:

Value: **150000000**

scriptPubKey: **2 67c1...4a70 bf9a...f9e3 cffd...1373 3**
OP_CHECKMULTISIG

Output:

Value: **150000000**

scriptPubKey: **2 67c1...4a70 bf9a...f9e3 cffd...1373 3**
OP_CHECKMULTISIG

...

In another embodiment, the first client provides a transaction ID of the first source transaction to the facilitator and the second client provides a transaction ID of the second source transaction to the facilitator before the facilitator transmits the first inchoate commit transaction and the second inchoate commit transaction. The facilitator creates the first inchoate commit transaction identical to the second inchoate commit transaction, each comprising a first principal input with a placeholder signature and a second principal input with a placeholder signature. Once the respective inchoate commit transactions are transmitted to the respective clients, the clients each sign their respective principal input (e.g., with `SIGHASH_ALL` | `SIGHASH_ANYONECANPAY`) before returning their respective signed inchoate commit transaction back to the facilitator. The facilitator collects the signed inchoate commit transactions and consolidates the signed inputs into a complete commit transaction. In such an embodiment, the first commit output and the second commit output could be consolidated, and the corresponding disbursement transaction and refund transaction could omit their respective second inputs.

12. The facilitator transmits the completed commit transaction to the first client who optionally stores it in non-transitory memory.
13. The facilitator transmits the completed commit transaction to the second client who optionally stores it in non-transitory memory.
14. The first client signs (e.g., `SIGHASH_ALL` | `SIGHASH_ANYONECANPAY` or `SIGHASH_SINGLE` | `SIGHASH_ANYONECANPAY`) an inchoate refund transaction

comprising:

- a. a lock time after the expiration time;
- b. a first input for receiving the first commit amount from the complete commit transaction;
- c. a second input for receiving the second commit amount from the complete commit transaction;
- d. a first refund output comprising a first refund amount and a first condition requiring approval of the first party; and
- e. a second refund output comprising a second refund amount and a second condition requiring approval of the second party.

Example inchoate refund transaction:

Input:

Previous tx: **11f0...8ea8**

Index: **0**

scriptSig: **OP_0 78a2...203181 [sig. placeholder]**

Input:

Previous tx: **11f0...8ea8**

Index: **1**

scriptSig: **OP_0 fdbe...893f81 [sig. placeholder]**

...

Output:

Value: **149995000**

scriptPubKey: **OP_DUP OP_HASH160 53a5...8974
OP_EQUALVERIFY OP_CHECKSIG**

Output:

Value: **149995000**

scriptPubKey: **OP_DUP OP_HASH160 30e6...2511**
OP_EQUALVERIFY OP_CHECKSIG

...

nLockTime: **2014-06-03T12:34:56Z**

15. The first client transmits the complete commit transaction and the inchoate refund transaction to the second client.
16. The second client creates the complete refund transaction from the inchoate refund transaction (e.g., signing with `SIGHASH_ALL` | `SIGHASH_ANYONECANPAY` or `SIGHASH_SINGLE` | `SIGHASH_ANYONECANPAY`) and saves a copy in non-transitory memory.

Example complete refund transaction:

ID: **eb09...3d15**

Input:

Previous tx: 11f0...8ea8

Index: 0

scriptSig: OP_0 78a2...203181 **b765...fc4383**

Input:

Previous tx: 11f0...8ea8

Index: 1

scriptSig: OP_0 fdbe...893f81 **91e4...4dd583**

...

Output:

Value: 149995000

scriptPubKey: OP_DUP OP_HASH160 53a5...8974
OP_EQUALVERIFY OP_CHECKSIG

Output:

Value: 149995000

scriptPubKey: OP_DUP OP_HASH160 30e6...2511
OP_EQUALVERIFY OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z

17. The second client transmits the complete refund transaction to the first client.
18. After creating or receiving both the complete commit transaction and the complete refund transaction, the first client broadcasts the first source transaction.
19. After creating or receiving both the complete commit transaction and the complete refund transaction, the second client broadcasts the second source transaction.
20. After seeing that both the first source transaction and second source transaction have been broadcast, one or both of the first client the second client broadcast the complete commit transaction.
21. On or after the expiration time, or at a time or upon an event as defined by the terms, and before the lock time of the complete refund transaction, the facilitator performs a calculation in accordance with the terms for determining a first disbursement amount and a second disbursement amount, optionally requesting information from an oracle for use in the calculation.
22. The facilitator signs a disbursement transaction (e.g., signing with SIGHASH_ALL | SIGHASH_ANYONECANPAY or SIGHASH_SINGLE | SIGHASH_ANYONECANPAY).

Example inchoate disbursement transaction:

Input:

Previous tx: **11f0...8ea8**

Index: **0**

scriptSig: **OP_0 [sig. placeholder] 8cd3...d86481**

Input:

Previous tx: **11f0...8ea8**

Index: **1**

scriptSig: **OP_0 [sig. placeholder] 12bc...825281**

...

Output:

Value: **142500736**

scriptPubKey: **OP_DUP OP_HASH160 53a5...8974
OP_EQUALVERIFY OP_CHECKSIG**

Output:

Value: **157479264**

scriptPubKey: **OP_DUP OP_HASH160 30e6...2511
OP_EQUALVERIFY OP_CHECKSIG**

Output:

Value: **10000**

scriptPubKey: **OP_DUP OP_HASH160 d377...5c8c
OP_EQUALVERIFY OP_CHECKSIG**

...

23. The facilitator transmits the inchoate disbursement transaction to both the first client and the second client, either of whom can broadcast it as in the prior example embodiment.

[48] Various verification steps have been omitted for brevity.

[49] It will become apparent to one skilled in the art that aspects of each of embodiments above may be comingled. For example, the first client could transmit the offer to the facilitator, where the second client could find and retrieve it. As mentioned above, aspects of one or both of the first client and the second client could coincide with the facilitator allowing many of the above steps to be omitted as redundant where the facilitator is entrusted to act as a proxy for or on behalf of one of the first party and the second party. The facilitator could contain aspects of one of the clients, but not the other, in which case the extra-facilitator client would optionally independently validate transactions it received from the facilitator before signing them, etc. In such embodiments, the facilitator typically comprises a means to control aspects of a client it comprises via an interface such as a web-based user interface (UI), an application programmer's interface (API), etc.

[50] In such embodiments, any party delegating authority to the facilitator must trust the facilitator to be secure and to act fairly, but these are similar to expectations many parties already have of traditional third party intermediaries. Assuming the first party has independent access to same key pairs the facilitator uses to act on behalf of the first party, and the second party has independent access to the same key pairs the facilitator uses to act on behalf of the second party, even if the facilitator is destroyed, both the first party and the second party may retrieve their assets, at worst by broadcasting any signed refund transaction on or after the lock time, assuming they have kept copies of the signed refund transaction in their respective non-transitory memories.

[51] In one embodiment, a client is configured such that when it detects a new spendable output comprising an amount (e.g., by monitoring changes in the blockchain when using the Bitcoin or similar protocol as the transfer mechanism), it automatically accepts a remote offer comprising an amount compatible with the amount of the new spendable output. If no such remote offer is available, it transmits an offer comprising an amount substantially similar to the new spendable output (e.g., to the facilitator, to another client, etc.). In another embodiment, when the client detects a second new spendable output, it attempts to rescind the offer. If successful, it transmits a new offer comprising an amount which comprises some or all of the new spendable output and some or all of the second new spendable output. Other variations are possible. For example, the client is configured to scan available offers and match the available offers to the amounts of the spendable outputs. Matching algorithms vary in complexity and are

known in the art. For example, many Bitcoin protocol client implementations provide such algorithms for matching spendable outputs to the inputs of simple transactions. Such algorithms are adaptable by those of ordinary skill in the art for this and similar embodiments of the invention.

[52] In various embodiments, the terms comprise a ratio of a first asset to a second asset, optionally denominated in a third asset, as well as an amount that each participant must allocate. For example, in one embodiment, the terms could offer to “sell” 2 BTC/USD with a required allocation of 3 BTC from each party. In other words, the swap defined by the terms offers exposure to 2 BTC of USD, and each participant must allocate 2 BTC to principal and 1 BTC to collateral for the duration of the swap (i.e., until it expires, or until the principal and collateral of one party is exhausted).

[53] The allocations for each party need not be equal. In one embodiment, if the market expects a particular asset pair to decline over the life of the swap, the party accepting exposure to that asset may be required to allocate more collateral than the counterparty. Note that in the previous example, the parties’ risk formulas are asymmetric. The most the offeror could lose is the principal of 2 BTC (if BTC become worthless when valued in USD). However, the offeree’s losses are unbounded (if USD becomes worthless when valued in BTC). In other words:

$$res_{base}(b_o, q_o, b_f, q_f) = principal \times \frac{b_f - b_o}{q_f - q_o} \quad [\text{eq. 3}]$$

[54] Alternately:

$$res_{base}(b_o, q_o, b_f, q_f) = principal \times \left(\frac{b_f}{q_f} - \frac{b_o}{q_o} \right) \quad [\text{eq. 4}]$$

[55] In other embodiments symmetrical models could be adopted. Consider:

$$res_{base}(b_o, q_o, b_f, q_f) = \begin{cases} \frac{b_f}{q_f} \leq \frac{b_o}{q_o} & : \quad principal \times \left(\frac{b_f q_o}{b_o q_f} - 1 \right) \\ \frac{b_f}{q_f} > \frac{b_o}{q_o} & : \quad principal \times \left(1 - \frac{b_o q_f}{b_f q_o} \right) \end{cases} \quad [\text{eq. 5}]$$

[56] Where $res_{base}(\dots)$ is the resulting gain or loss to the party taking the base asset exposure

at time f given the initial value of the base asset b_o , the initial value of the quote asset q_o , the value of the base asset b_f at time f , and the value of the quote asset q_f at time f . The resulting gain or loss for the party taking the quote asset exposure is inverted:

$$\begin{aligned} res_{quote}(b_o, q_o, b_f, q_f) &= -res_{base}(b_o, q_o, b_f, q_f) \\ &= \begin{cases} \frac{b_f}{q_f} \leq \frac{b_o}{q_o} & : \text{principal} \times \left(1 - \frac{b_f q_o}{b_o q_f}\right) \\ \frac{b_f}{q_f} > \frac{b_o}{q_o} & : \text{principal} \times \left(\frac{b_o q_f}{b_f q_o} - 1\right) \end{cases} \end{aligned} \quad [\text{eq. 6}]$$

[57] In this embodiment, the parties' risk formulas are symmetric. If the base asset goes to zero, the most the party taking the base asset exposure can lose is the principal. Likewise, if the quote asset goes to zero, the most the party taking the quote asset exposure can lose is the principal. Note that no collateral is needed. Alternately, consider:

$$\begin{aligned} res_{base}(b_o, q_o, b_f, q_f) &= -res_{quote}(b_o, q_o, b_f, q_f) \\ &= \begin{cases} \frac{b_f}{q_f} \leq \frac{b_o}{q_o} & : -\text{principal} \times \frac{b_o q_f}{b_f q_o} \\ \frac{b_f}{q_f} > \frac{b_o}{q_o} & : \text{principal} \times \frac{b_f q_o}{b_o q_f} \end{cases} \end{aligned} \quad [\text{eq. 7}]$$

[58] In this embodiment, the parties' risk formulas are also symmetric. However, as the base asset goes to zero, the loss incurred by the party taking the base asset approaches infinity, all else being equal. Likewise, as the quote asset goes to zero, the loss incurred by the party taking the quote asset position approaches infinity, all else being equal. Note that collateral is needed when losses exceed principal amounts. The more volatile the asset pair, the more collateral may be required to minimize risk of termination before expiration. These are but a few basic examples. Terms affecting the calculation for determining the allocation disbursement amounts can be arbitrarily complex and are limited by the imaginations of the participants. All such variations are contemplated by the invention.

[59] In some circumstances, a party may wish to exit a swap before it terminates. The parties may agree to terminate prematurely. In one embodiment, the facilitator facilitates this by creating the unsigned disbursement transaction as if the swap was terminated when the parties agreed to exit. The requesting party signs the unsigned disbursement transaction and transmits

it to the acquiescing party who signs and broadcasts it. Optionally, if the facilitator includes a fee output to a third party, the acquiescing party may require that the fee would be born disproportionately, or entirely by the requesting party.

[60] Where one party wishes to exit before termination, but cannot secure an agreement from the counterparty, another option is for the party seeking premature termination to find a third party substitute. FIGS. 6-7 depict transaction chains from various example swap embodiments comprising such substitutions.

[61] FIG. 6 depicts aspects of an embodiment where a withdrawing party (A) has convinced an entering party (C) to substitute into a transaction with a remaining party (B). In addition, the entering party transfers a negotiated amount (ϵ) to the withdrawing party. This is facilitated in the depicted embodiment by a substitution transaction, a second commit transaction, and a second refund transaction.

[62] For clarity of illustration, the outputs of the commit transaction and the corresponding inputs of the substitution transaction are depicted as separate for each of the first principal (P_A), the first collateral (C_A), the second principal (P_B), and the second collateral (C_B). This is not a limitation of the invention. Just as with the previously described embodiments, the outputs of the commit transaction, and corresponding inputs of the substitution transaction could be any configuration considered valid by the transfer mechanism. The outputs of the substitution transaction and inputs to the second commit transaction are similarly depicted for clarity of illustration. Again, all valid configurations of inputs and outputs between transactions are contemplated by the invention.

[63] A difference (∂) used to calculate the first disbursement amount and the second disbursement amount as if the transaction had been terminated at the time of the substitution. In the embodiment depicted in FIG. 6, this favors the remaining party. Therefore, the substitution transaction is constructed such that the withdrawing party takes a loss in proportion to that difference, and the entering party need only provide assets to cover the remaining position.

[64] Also, in the embodiment depicted in FIG. 6, the substitute refund is asymmetric. The entering party is refunded what that party committed to the transaction (less the negotiated amount), and the remaining party is refunded what that party would have received had the swap been terminated at the time of substitution. Other variations are possible. For example, in one

embodiment, the negotiated amount may be transferred separately, or at another phase of the swap.

[65] In the embodiment depicted in FIG. 7, the substitution favors the withdrawing party. In that embodiment, the substitute refund is symmetric. The remaining party is refunded what that party would have received had the original transaction been refunded.

[66] In one embodiment, a substitution is facilitated by the following steps:

1. The facilitator performs a calculation in accordance with the terms for determining a withdrawal amount and an entry amount, optionally requesting information from an oracle for use in the calculation.
2. The facilitator creates an inchoate substitution transaction comprising:
 - a. a first input for receiving an amount from a commit transaction;
 - b. an entry input for receiving the entry amount from a source transaction;
 - c. a withdrawal output comprising the withdrawal amount and a first condition requiring approval of the first party; and
 - d. a substitution output comprising a substitution amount and a second condition requiring approval of two of:
 - i. the second party;
 - ii. the third party; and
 - iii. the facilitator.

Example substitution transaction:

Input:

Previous tx: **6b24...b607**

Index: **0**

scriptSig: **OP_0 [sig. placeholder] [sig. placeholder]**

Input:

Previous tx: **dd66...ae8e**

Index: **3**

scriptSig: **[sig. placeholder]**

Output:

Value: **300000000**

scriptPubKey: **2 bf9a...f9e3 952b...0542 cffd...1373 3
OP_CHECKMULTISIG**

Output:

Value: **121871000**

scriptPubKey: **OP_DUP OP_HASH160 6250...6cfc
OP_EQUALVERIFY OP_CHECKSIG**

...

3. The facilitator transmits the inchoate substitution transaction to the first party and the third party.
4. The first party signs the first input of inchoate substitution transaction (e.g., signing with `SIGHASH_ALL | SIGHASH_ANYONECANPAY`) and transmits the first signed inchoate substitution transaction to the facilitator.
5. The third party signs the entry input of the inchoate substitution transaction (e.g., signing with `SIGHASH_ALL | SIGHASH_ANYONECANPAY`) and transmits the second signed inchoate substitution transaction to the facilitator.
6. The facilitator creates a complete substitution transaction (e.g., ID: `9c8b...4794`) from the first inchoate substitution transaction and the second inchoate substitution transaction.
7. The facilitator signs an inchoate substitute refund transaction comprising:

- a. a lock time after the expiration time;
- b. an input for receiving the substitution amount from the substitution transaction;
- c. a first refund output comprising a first refund amount and a first condition requiring approval of the second party; and
- d. a second refund output comprising a second refund amount and a condition requiring approval of the third party.

Example inchoate substitute refund transaction:

Input:

Previous tx: **9c8b...4794**

Index: **0**

scriptSig: **OP_0 [sig. placeholder] b2ac...8a4601**

Output:

Value: **178124000**

scriptPubKey: **OP_DUP OP_HASH160 30e6...2511**

OP_EQUALVERIFY OP_CHECKSIG

Output:

Value: **121866000**

scriptPubKey: **OP_DUP OP_HASH160 94e2...4fb6**

OP_EQUALVERIFY OP_CHECKSIG

...

nLockTime: **2014-06-03T12:34:56Z**

8. The facilitator signs the inchoate substitute refund transaction and transmits the signed substitute refund transaction to the second party and the third party.
9. The facilitator broadcasts the signed substitution transaction.

[67] Various verification and details steps disclosed in previous embodiments have been omitted for brevity. In other embodiments, the transactions are created or signed by the first party or the second party instead of the facilitator. For example, the first party and the second party could agree upon the amounts in the substitution transaction, and each could sign it without involving the facilitator. All such variations are considered part of the invention.

[68] A letter of credit (L/C) is well known in the art, but is fundamentally an agreement where a third party transfers assets to a second party on behalf of a first party upon some agreed upon condition being demonstrated as met before an agreed upon time (an expiration). Typically, this comprises an expensive manual review of arcane shipping documents by an intermediary financial institution before it will release funds on behalf of a buyer. However this costly approach can be eschewed in favor of one embodiment of the invention in which the facilitator conditions the creation and transmission of a disbursement transaction based on the result from a query to a shipper's public API regarding a known tracking number. In other embodiments, L/C terms comprise evaluating search results, observation of the presence or absence of data at an anticipated location, checking that the value of a variable or response from an API is within a set of expected values or matches an anticipated pattern, taking a measurement from an instrument and validating that it is within an anticipated range or tolerance, etc. The possibilities are many and varied. For example, US continuation application 13/970,755 ('755) describes systems and methods for efficiently calculating geospatial nearness. Others are known in the art. In one embodiment, the calculation comprises a condition whereupon an object is or was "at" or "near" (i.e., within a specified distance of) a particular location. Mechanisms to discover the location of said object are known in the art (e.g., self-reporting GPSs, Automatic Identification and Data Capture (AIDC) devices, such as barcodes, Quick Response (QR) Codes, Radio Frequency Identification (RFID) tags, in proximity of a reporting detector or sensor at a known location, etc.). Many possible configurations are contemplated by the invention, and will become apparent to one skilled in the art.

[69] FIG. 8 depicts aspects of one embodiment pertaining to an L/C comprising a source transaction and a commit transaction. As depicted, the commit transaction comprises a first input for accepting a first amount from a first source transaction (i.e., from a first party), and one or more outputs for directing a portion of the first amount to one or more other transactions (not depicted). In other embodiments (portions of which are depicted in other figures), the commit transaction further comprises a second input for accepting a second amount from a second source transaction (i.e., from a second party), where the first amount and second amount

total an expected amount. In some cases the amounts comprise a principal amount (P), and (optionally) a collateral amount (C), as depicted in the various figures. While only a first source transaction is depicted in FIG. 8, that should not be construed as a limitation of the invention.

[70] FIG. 9 depicts aspects of one embodiment pertaining to an L/C comprising a commit transaction and an expiration transaction, the expiration transaction being analogous to the refund transaction in previously described embodiments. However, where a refund transaction is meant exclusively for recovery of funds an exception (e.g., the facilitator becomes unavailable to create or sign a disbursement transaction), use of an expiration transaction, in addition to recovery, is contemplated by the offer (e.g., if the conditions set forth are not satisfied before the expiration time, despite the facilitator being operational). The difference is largely conceptual. The two function almost identically within the invention. The commit transaction comprises a first input for receiving a first principal amount (P_A), and a commit output. The expiration transaction comprises an input for receiving an amount from the commit output, a first expiration output to the first party. In other embodiments where the commit transaction comprises a second input for receiving a second amount, the expiration transaction comprises a second expiration output to the second party.

[71] FIGS. 10-11 depict aspects of L/C embodiments comprising relatively simple disbursement transactions in a situation involving principal and collateral. In FIG. 10, the commit transaction comprises a first joined principal and collateral ($(P+C)_A$) input from a first party. In other embodiments, just as with those mentioned above, the inputs need not be joined. In FIG. 11, the commit transaction comprises a first joined principal and collateral input from a first party, and a second collateral (C_B) input from the second party. These are but two of many possible configurations contemplated by the invention. For example, a commit transaction could comprise a principal input from a first party, a collateral input from a third party (e.g., a guarantor of the first party, not depicted), and a collateral input from a second party.

[72] In the embodiments depicted in FIGS. 10-11, each of the disbursement transactions comprises an input for receiving an amount from the commit output. In FIG. 10, the disbursement transaction comprises a first collateral disbursement output to the first party, a first principal disbursement output to the second party, and an optional fee (ϕ) output to a third party, where the fee is deducted from the collateral. In FIG. 11, the disbursement transaction comprises a collateral disbursement output to the first party, and a joined principal and collateral disbursement output to the second party. In addition, the commit transaction

comprises an optional fee output to a third party, which is born equally by the parties in the disbursement transaction. Again, these are but two of many possible configurations contemplated by the invention. For example, the optional fee output could be allocated at any stage, or multiple stages. It could be born solely or disproportionately by one party at the same or different stages.

[73] To illustrate by way of example how some of the various components above may be used together to facilitate various L/C agreements, the following steps occur in one embodiment using the Bitcoin or similar protocol as the transfer mechanism, where the parties do not trust each other, and the facilitator is not fully trusted by any of the parties:

10. A first client creates an offer, the offer comprising terms, the terms comprising:
 - a. one of a disbursement condition, a reference to a disbursement condition, a disbursement function, and a reference to a disbursement function;
 - b. a principal amount;
 - c. an expiration time;
 - d. optionally, a first collateral amount; and
 - e. optionally, a second collateral amount.

Example terms:

Payer principal: 0.5 (BTC)

Payer collateral: $1 \times \text{principal}$

Payee collateral: $0.05 \times \text{principal}$

Disbursement condition:

`FedEx("987654321").deliveredToCarrier() == true`

Expiration: 2014-06-01T12:34:56Z

...

11. The first client signs a first source transaction.

12. The first client creates an inchoate commit transaction comprising:
 - a. the first input for receiving the first amount from the first source transaction;
 - b. optionally, a second input for receiving a second amount from a second source transaction;
 - c. a commit output comprising a commit amount and a condition requiring approval of two of:
 - i. a first party;
 - ii. a second party; and
 - iii. a facilitator.
13. Optionally, the first client transmits the offer to the facilitator, who validates aspects of the offer (e.g., that the facilitator can interpret the terms, that the expiration time is within an acceptable range, etc.). If validation fails, the facilitator may reject the offer, optionally with an error message to the first client.
14. The first client transmits the offer to a second client.
15. Optionally, if the inchoate commit transaction comprises a second input, the first client transmits the inchoate commit offer to the second client. The second client signs a second source transaction. The second client signs the inchoate commit transaction. The second client transmits the inchoate commit transaction back to the first client.
16. The first client signs (e.g., with `SIGHASH_ALL` | `SIGHASH_ANYONECANPAY`) the inchoate commit transaction to create a complete commit transaction, optionally storing the complete commit transaction in non-transitory memory.

Example complete commit transaction:

ID: **c215...fc9b**

Input:

Previous tx: **85f7...e06c**

Index: **4**

scriptSig: **186b...ed3d81 9a9c...0fc5**

Input:

Previous tx: **6b03...e16e**

Index: **7**

scriptSig: **c48e...353c81 4afe...2c8d**

...

Output:

Value: **150000000**

scriptPubKey: **2 67c1...4a70 bf9a...f9e3 cffd...1373 3**
OP_CHECKMULTISIG

...

17. The first client signs an inchoate expiration transaction comprising:
- a lock time on or after the expiration time;
 - an input for receiving the commit amount from the complete commit transaction;
 - a first expiration output comprising a first expiration amount and a first condition requiring approval of the first party; and
 - optionally, a second expiration output comprising a second expiration amount and a condition requiring approval of the second party.

Example inchoate expiration transaction:

Input:

Previous tx: **c215...fc9b**

Index: **0**

scriptSig: **OP_0 7d17...0b5101 [sig. placeholder]**

...

Output:

Value: **99995000**

scriptPubKey: **OP_DUP OP_HASH160 53a5...8974**
OP_EQUALVERIFY OP_CHECKSIG

Output:

Value: **4995000**

scriptPubKey: **OP_DUP OP_HASH160 30e6...2511**
OP_EQUALVERIFY OP_CHECKSIG

...

nLockTime: **2014-06-01T12:34:56Z**

18. The first client transmits the complete commit transaction and the inchoate expiration transaction to the second client who optionally stores the complete expiration transaction in non-transitory memory.
19. The second client signs the inchoate expiration transaction to create a complete expiration transaction and stores the complete expiration transaction in non-transitory memory.
20. The second client transmits the complete expiration transaction to the first client.
21. After creating or receiving both the complete commit transaction and the complete expiration transaction, the first client broadcasts the first source transaction.
22. After creating or receiving both the complete commit transaction and the complete expiration transaction, the second client broadcasts the second source transaction.
23. After seeing that both the first source transaction and second source transaction have been broadcast, one or both of the first client the second client broadcast the complete commit transaction.
24. At a time or upon an event as defined by the terms or upon a query by the first client or

the second client (optionally providing one or more of the complete commit transaction, a reference to the complete commit transaction, and the terms), and before the lock time of the complete expiration transaction, the facilitator performs a calculation in accordance with the terms for determining a first disbursement amount, and optionally a second disbursement amount, optionally requesting information from an oracle for use in the calculation (e.g., whether an anticipated shipment has been delivered to a shipper, a destination address, etc., etc.). In one embodiment, the facilitator queries an oracle, which comprises a data source. This could be an external API, internal database, etc.

In a typical embodiment, the disbursement amounts are such that any remaining collateral is returned to the respective providing party, and the principal is transferred from the providing party (payer) to the counterparty (payee).

25. The facilitator signs an inchoate disbursement transaction, which comprises:
- a. an input for receiving the commit amount from the complete commit transaction;
 - b. a first disbursement output comprising the first disbursement amount and a first condition requiring approval of the second party;
 - c. optionally, a second disbursement output comprising the second disbursement amount and a condition requiring approval of the first party;
 - d. optionally a third disbursement output comprising a fee amount and a condition requiring approval of a third party;

typically where the sum of the first disbursement amount, any second disbursement amount, and any fee amount is not more than the commit amount from the complete commit transaction.

Example inchoate disbursement transaction:

Input:

Previous tx: **c215...fc9b**

Index: **0**

scriptSig: **OP_0 [sig. placeholder] 8205...424901**

Output:

Value: **49990000**

scriptPubKey: **OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
OP_CHECKSIG**

Output:

Value: **54990000**

scriptPubKey: **OP_DUP OP_HASH160 6250...6cfc OP_EQUALVERIFY
OP_CHECKSIG**

Output:

Value: **10000**

scriptPubKey: **OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY
OP_CHECKSIG**

...

26. The facilitator transmits the inchoate disbursement transaction to both the first client and the second client, either of whom can broadcast it as in the prior example embodiments.

[74] In another embodiment, the condition of the commit output requires approval of either the first party and the second party or the second party and one or more service providers, (e.g., a shipper, insurance provider, inspector, etc.). An inchoate disbursement transaction is constructed with placeholders for the second party, and each of the service providers. When all of the service providers have signed their respective portions, the second party may sign and broadcast the disbursement transaction. In a further embodiment, the second party commits assets to the commit transaction for paying each of the service providers, and each of the service providers are paid out of the disbursement transaction.

[75] FIGS. 12-14 depict transaction chains from various example L/C embodiments comprising substitutions of parties. FIG. 12 depicts aspects of an embodiment where a payer party (A) has convinced a substituting party (C) to substitute into a transaction with a payee

party (B). In addition, the payer party transfers a negotiated amount (ϵ) to the substituting party. For example, the payer party could have committed to purchasing goods from the payee party, but due to unanticipated market conditions, decided to sell the right to take delivery of the goods to the substituting party at a loss. This is facilitated in the depicted embodiment by a substitution transaction and a second expiration transaction. In a related embodiment where the payer party sold the right to take delivery for a profit, the negotiated amount might flow from the substituting party to the payer party. In the embodiment depicted in FIG. 12, an optional fee (ϕ) is paid to a third party, and is born by the payee party.

[76] FIG. 13 depicts aspects of an embodiment where a payee party (B) has convinced a substituting party (C) to substitute into a transaction with a payer party (A). In addition, the substituting party transfers a negotiated amount (ϵ) to the payer party. For example, the third party, may be interested in having the right to receive payment under a future disbursement transaction, perhaps due to the decreasing relative value of the substituting party's other assets. This is facilitated in the depicted embodiment by a substitution transaction, and a second expiration transaction. In a related embodiment where the payee party sold the right to receive payment at a loss, the negotiated amount might flow from the payee party to the substituting party. Similar to FIG. 12, in the embodiment depicted in FIG. 13, an optional fee (ϕ) is paid to a third party, and is born by the substituting party.

[77] FIG. 14 depicts aspects of an embodiment where a payer party (A) has convinced a substituting party (C) to substitute in part (as depicted to cover the collateral originally paid by the payer party) into a transaction with a payee party (B). In addition, the substituting party transfers a negotiated amount (ϵ) to the payer party. This is facilitated in the depicted embodiment by a substitution transaction and a second expiration transaction. In some embodiments, the substitution output of the substitute transaction comprises a condition requiring approval of three of three parties, three of four parties, or two of four parties (e.g., where the substituting party has been delegated authority to approve or sign on behalf of itself and for the payer party). Many possible configurations are contemplated by the invention. In such embodiments, the facilitator can act as a referee in creating the substitution transaction to the satisfaction of all parties, for example, maintaining the ability to dispute the transaction with a chosen mediator as described below.

[78] For clarity of illustration in FIGS. 12-14, the outputs of the commit transaction and the corresponding inputs of the substitution transaction are depicted as separate for each of the first

joined principal and collateral $((P+C)_A)$, and the second collateral (C_B) . This is not a limitation of the invention. The outputs of the commit transaction, and corresponding inputs of the substitution transaction could be any configuration considered valid by the transfer mechanism. The outputs of the substitution transaction and inputs to the second commit transaction are similarly depicted for clarity of illustration. Again, all valid configurations of inputs and outputs between transactions are contemplated by the invention. Also, in other embodiments, any fee could be paid, in part or in whole, by any party, even a fourth party.

[79] Where the Bitcoin protocol, the Ethereum protocol, or similar is used as the transfer mechanism, another embodiment of the invention enables arbitrary offers—such as offers for arbitrary swaps, L/Cs, and any other offer where terms describing that may be expressed and interpreted by the facilitator—to be made by broadcasting a specialized transaction in which the terms, a reference to the terms (e.g., a URI for the terms, a hash of the terms, etc.), or some combination thereof is encoded into the offer transaction itself, rather than associated via an extra transfer mechanism means (i.e., “off blockchain” in Bitcoin protocol terms), such as a centralized authority, or shared decentralized data store (e.g., a torrent, an “altcoin”, etc.).

[80] In one embodiment, this could be encoded as transaction metadata, or—where the Bitcoin Protocol or similar is used as the transfer mechanism—unused data in an input or output (e.g., `<data> OP_DROP <script>`, via the `OP_RETURN <data>` technique in a single output, etc.). For illustration, the following steps describe but a few of many such embodiments:

1. In one embodiment, a first client (offeror) creates an offer transaction comprising associated data and an offer output comprising an offer amount and a condition requiring approval of one of a first party and, optionally, a facilitator. The associated data comprise one or both of terms and a reference to the terms. Optionally, the associated data comprise a reference to the facilitator (e.g., a domain name, a payment address, D&B number, URI, etc.). Also optionally, the first client transmits the terms, the associated data, or offer transaction to the facilitator for validation before broadcasting it (e.g., to ensure the facilitator can interpret the terms, that the facilitator is appropriately identified, etc.). In another embodiment, at the first client’s request, the facilitator creates an inchoate offer transaction (e.g., not including a signed input) for creating a complete offer transaction, and the first client optionally verifies whether the facilitator created the transaction correctly, whether it’s available via the facilitator-provided reference (if applicable), etc.

Example inchoate offer transaction:

```
% # Post the terms to the facilitator
% curl -X POST -d
'{"base":"USD","quote":"AUD","denom":"BTC","pcpl":0.5,"cltl":1.0,
"res":"symunbound","offerexp":"2014-06-
01T00:00:00Z","swapexp":"2014-07-
01T00:00:00Z","facuri":"https://facilitator.dom/api/v1"}' ...
https://facilitator.dom/api/v1/swap
{"ok":true,"offersha256":"3a72...f9a4","offerref":"facswap:3a72...
.f9a4","offeruri":"https://facilitator.dom/api/v1/swap/3a72...f9a
4"}
```

ID: **9fcd...429c**

...

Output:

Value: **150000000**

scriptPubKey: **666163737761703a3a72...f9a4 OP_DROP 1**
67c1...4a70 cffd...1373 2 OP_CHECKMULTISIG

...

“666163737761703a” is hexadecimal for the eight byte ascii string “facswap”.

Alternate embodiment example offer transaction:

```
% # Post the terms to the facilitator
% curl -X POST -d '{"pubkey":"67c1...4a70","terms":
{"base":"USD",...,"facuri":"https://facilitator.dom/api/v1"}'}' ..
. https://facilitator.dom/api/v1/swap
{"ok":true,"offersha256":"3a72...f9a4","offerref":"facswap:3a72...
.f9a4","offeruri":"https://facilitator.dom/api/v1/swap/3a72...f9a
4","offertxn":"04000000...0280d1f0080000000008901014b67c1...4a704b
cffd...13730102ae...00000000000000002a6a28666163737761703a3a72...
f9a400000000"}
```

⌘ **# Validate "offertxn", add change outputs, etc.**

"offertxn" is annotated as follows:

```
04000000 [version: 4] ... 02 [output count: 1] 80d1f00800000000
[amount: 1.5 BTC] 89 [script len: 137] 01 [push next 1 byte] 01
[1] 4b [push next 75 bytes] 67c1...4a70 [pub. key] 4b [push next
75 bytes] cffd...1373 [fac. pub. key] 01 [push next 1 byte] 02
[2] ae [OP_CHECKMULTISIG] ... 0000000000000000 [amount: 0.0 BTC]
2a [script len: 42] 6a [OP_RETURN] 28 [push next 40 bytes]
666163737761703a3a72...f9a4 [offerref: "facswap:3a72...f9a4"]
00000000 [lock time: none]
```

Note that some parts (such as any inputs or input placeholders) have been skipped with ellipses to assist with readability. In an alternate embodiment, Pay-to-Script Hash (P2SH) is used.

2. In one embodiment, the first client creates, or, in another embodiment, the facilitator creates an inchoate commit transaction for creating a complete commit transaction much like those described in previous embodiments, except whose first commit input is for accepting the offer amount from the offer transaction, and whose second input is for accepting an amount from a source transaction yet to be identified.
3. The first client signs and broadcasts the signed offer transaction.
4. The facilitator receives the broadcast signed offer transaction.
5. A second client transmits a public key to the facilitator.
6. The facilitator adds the public key to the inchoate commit transaction and transmits the inchoate commit transaction to the second client.
7. The second client signs a source transaction having a transaction ID.
8. The second client adds the transaction ID to the inchoate commit transaction and signs it.

Example inchoate commit transaction:

Input:

Previous tx: **9fcd...429c**

Index: **0**

scriptSig: **[sig. placeholder]**

Input:

Previous tx: **b5e8...6f57**

Index: **6**

scriptSig: **9b6b...8f3701 ac2f...b01b**

...

Output:

Value: **149990000**

scriptPubKey: **2 67c1...4a70 dbe4...4cbe cffd...1373 3
OP_CHECKMULTISIG**

...

9. The second client transmits the signed inchoate commit transaction to the facilitator.
10. Either the first client or, optionally (where allowed), the facilitator creates the complete commit transaction (e.g., ID: 6996...ec3d) by signing the inchoate commit transaction, optionally storing the complete commit transaction in non-transitory memory.

Embodiments where one of the first party and the facilitator can approve spending the offer output require the first party to trust the facilitator to perform some verification (e.g., that the second source transaction has sufficient assets, that a nefarious party is not attempting to commit a huge number of very tiny inputs such that the mining fee will be large, or difficult to meet, etc.) and to craft the commit transaction correctly and consistently with the terms.

11. The facilitator creates an inchoate refund or expiration transaction and transmits the inchoate refund or expiration transaction to the second client.
12. The second client signs the inchoate refund or expiration transaction and transmits the signed inchoate refund or expiration transaction to the facilitator.
13. Either the first client or, optionally (where allowed), the facilitator creates the complete refund or expiration transaction by signing the inchoate refund transaction, storing the complete refund or expiration transaction in non-transitory memory.
14. The facilitator transmits the complete commit transaction and the complete refund or expiration transaction to the second client.
15. The second client broadcasts the source transaction.
16. After seeing that the source transaction has been broadcast, one, several, or all of the first client, the second client, and the facilitator broadcast the complete commit transaction, after which the process is analogous to previously described embodiments.

[81] In an alternate embodiment, the offer comprises a “hard offer”, the condition of the offer output requires approval of both the first party and the facilitator, and the facilitator signs and transmits to the first party an offer expiration transaction comprising a lock time set to the time the hard offer expires, an input for receiving the offer amount, and an expiration output comprising an expiration amount and a condition requiring approval of the first party.

[82] In other embodiments of the invention, the transacting parties agree on a third party to act as a mediator in a dispute. For example, if the facilitator becomes unavailable, rather than electing to invoke a refund, one party triggers a dispute whereby a mediator stands in place of the unavailable facilitator. The condition of the commit output of the complete commit transaction requires approval of two of the first party, the second party, the facilitator, and the mediator. On or after the expiration time, or at a time or upon an event as defined by the terms, and before the lock time of the complete refund transaction, each of the disputing party and the mediator signs and one party broadcasts a dispute transaction comprising an input for receiving the commit amount from the complete commit transaction, and a dispute output comprising a dispute amount and a condition requiring approval of two of the first party, the second party, and the mediator. Once the dispute has been resolved, either the parties sign, or the mediator and one of the parties sign a settlement transaction similar to the disbursement transaction above,

but reflecting the mediated settlement.

[83] FIGS. 15-16 depict aspects of two such embodiments. In FIG. 15, the dispute transaction further comprises a first fee output comprising a facilitator fee amount (ϕ_x) and second fee output comprising a mediator fee amount (ϕ_m), the fees being shared by the parties. In FIG. 16, the dispute transaction comprises the facilitator fee amount shared by the parties, and the settlement transaction comprises the mediator fee amount paid by the party that initiated the dispute (B). In another embodiment, any mediator fee is determined as a term of the settlement, and included with the settlement transaction.

[84] Optionally (and preferably), the parties also sign and transmit to each other a dispute refund transaction similar to that above, but instead taking its input from the dispute transaction, and with a lock time set in the future with enough time to reach a settlement. This way if the mediator becomes unavailable, the parties can again revert to broadcasting a refund. In another embodiment, the dispute transaction could also be “mediatable”, allowing for a chain of such disputes, for example naming a second mediator in the event that the mediator becomes unavailable, or the same mediator to allow more time to reach a settlement if the lock time of the dispute refund transaction is approaching.

[85] In other embodiments, mediation can be automated. For example, in embodiments pertaining to swaps or similar transactions, the facilitator periodically transmits an unsigned disbursement transaction to the parties as if the trade were halted at the time the unsigned disbursement transaction is created. The unsigned disbursement transaction comprises a verifiable time at which it was created, or a reference to such a time (e.g., where the transfer mechanism is the Bitcoin or similar protocol, as unused but signed data embedded in one of the scripts, signature by a separate key owned by the facilitator, but not used for signing any inputs, etc.). If the facilitator becomes unavailable before it can transmit the signed disbursement transaction, and remains unavailable past the expiration time, a dispute could be initiated, and the parties would have a window during which they have an opportunity to transmit the terms (preferably signed by each party, but this is not necessary if the parties agree on the terms, i.e., both transmit the same terms to the mediator) and some or all of the unsigned disbursement transactions they received from the facilitator to the mediator. The mediator examines the terms and the disbursement transactions presented by both parties. The mediator examines the undisputed or signed terms, and all verifiable unsigned disbursement transactions received from both parties. In one embodiment, the mediator merely selects the most recent verifiable

unsigned disbursement transaction. In another embodiment, the mediator “plays back” the unsigned disbursement transactions in order, verifying whether any unsigned disbursement transaction should have triggered an early exit to the trade (e.g., if collateral was exhausted). In yet another embodiment, the mediator performs its own independent evaluation of the terms, possibly requesting information from an oracle, to stand in place of the facilitator by creating a new settlement transaction as close to the disbursement transaction that would have been created by the facilitator if it was available as the mediator is able to determine.

[86] Note that the depicted embodiments are among the more basic of the invention. The various combinations of source transactions, commit transactions, disbursement transactions, refund transactions, expiration transactions, inputs, outputs, and parties, as well as any principal, collateral, or fees, are limited only by the agreements among the participating parties and are enabled by the invention. Additionally, certain steps of the embodiments disclosed throughout this application are described as being performed by certain entities. In other embodiments, similar or equivalent steps could be performed—wholly or partly—by different parties in lieu of or in addition to those described herein. All such embodiments are considered within the scope of the invention.

[87] As a very simple example, in an embodiment using the Bitcoin protocol, the Ethereum protocol, or similar, transactions use P2SH in place of multi-sig transactions. Other steps may be omitted in certain embodiments. For example, in an embodiment using the Bitcoin or similar protocol, the creation of the signed complete refund or expiration transaction—while highly recommended as a contingency to avoid loss in case the facilitator or counterparty disappears or becomes uncooperative—is not strictly necessary to practice the invention. In embodiments involving a mediator, an unsigned dispute transaction could be created by the facilitator and transmitted to the parties for use with the mediator, for example, at the time the refund or expiration transaction is created and transmitted.

INDUSTRIAL APPLICABILITY

[88] The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance.

CLAIMS

What is claimed is:

1. A method for performing low-trust or zero-trust transactions between a first client at least intermittently connected to a second client, the method comprising the steps:
 - a. creating an offer, the offer comprising:
 - i. terms comprising:
 - A. a principal amount; and
 - B. an expiration time;
 - b. creating a commit transaction in accordance with the terms, the commit transaction comprising:
 - i. a first principal input for receiving a first principal amount;
 - ii. a second principal input for receiving a second principal amount; and
 - iii. a commit output comprising a commit amount;
 - c. creating a digital signature to associate with the commit transaction by the first client using a first asymmetric key pair;
 - d. creating a digital signature to associate with the commit transaction by the second client using a second asymmetric key pair;
 - e. broadcasting the signed commit transaction onto a computer network accessible by a transfer mechanism.
2. The method of claim 1, where the terms further comprise a collateral amount, where the commit transaction further comprises one or both of an input for receiving a first collateral amount and an input for receiving a second collateral amount.
3. The method of claim 1, where the commit transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.
4. The method of claim 1, where the terms further comprise:

- a. a reference to a base asset; and
 - b. a reference to a quote asset.
- 5. The method of claim 4 further comprising the steps:
 - a. creating a refund transaction comprising:
 - i. a lock time after the expiration time;
 - ii. an input for receiving the commit amount from the commit transaction;
 - iii. a first refund output comprising a first refund amount and a first refund condition requiring approval from a first party; and
 - iv. a second refund output comprising a second refund amount and a second refund condition requiring approval from a second party; and
 - b. storing the refund transaction in a non-transitory computer memory.
- 6. The method of claim 5 further comprising the steps:
 - a. calculating a first disbursement amount and a second disbursement amount in accordance with the terms;
 - b. creating a disbursement transaction comprising:
 - i. an input for receiving the commit amount from the commit transaction;
 - ii. a first disbursement output comprising a first disbursement amount and a first disbursement condition requiring approval from the first party; and
 - iii. a second disbursement output comprising a second disbursement amount and a second disbursement condition requiring approval from the second party; and
 - c. broadcasting the disbursement transaction onto the computer network before the lock time of the refund transaction.
- 7. The method of claim 4 further comprising the steps:

- a. calculating a first disbursement amount and a second disbursement amount in accordance with the terms;
 - b. creating a disbursement transaction comprising:
 - i. an input for receiving the commit amount from the commit transaction;
 - ii. a first disbursement output comprising the first disbursement amount and a first disbursement condition requiring approval from the first party; and
 - iii. a second disbursement output comprising the second disbursement amount and a second disbursement condition requiring approval from the second party; and
 - c. broadcasting the disbursement transaction onto the computer network.
8. The method of claim 7, where the step of calculating the first disbursement amount and the second disbursement amount in accordance with the terms is performed on or after the expiration time.
9. The method of claim 7, where the disbursement transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.
10. The method of claim 1, where the terms further comprise:
- a. a disbursement condition.
11. The method of claim 10 further comprising the steps:
- a. creating an expiration transaction comprising:
 - i. a lock time after the expiration time;
 - ii. an input for receiving the commit amount from the commit transaction; and
 - iii. an expiration output comprising an expiration amount and an expiration condition requiring approval from a first party; and

- b. storing the expiration transaction in a non-transitory computer memory.
- 12. The method of claim 10 further comprising the steps:
 - a. calculating a disbursement amount in accordance with the terms;
 - b. creating a disbursement transaction comprising:
 - i. an input for receiving the commit amount from the commit transaction;
 - ii. a disbursement output comprising the disbursement amount and a disbursement condition requiring approval from the second party; and
 - c. broadcasting the disbursement transaction onto the computer network.
- 13. The method of claim 12, where the step of calculating the disbursement amount in accordance with the terms is performed on or after the expiration time.
- 14. The method of claim 12, where the disbursement transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.
- 15. The method of claim 11 further comprising the steps:
 - a. creating a dispute transaction comprising:
 - i. an input for receiving the commit amount from the commit transaction; and
 - ii. a dispute output comprising a dispute amount; and
 - b. broadcasting the dispute transaction onto the computer network before the lock time of the expiration transaction.
- 16. The method of claim 15, where the dispute transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.
- 17. The method of claim 15 further comprising the steps:
 - a. creating a settlement transaction comprising:

- i. an input for receiving the dispute amount from the dispute transaction;
 - ii. one of:
 - A. a first settlement output comprising a first settlement amount and a first settlement condition requiring approval from a first party; and
 - B. a second settlement output comprising a second settlement amount and a second settlement condition requiring approval from a second party; and
 - b. broadcasting the settlement transaction onto the computer network.
- 18. The method of claim 17, where the dispute transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.
- 19. The method of claim 5 further comprising the steps:
 - a. creating a substitution transaction comprising:
 - i. a commit input for receiving the commit amount from the commit transaction;
 - ii. an entry input for receiving an entry amount;
 - iii. a withdrawal output comprising a withdrawal amount and a first condition requiring approval of one of the first party and the second party; and
 - iv. a substitution output comprising a substitution amount;
 - b. creating a digital signature to associate with the substitution transaction by a third client using a third asymmetric key pair; and
 - c. broadcasting the substitution transaction onto the computer network before the lock time of the refund transaction.
- 20. The method of claim 19, where the substitution transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third

party.

21. The method of claim 19 further comprising the steps:
 - a. creating a substitute refund transaction comprising:
 - i. a lock time after the expiration time;
 - ii. an input for receiving the substitution amount from the substitution transaction;
 - iii. a first refund output comprising a first refund amount and a first refund condition requiring approval from a third party; and
 - iv. a second refund output comprising a second refund amount and a second refund condition requiring approval from a second party; and
 - b. storing the substitute refund transaction in a non-transitory computer memory.
22. The method of claim 21 further comprising the steps:
 - a. calculating a first disbursement amount and a second disbursement amount in accordance with the terms;
 - b. creating a disbursement transaction comprising:
 - i. an input for receiving the substitution amount from the substitution transaction;
 - ii. a first disbursement output comprising a first disbursement amount and a first disbursement condition requiring approval from the third party; and
 - iii. a second disbursement output comprising a second disbursement amount and a second disbursement condition requiring approval from the second party; and
 - c. broadcasting the disbursement transaction onto the computer network before the lock time of the substitute refund transaction.
23. The method of claim 22, where the step of calculating the first disbursement amount and the second disbursement amount in accordance with the terms is performed on or after

the expiration time.

24. The method of claim 22, where the disbursement transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.
25. A system for performing low-trust or zero-trust swap transactions comprising terms, the system comprising a facilitator coupled to a computer network accessible by a transfer mechanism, the facilitator comprising:
 - a. an interface for receiving terms comprising:
 - i. a reference to a base asset;
 - ii. a reference to a quote asset;
 - iii. a principal amount; and
 - iv. an expiration time;
 - b. a first non-transitory memory for storing a first asymmetric key pair; and
 - c. a first computer processor configured for one of:
 - i. transmitting a transaction to a client, the client comprising:
 - A. an interface for receiving a transaction;
 - B. a second non-transitory memory for storing a second asymmetric key pair and a transaction; and
 - C. a second computer processor configured for one of:
 - I. signing a transaction using the second asymmetric key pair; and
 - II. transmitting a signed transaction over the computer network;
 - ii. signing a transaction using the first asymmetric key pair;

- iii. calculating a first disbursement amount and a second disbursement amount in accordance with the terms;
 - iv. creating a disbursement transaction comprising:
 - A. a first disbursement output comprising a first disbursement amount and a first disbursement condition requiring approval from a first party; and
 - B. a second disbursement output comprising a second disbursement amount and a second disbursement condition requiring approval from a second party; and
 - v. broadcasting the disbursement transaction onto the computer network.
26. The system of claim 25, where the second non-transitory memory is further for storing a complete transaction.
27. The system of claim 25, where the first computer processor is the second computer processor, and where the first non-transitory memory is the second non-transitory memory.

ABSTRACT

Systems and methods enabling parties with little trust or no trust in each other to enter into and enforce agreements conditioned on input from or participation of a third party, over arbitrary distances, without special technical knowledge of the underlying transfer mechanism(s), optionally affording participation of third-party mediators, substitution of transferors and transferees, term substitution, revision, or reformation, etc. Such transactions can occur reliably without involving costly third-party intermediaries who traditionally may otherwise be required for such transactions, and without traditional exposure to counterparty risk..

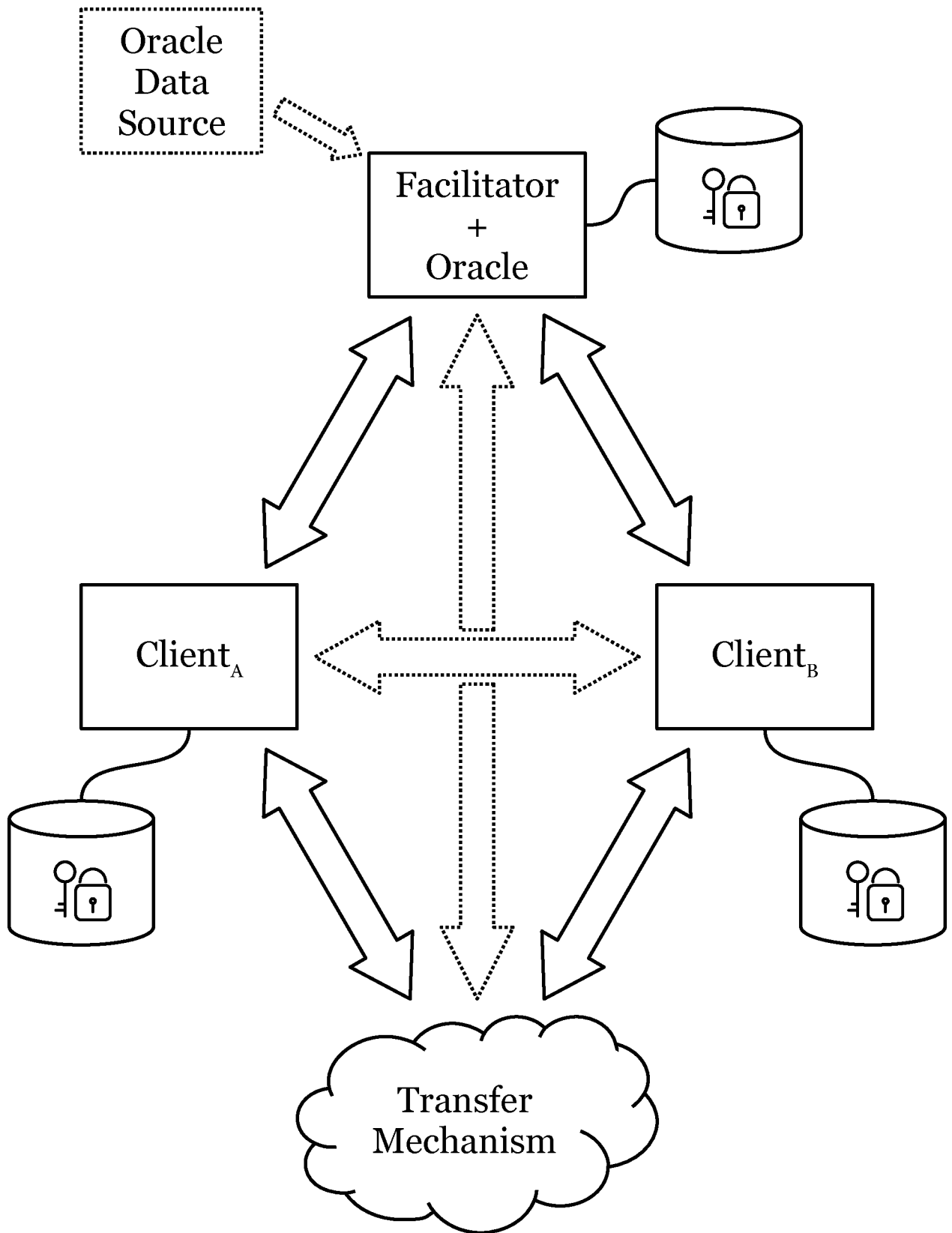


FIG. 1

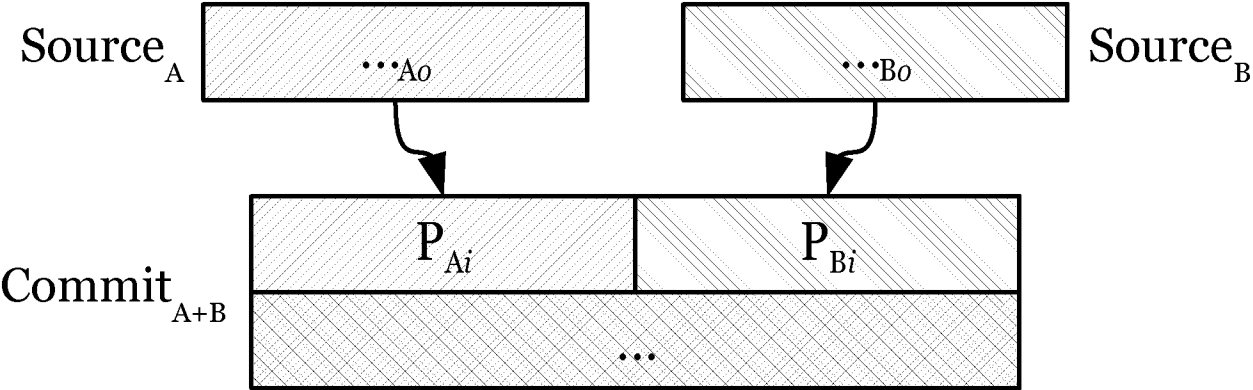


FIG. 2

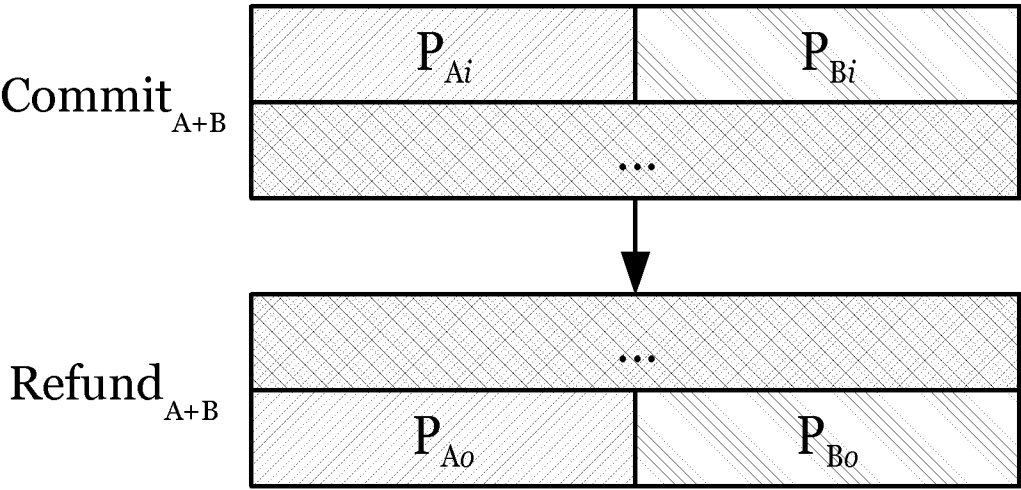


FIG. 3

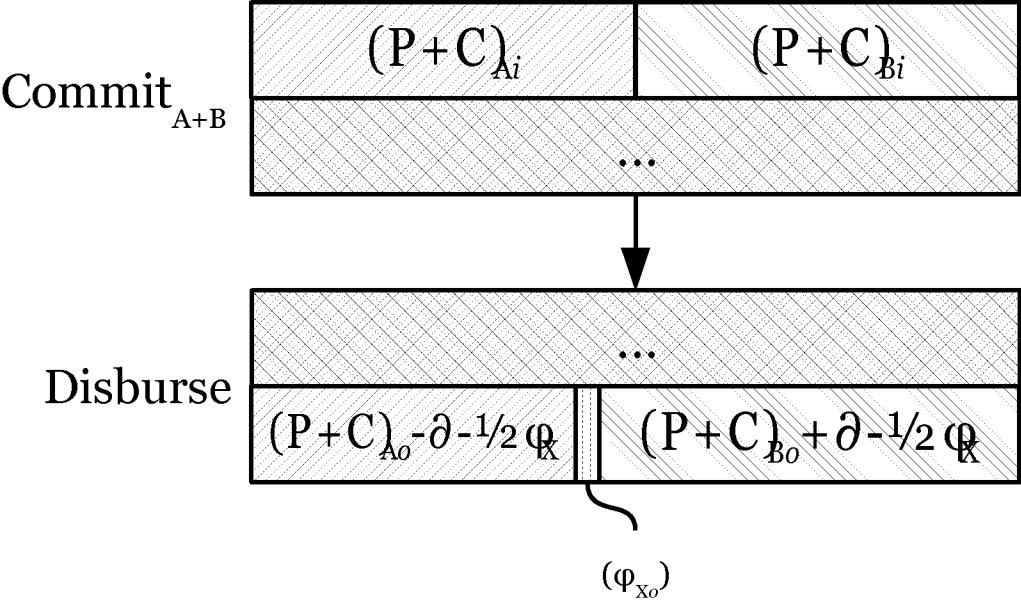


FIG. 4

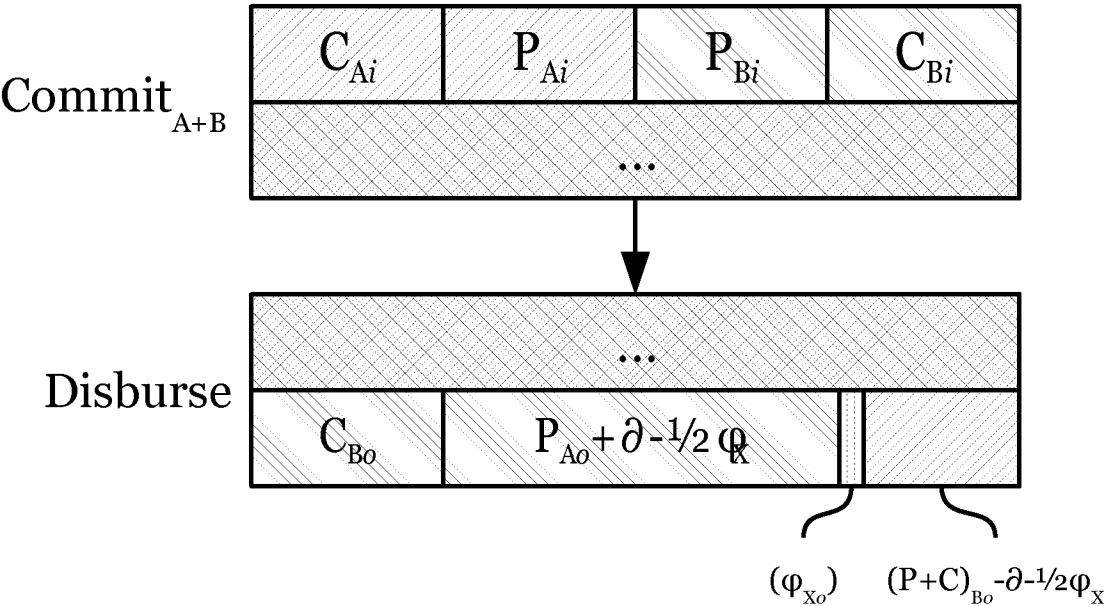


FIG. 5

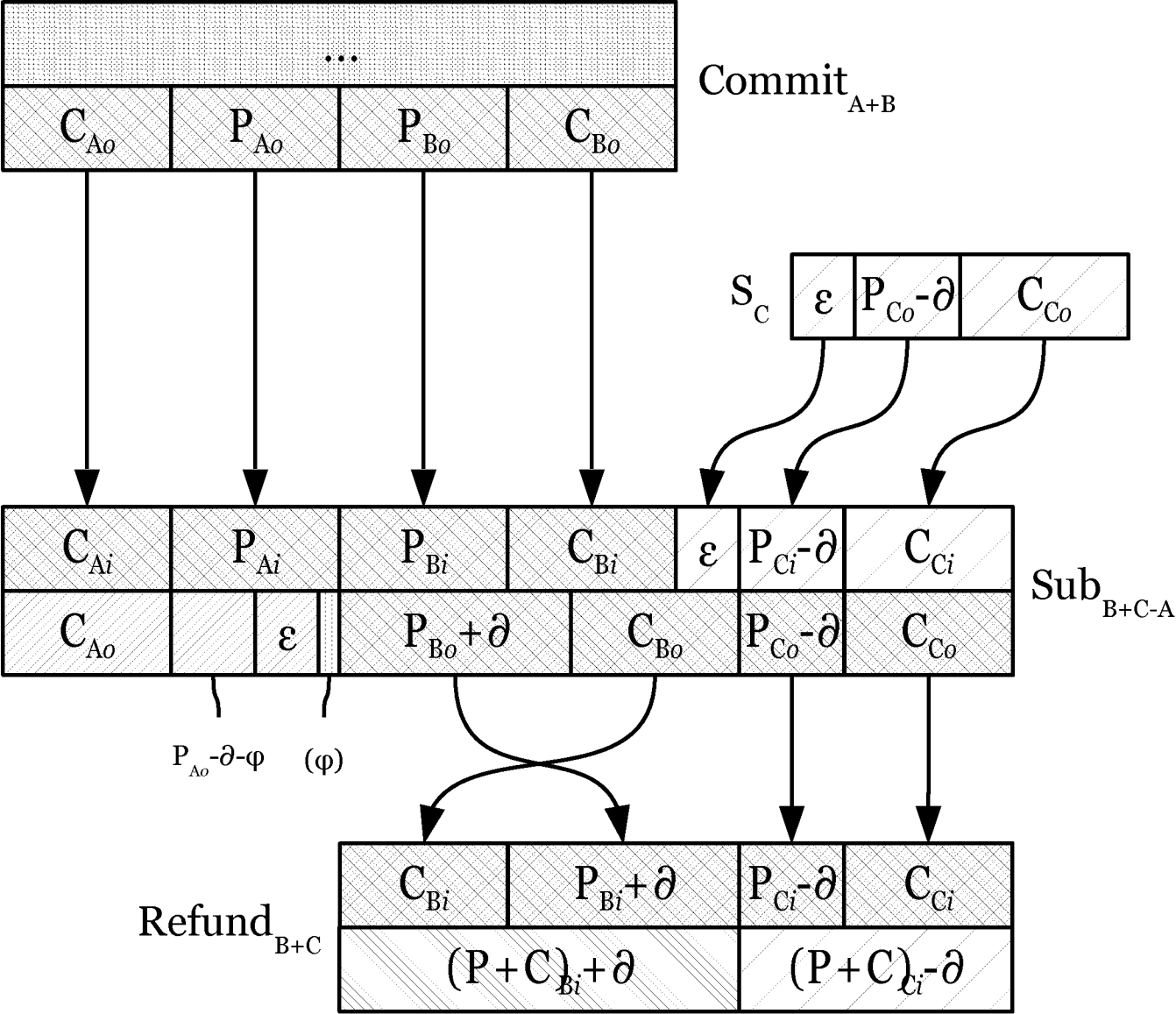


FIG. 6

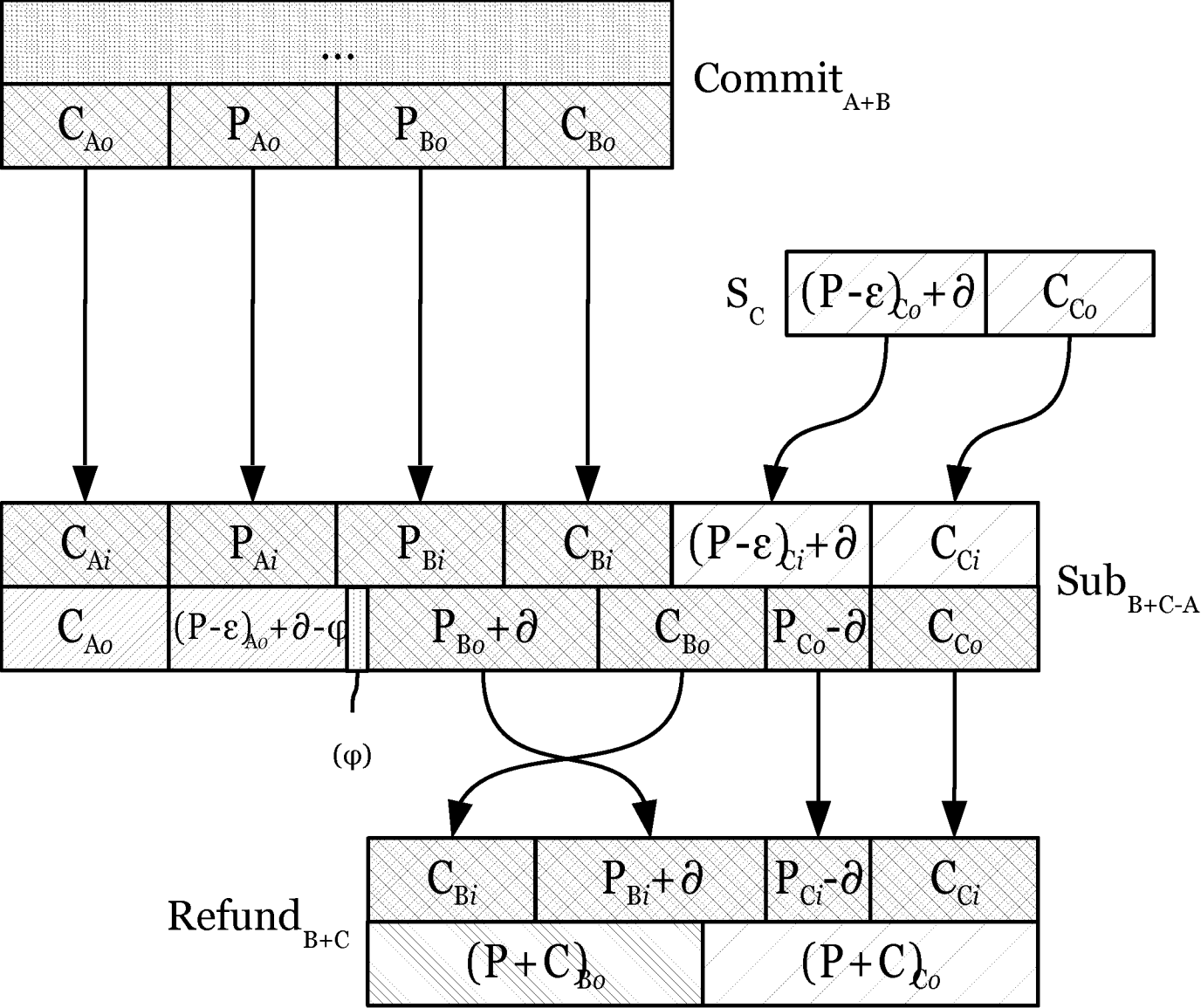


FIG. 7

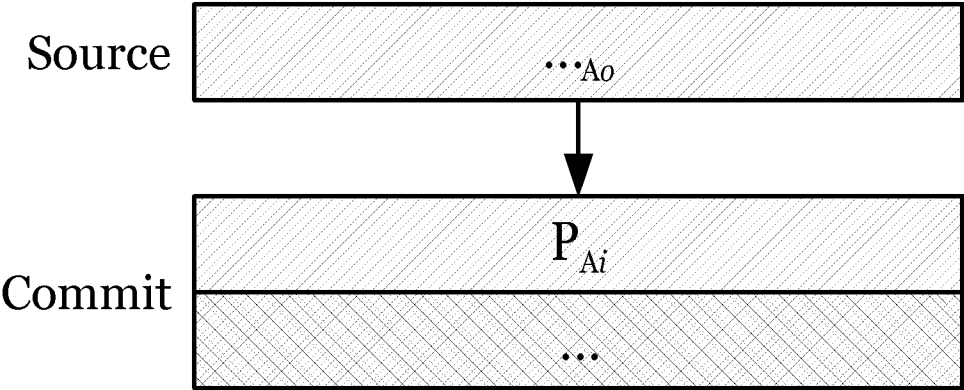


FIG. 8

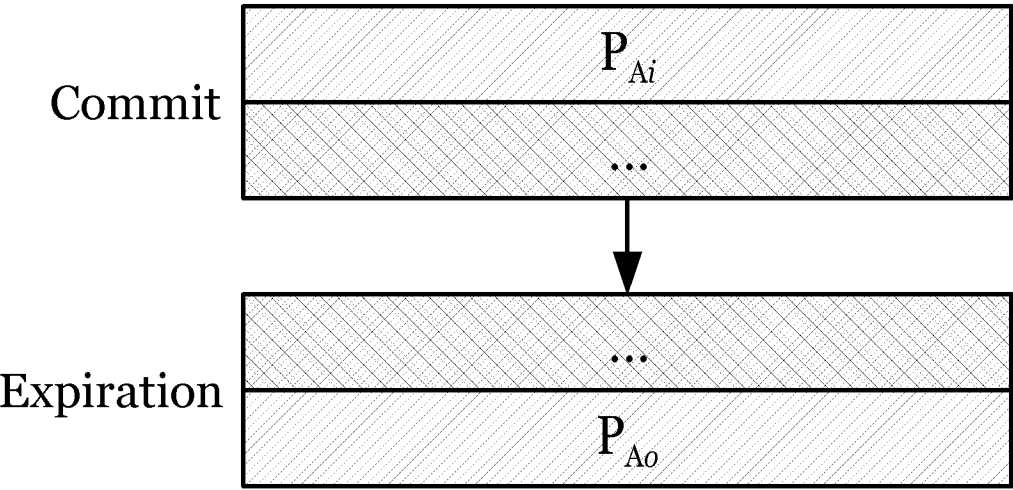


FIG. 9

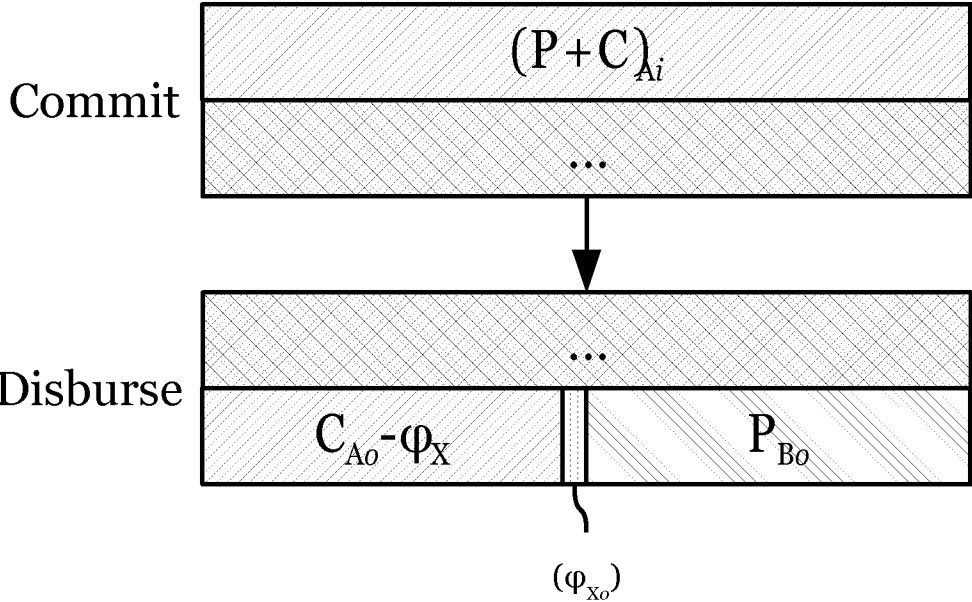


FIG. 10

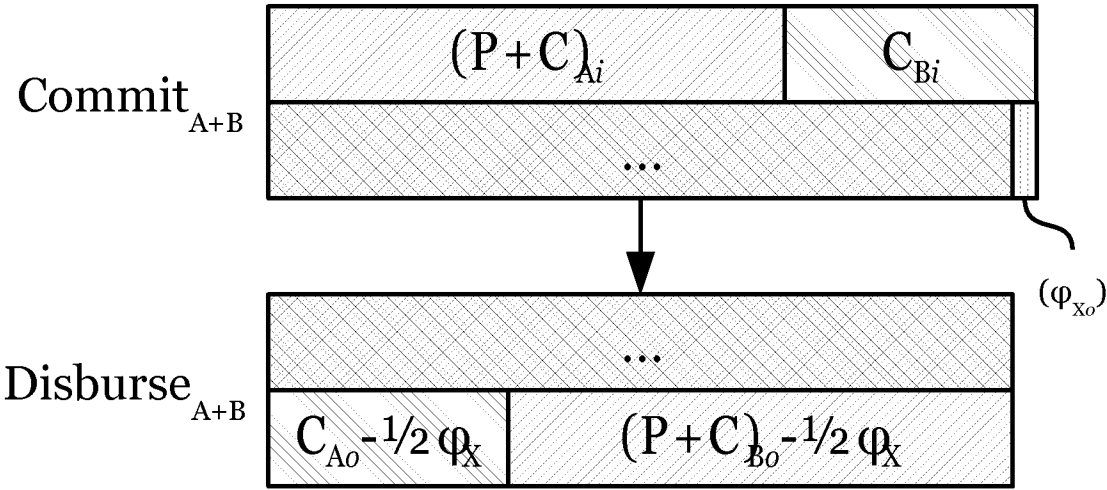


FIG. 11

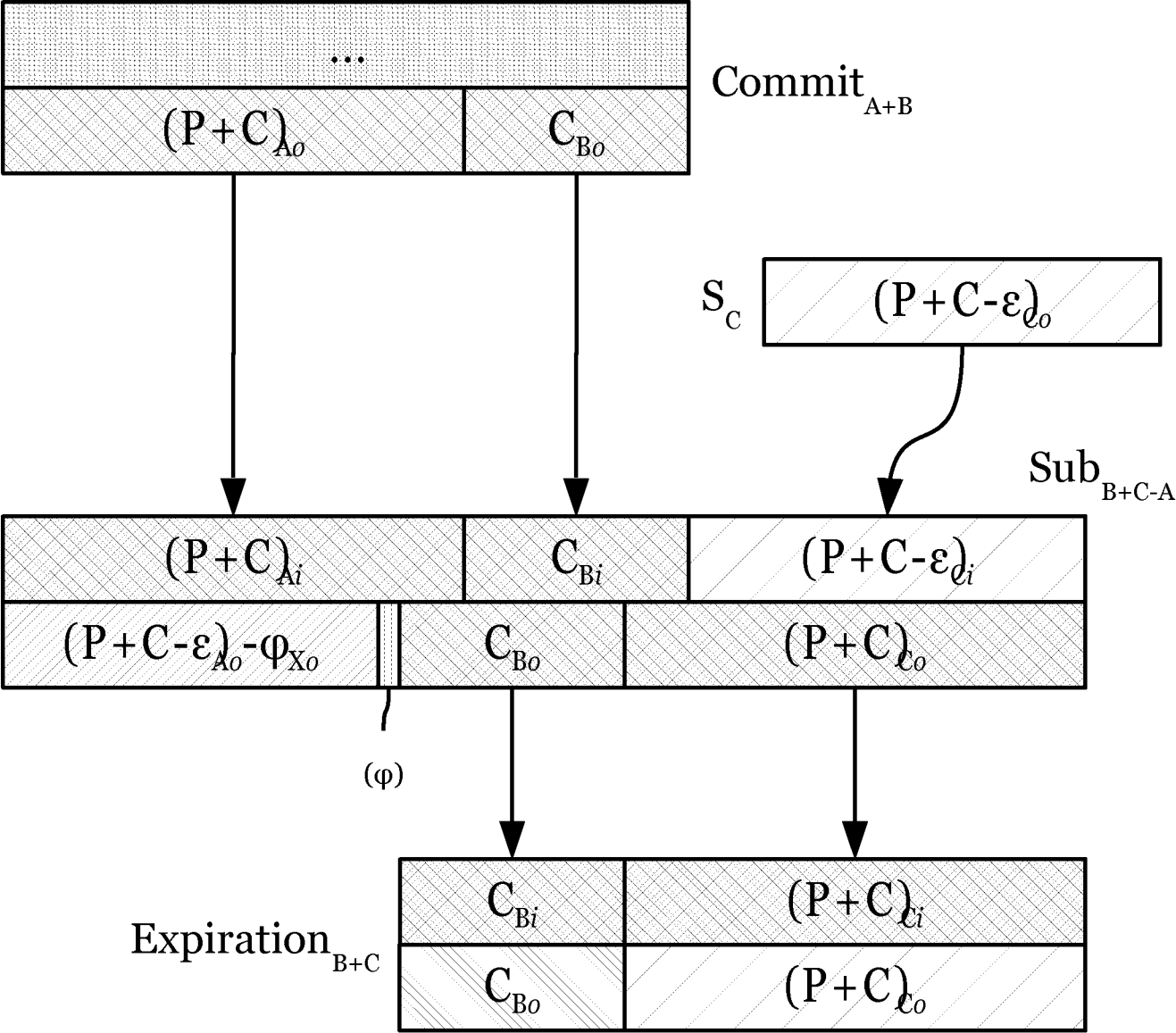


FIG. 12

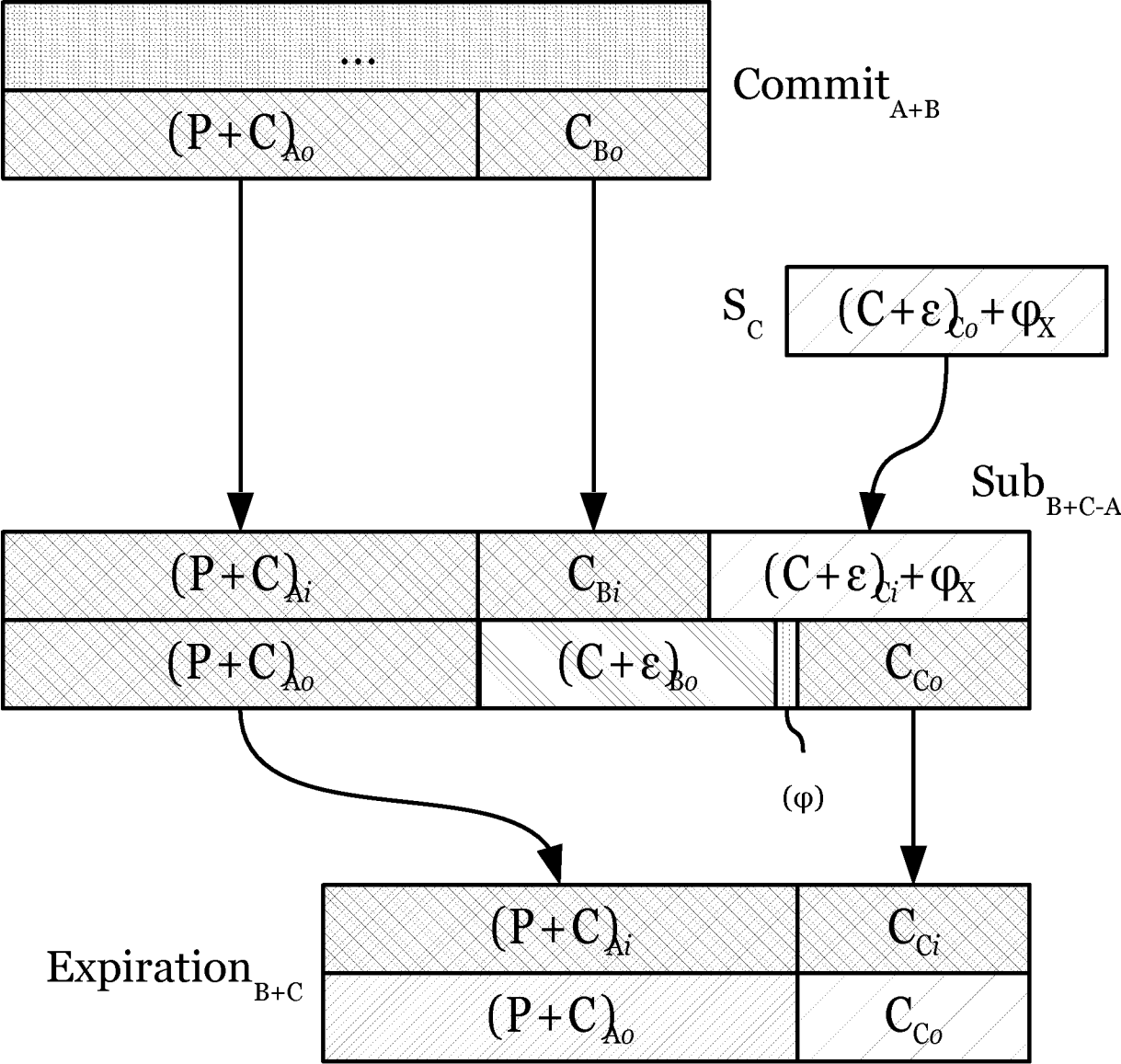


FIG. 13

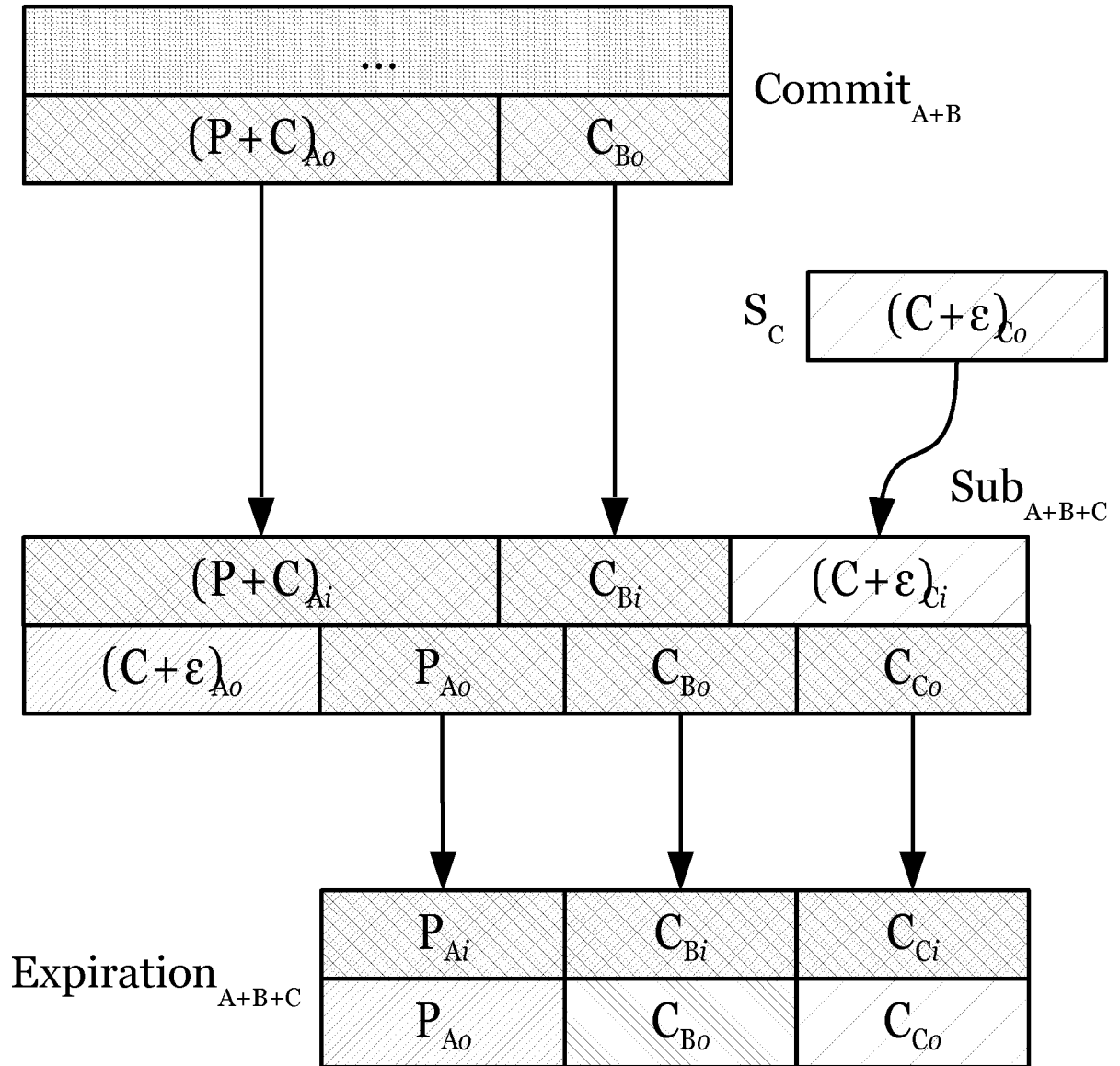


FIG. 14

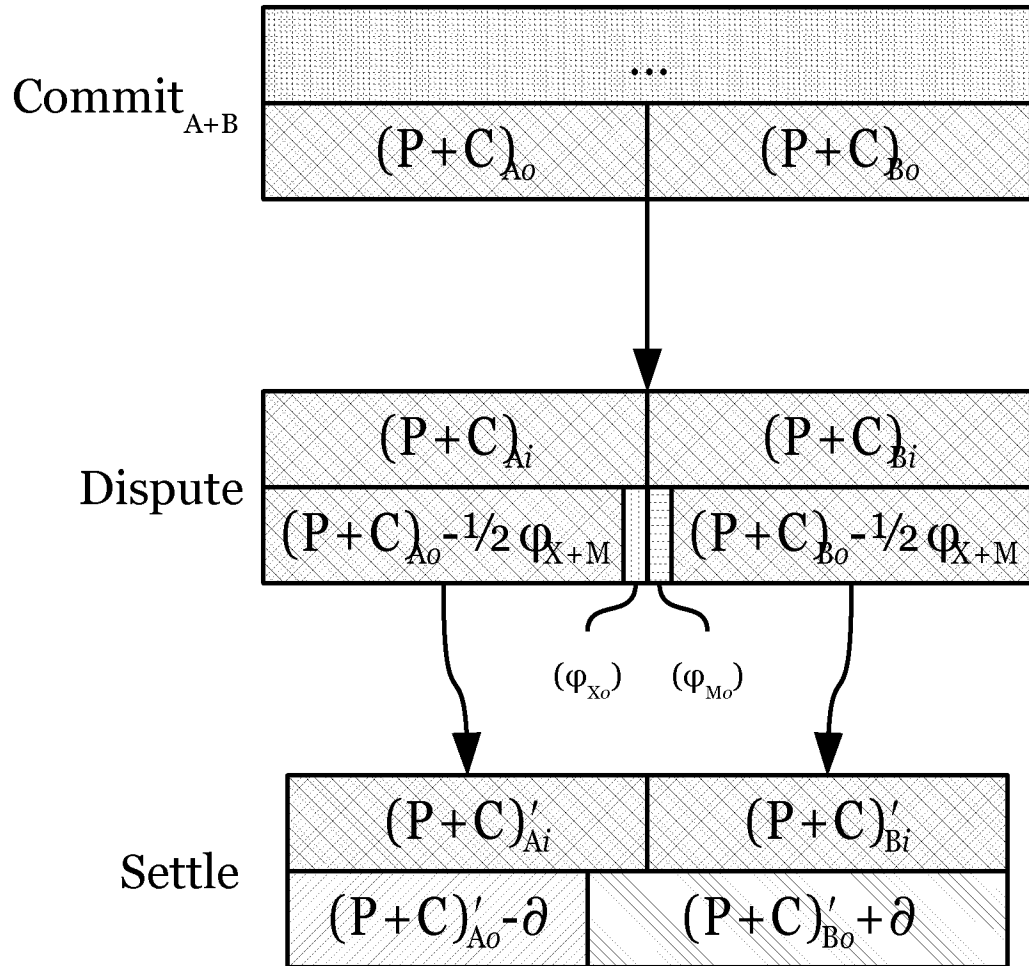


FIG. 15

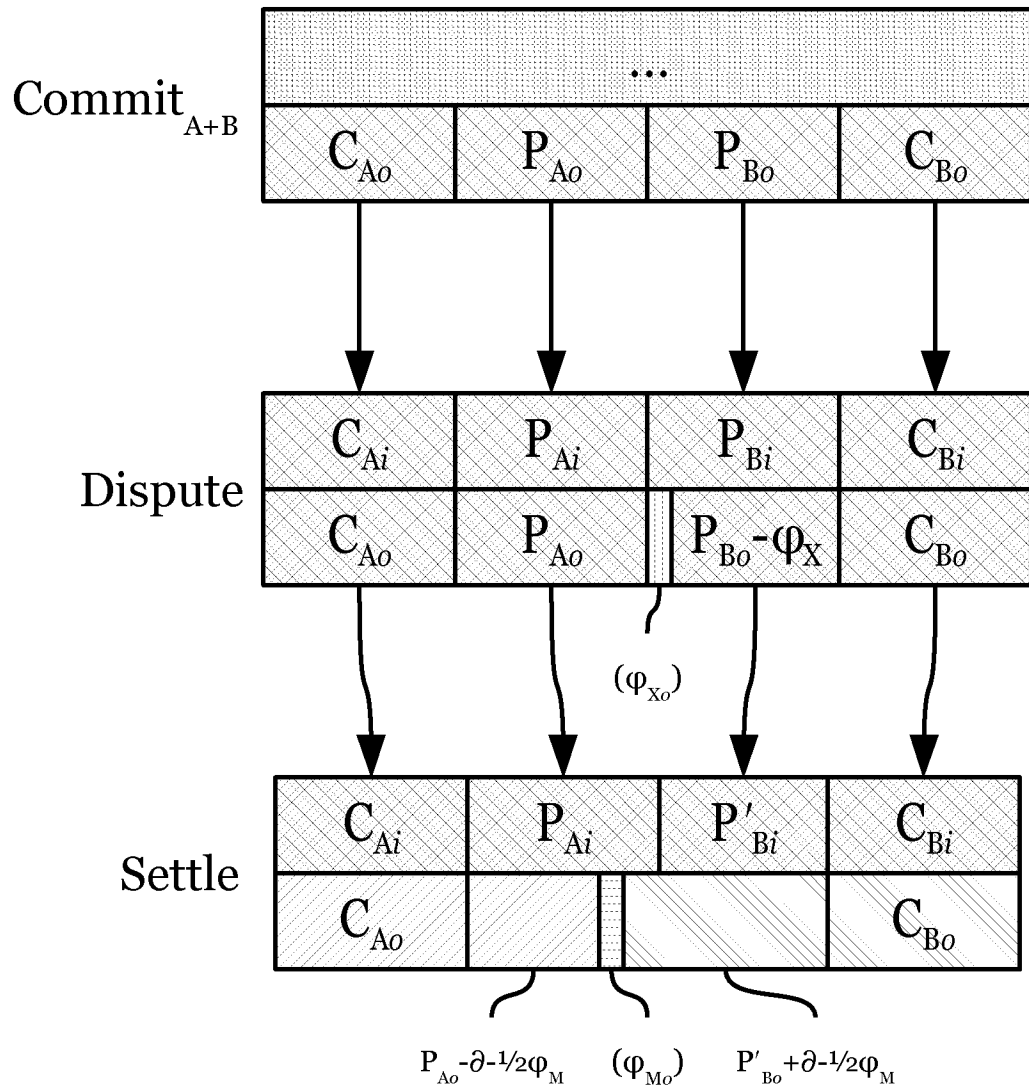


FIG. 16

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SYSTEMS AND METHODS FOR LOW TRUST AND ZERO TRUST TRANSACTIONS		
First Named Inventor/Applicant Name:		Reginald C. Middleton		
Filer:		Matthew Thomas Bogosian		
Attorney Docket Number:		UC-LC-PROV1		
Filed as Small Entity				
Provisional Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Provisional Application Filing Fee	2005	1	130	130
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				130

Electronic Acknowledgement Receipt

EFS ID:	18986713
Application Number:	61990795
International Application Number:	
Confirmation Number:	8467
Title of Invention:	SYSTEMS AND METHODS FOR LOW TRUST AND ZERO TRUST TRANSACTIONS
First Named Inventor/Applicant Name:	Reginald C. Middleton
Customer Number:	94276
Filer:	Matthew Thomas Bogosian
Filer Authorized By:	
Attorney Docket Number:	UC-LC-PROV1
Receipt Date:	09-MAY-2014
Filing Date:	
Time Stamp:	11:23:59
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 130
RAM confirmation Number	7336
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1		ultracoin_lc_app-20140509.pdf	2835898 fb6f02c208b1e911e232a40790393037fae97871	yes	75
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Provisional Cover Sheet (SB16)		1	2	
	Specification		3	54	
	Claims		55	62	
	Abstract		63	63	
	Drawings-only black and white line drawings		64	75	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	29622 6f4f88113a54049f97b970a54cdf6c9166a4f361	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2865520		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.					