A payment processor receives currency information and identification information. The currency information comprising a payer fiat-currency and a payee fiat-currency and the identification information comprises information verifying the identity of a payer and a payee. The payment processor utilizes the currency information and the identification information to determine a transaction restriction level and verifies that the identification information meets the threshold for the transaction restriction level. The payment processor receives payment in the payer fiat-currency and initiates a transaction to convert the payer fiat-currency amount into a crypto-currency amount. The payment processor converts the crypto-currency amount into the payee fiat-currency. The payment processor initiates a transfer of the payee fiat-currency amount to the payee.
SYSTEM AND METHOD FOR PAYMENT PROCESSING USING CRYPTO CURRENCIES

CROSS-REFERENCE TO RELATED APPLICATION(S)


FIELD OF THE INVENTION

[0002] The present invention is related to the field of payment processing and currency exchange using cryptocurrencies.

BACKGROUND OF THE INVENTION

[0003] Currencies may be transferred from a payer to a payee for various reasons. A buyer may purchase goods or services from a merchant in person, via telephone or through an Internet web site. A merchant or business may be paying a supplier, employees, sales people, consultants, or others. They may also be issuing refunds or rebates to customers or suppliers, or making payments as part of an affiliate program with another business or individual. Businesses may be paying salaries to employees or consultants on a reoccurring or one-time basis. There are a number of other situations where an individual will be simply transferring currencies to an associate or family member in another country. Payments may be small or large and completion of the payment may be required quickly or to be completed at a specific time, for example, at the end of the business day in a particular time zone. Payments may be made in the same or different currencies.

[0004] When dealing with financial transactions between countries, the currency of a sender is often exchanged for the local currency of the receiver. Currencies are publically traded on global foreign exchanges which sets a base bid and ask rate for each currency with respect to other currencies.

[0005] Currencies may be the fiat-currency of a country such as a US dollar, Euro, or Yen or may be a crypto-currency, of which bitcoin is one example. While fiat-currencies are usually exchanged at a bank or currency exchange using well established rules, crypto-currencies transactions are based on a blockchain, a digital ledger used to record transactions, and are exchanged through crypto-exchanges. The term currency can be used generally to refer to
both a fiat-currency and a crypto-currency. The term exchange can be used generally to refer to both a bank or currency exchange for fiat-currencies, and to refer to a crypto-exchange that utilizes a blockchain or similar technology to record exchanges. Exchange rates apply to conversions between two fiat-currencies, two crypto-currencies, or between a fiat-currency and a crypto-currency.

[0006] When the payments are exchanged, the process can be described as a "rail." The rail can be visualized as the path the transaction takes from sender to receiver. A sender may deposit an amount of their local fiat-currency into their local bank account and initiate a transfer to a receiver in another country. The deposited fiat-currency may be exchanged at the bank into an intermediate currency and then transferred to the receiver. The route the transfer takes from bank to first exchange to second exchange is the rail that was utilized for the transaction. A payment transaction can use multiple rails to transfer an amount of currency from the sender to the receiver.

[0007] At any point in time, there is a global exchange rate between currencies that is decided by the large global exchanges or payment processors. Smaller exchanges will use a variation of the bid and ask rate that is based on the global exchange rate. The spread between the bid and ask rate represents part of the cost of the transaction. A small spread, the difference between the bid and ask rate, reduces the cost of the transaction while a large spread increases the cost. National banks, large banks, and large corporations transferring large amounts of currency typically benefit from a small spread. Smaller companies and individuals usually pay more.

[0008] As well as the spread between the rates, many exchanges charge a fee to the sender, the receiver, or both parties. The fees vary between exchanges but for most fiat-currency exchanges, the fees for a particular exchange vary slowly over time. When a sender or receiver requires a transfer of funds, the payment processor determines what rail to use for their transaction by querying the bank or exchange for their fees and their bid and ask prices for that day and decide which rail to use. When only using fiat-currencies and fiat-exchanges for the transaction, the task of choosing a rail to minimize costs can be done manually, by deciding to use one or two well-known exchanges, or by using, computer aided methods.

[0009] Digital or crypto-currencies have been developed that can be used to provide payment for goods and service and be used by both payers and payees and be used for both domestic and international transfers, payments and exchanges. Crypto-currencies are a medium of exchange designed around securely exchanging information and value. A crypto-currency can
be centralized or decentralized. Crypto-currencies may take the form of digital data but may also be physically represented by cards or printed paper.

[0010] Public-private key pairs are used to ensure the security of crypto-currencies. Public and private key pairs together, separately and individually are used to sign transactions, crypto currencies or other related ecommerce transactions in order to unlock value or show ownership of a particular crypto currency, transaction or combination thereof.

[0011] Keys may be simple or complex and the more complex the key and its associated management and application, the more secure the use of crypto-currencies. Addresses are used to refer to public keys, which must be combined with their private keys to access the crypto-currency. To access a crypto currency transaction containing a specific amount of crypto currency a single or combination of public-private key pairs is required.

[0012] In order to use a crypto-currency for a financial transaction it is typically stored in a digital or offline wallet. Crypto-currency wallets are associated with addresses that act as a locator to the wallet to allow depositing and withdrawing from the wallet. Private keys are used to access the wallet addresses.

[0013] Private keys are used to sign a multi-signature address which then cause the payment to be released to the receiver or sent back to the sender. In traditional payments, multi-signature addressed are merely proxies to existing payment types such as cards, bank accounts, wallets, gift cards or other forms of payments.

[0014] Crypto-currencies have the characteristics of being stateless, with transactions done on the Internet and with exchanges located in many countries of the world. Due to their locations and various factors in their home countries such as government regulations, as well as competition between exchanges, each offers different services and charge different rates for those services which may be taken advantage of by new technology. Furthermore, since they are accessed over the Internet, a larger number of crypto-currency exchanges can now be used for as currency exchange rails.

[0015] The exchange rates for crypto-currencies have historically also been extremely volatile with exchange rates versus fiat-currencies quickly changing by large amounts. One reason for the high volatility is the high speed of Internet trading and the speed at which both good and bad news is disseminated and received by investors and traders. The fees for crypto-currency exchanges also change quickly and may be difficult to track.

[0016] By allowing currency exchanges to use both fiat-currency exchanges and crypto-exchanges the number of exchanges is much larger than the case of only using fiat-currencies. The crypto-currency exchange rates and the volatility of fees charged by crypto-
currency exchanges means that the best rail can change in real time. This leads to the situation where the number of possible rails to use for a transaction becomes very large and the cost of utilizing different rails for the transaction can vary widely both between exchanges and over time.

[0017] A payment processor is a company that provides financial services that included the transfer of different currencies or same currencies from a sender to a receiver. The payment processor must charge fees to remain profitable while still offering competitive rates. Due to the use of multiple rails, the task for a payment processor of choosing a rail for a currency transaction is no longer a simple task and requires new methods in order to do it in a timely and effective manner.

[0018] Other than cash payments, there exist a number of methods of making payments including checks, credit or debit card accounts, wire transfers, and many other means. Transaction fees are typically charged by the financial institutions and these fees can be applied to the payer, the payee, or both. In the case where the payer pays in one national or fiat-currency and the payee wishes to receive payment in another fiat-currency, the fiat exchange rate may also represent another type of fee. Fees can be substantial and, in the case of transferring small amounts, could represent a significant amount of the payment or even exceed it.

[0019] Some entities such as companies employing many independent contractors must pay their employees a relatively small amount monthly. The employer often is assessed a per transaction fee for each payment and each independent contractor must often also pay a transaction fee to receive a payment. If the fee is based on the transaction rather than the amount transferred and the amount is small, the fees can amount to a significant portion of the total payment. An extreme case is organizations who deal in micropayments that may be less than $1, $5, or $20 depending on the case. Even very small transaction fees may exceed the amount of the payment, making these types of business models unfeasible.

[0020] The time to make a payment can vary from being almost instantaneous to days, to months for some types of international transfers. Reporting and confirmation of payments can also be an issue with neither the payer nor the payee completely sure who sent a payment, what fees and exchange rates were charges, and if it was actually received. Should a payment be delayed or the received amount not match the expected amount, it can be difficult and time-consuming working with the banks and payment processors to determine what has happened.
[0021] Digital or crypto-currencies have been developed that can be used to provide payment for goods and service and be used by both payers and payees and be used for both domestic and international transfers. Crypto-currencies are a medium of exchange designed around securely exchanging information and value. A crypto-currency can be either centralized or decentralized. Crypto-currencies often require a digital wallet or exchange in order to make or receive payments, and exchanging fiat-currencies with crypto-currencies can be quite difficult.

[0022] Despite the benefits of crypto-currencies, some applications have been criticized as not complying with government regulations regarding money transfers. These regulations include Anti-Money Laundering (AML) policies and Know-Your-Customer (KYC) requirements. Crypto-currencies transactions have been associated with criminal activities and this causes legitimate businesses and banks to avoid their use. There is a lack of trusted crypto-currency exchanges that businesses are willing to use. In particular, public companies or companies subject to regulatory or audit requirements may be prohibited from using exchanges that do not comply with certain government regulations.

[0023] The exchange rate of crypto-currencies to fiat-currencies has also been extremely volatile which has leads to speculation and some holders of crypto-currencies experiencing large gains or losses. Due to this, many businesses and individuals are reluctant to hold crypto-currencies or to use them as a currency for business transactions.

**BRIEF SUMMARY**

[0024] In a first major embodiment of the invention a payment processor receives currency information and identification information. The currency information comprising a payer fiat-currency and a payee fiat-currency, and identification information comprising information verifying the identify of a payer and a payee. The payment processor utilizes the currency information and the identification information to determine a transaction restriction level. The payment processor verifies that the identification information meets a threshold for the transaction restriction level. The payment processor receives payment in the payer fiat-currency and initiates a transaction to convert the payer fiat-currency amount into a crypto-currency amount. The payment processor converts the crypto-currency amount into the payee fiat-currency and initiates a transfer of the payee fiat-currency amount to the payee.

[0025] In some embodiments the payment processor determines criteria to be used to select the crypto-currency and selects the crypto-currency.
[0026] In another embodiment of the invention a payment processor receives currency information and identification information. The currency information comprises a payer fiat-currency and a payee fiat-currency. The identification information comprises information verifying the identity of a payer and a payee. The payment processor utilizes the currency information and the identification information to determine a transaction restriction level. The payment processor verifies that the identification information does not meet a threshold for the transaction restriction level and augments the identification information to meet the threshold for the transaction restriction level. The payment processor receives payment in the payer fiat-currency and initiates a transaction to convert the payer fiat-currency amount into a crypto-currency amount. The payment processor converts the crypto-currency amount into the payee fiat-currency and initiates a transfer of the payee fiat-currency amount to the payee.

[0027] The payment processor may augment the identification information by verifying the identity of the payer or payee with a portion of information provided by the payer and a portion of information provided by the payee.

[0028] A further embodiment of the invention a payment processor receives currency information and identification information. The currency information comprises a payer fiat-currency and a payee fiat-currency. The identification information comprising information comprising a payer trusted level and a payee trusted level. The payment processor utilizes the currency information and the identification information to determine a transaction restriction level. The payment processor verifies that the payer trusted level and the payee trusted level meet a threshold for the transaction restriction level. The payment processor receives payment in the payer fiat-currency and initiates a transaction to convert the payer fiat-currency amount into a crypto-currency amount. The payment processor converts the crypto-currency amount into the payee fiat-currency and initiates a transfer of the payee fiat-currency amount to the payee.

[0029] In a second major embodiment of the invention a payment processor receives a first fiat-currency amount and information comprising a payee deposit destination. The payment processor receives a first plurality of criteria and evaluates a first plurality of exchanges against the first plurality of criteria to select a first transaction exchange from the first plurality of exchanges to initiate a first conversion between a first fiat-currency amount and a cryptocurrency amount. The payment processor receives a second plurality of criteria and evaluates a second plurality of exchanges against the second plurality of criteria. The payment processor selects a second transaction exchange from the second plurality of exchanges to perform a second conversion between the crypto-currency amount and a second
fiat-currency amount. The payment processor initiates a transfer of said second fiat-currency amount to the payee deposit destination.

[0030] In another embodiment of the invention a payment processor receives a first fiat-currency amount and information comprising a payee deposit destination. The payment processor receives a first plurality of criteria and assigns a least a first weighting to at least one of the first plurality of criteria and uses the first weighting to produce a first weighted criteria. The payment processor evaluates a first plurality of exchanges against at least one of the first plurality of criteria and the first weighted criteria, and selects a first transaction exchange from the first plurality of exchanges to initiate a first conversion between a first fiat-currency amount and a crypto-currency amount. The payment processor initiates a transfer of the second fiat-currency amount to the payee deposit destination.

[0031] In a third major embodiment of the invention a process for generating a multi-signature address comprises defining an address associated with said multi-signature address and generating a plurality of keys and associating them with the address. For each of the plurality of keys, one or more rules is defined that when triggered enable each of their corresponding plurality of keys to be signed. Each of the one or more rules is a logical combination of one or more conditions, where each condition has one or more attributes that when true allow each of the conditions to be true. The number of keys that must be signed in order to unlock the address is also defined. One or more exit rules may be defined associated with each address where if not all of the plurality of keys have been signed before the exit rule is triggered then all of the plurality of keys are reset to an unsigned state cancelling the transaction.

[0032] In another embodiment of the invention a multi-signature address is received and a plurality of keys is determined from the address. The number of the plurality of keys that must be signed in order to unlock said address is also determined. At least one rule associated with at least two of the plurality of keys is determined. One of said at least two of the plurality of keys is signed after waiting until the at least one condition occurs. At least one
condition having one or more attributes that when true allow said at least one condition to be true. The address is unlocked when the required number of the plurality of keys are signed.

[0033] In a further embodiment of the invention a multi-signature address has an address associated with it and a plurality of keys are associated with the address. For each of the plurality of keys, there are one or more rules that when triggered enable each of their corresponding plurality of keys to be signed. Each of the one or more rules is a logical combination of one or more conditions and each of the one or more conditions have one or more attributes that when true allow each of said conditions to be true. A number of the plurality of keys that must be signed in order to unlock said address. One or more exit rules may be associated with the address wherein if not all of the plurality of keys have been signed before the exit rule is triggered then all of the plurality of keys are reset to an unsigned state.

[0034] Yet another embodiment of the invention involves a method for implementing a policy for financial transactions involving a merchant, a consumer, and a payment processor. A plurality of multi-signature addresses are defined and addresses associated with each of said plurality of multi-signature addresses are defined. A plurality of keys are associated with each of said address. For each of the plurality of keys, one or more rules are defined that when triggered enable each of the corresponding plurality of keys to be signed. Each one or more rules are a logical combination of one or more conditions, where the one or more conditions each have one or more attributes that when true allow each of the conditions to be true. A number of the plurality of keys that must be signed in order to unlock the addresses. The financial transactions may utilize crypto-currencies. The number of keys that must be signed to unlock the addresses, the rules, the conditions, and the attributes may be defined by the consumer, the merchant, or the payment processor.

[0035] Payment processing policies for implementing using multi-signature addresses includes defining an address associated with the multi-signature addresses and generating a plurality of keys and associating them with each of the addresses. For each of the plurality of keys one or more rules is defined that when triggered enable each of their corresponding plurality of keys to be signed. Each rule is a logical combination of one or more conditions and each of the one or more conditions has one or more attributes that when true allow each of the conditions to be true. A number of keys must be signed in order to unlock each address. One or more exit rules may be defined associated with each address where if not all of the plurality of keys have been signed before the exit rule is triggered then all of the plurality of keys are reset to an unsigned state cancelling the transaction.
[0036] The foregoing and additional aspects and embodiments of the present disclosure will be apparent to those of ordinary skill in the art in view of the detailed description of various embodiments and/or aspects, which is made with reference to the drawings, a brief description of which is provided next.

**BRIEF DESCRIPTION OF THE DRAWINGS**

[0037] The foregoing and other advantages of the disclosure will become apparent upon reading the following detailed description and upon reference to the drawings.

[0038] FIG. 1 shows an overview of a financial transaction using an embodiment of the invention.

[0039] FIG. 2 shows an overview of a payer or payee being verified by the system

[0040] FIG. 3 shows an overview of an embodiment of a level 1 verification.

[0041] FIG. 4 shows an overview of an embodiment of a level 2 verification.

[0042] FIG. 5 shows an overview of an embodiment of a level 3 verification.

[0043] FIG. 6 shows a detailed embodiment of paying an invoice and sending an invoice.

[0044] FIG. 7 shows an overview of a transaction being made where exchanges are chosen using criteria.

[0045] FIG. 8 shows an overview of a transaction being made where exchanges are chosen using criteria and where payments may be made in the presence of reserves.

[0046] FIG. 9 shows an overview of choosing the best rail to make a conversion and transfer.

[0047] FIG. 10 illustrates the process of converting different amounts of currency in different countries.

[0048] FIG. 11 illustrated the network used to initiated and make a fiat-currency transfer using a crypto-currency rail.

[0049] FIG. 12 shows the hierarchy of policies, multi-signature addresses, keys, rules, conditions, and attributes.

[0050] FIG. 13 shows examples of rules, conditions, and attributes

[0051] While the present disclosure is susceptible to various modifications and alternative forms, specific embodiments or implementations have been shown by way of example in the drawings and will be described in detail herein. It should be understood, however, that the disclosure is not intended to be limited to the particular forms disclosed. Rather, the disclosure is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of an invention as defined by the appended claims.
DETAILED DESCRIPTION

[0052] Embodiments of the invention relate to trusted currency transactions involving two parties who are customers of a payment processor. Typically, at least one party will be a business. The other party may be a business or an individual. One party of the transaction is the payer, who is making a payment. The other party is the payee, who is receiving a payment. Transactions require both a payer and a payee. Transactions using embodiments of this invention may be initiated by either the payer or the payee. The payer may receive a request for payment and then respond by paying the specified amount or the payer can initiate a transaction to send or pay money to a payee. Similarly, the payee may receive money from a payer or may initiate a transaction to request or demand payment from the payee.

[0053] Referring to FIG. 1, the payer 100 may be a shopper paying a merchant or a business paying a supplier. Often the payee 101 will be a supplier receiving a payment, an employee, or a consultant. A shopper may initiate a transaction by indicating a desire to purchase a good through a variety of means such as a website, over the telephone, or through an e-mail or traditional, hard copy mail. A payer 100 such as an employer may initiate a single or multiple payments on a one-time or recurring basis in order to pay the salary of an employee or contractor. Payments to suppliers may also be on a one-time or recurring basis. A payee 101 such as a company selling goods may initiate an invoice transaction to demand payment for goods sold and delivered to the payer which may be an individual, another company, or another organization.

[0054] Besides the payer 100 and payee 101, parties involved in the transaction are one or more payment processors 102, one or multiple crypto-currency exchanges 103, and one or more banking institutions 104. The payment processor 102 acts as a coordinator for the transaction. The payment processor 102 is an entity, likely a company or organization, that is providing a service for facilitating the financial transaction between the payer 100 and payee 101. The payment processor 102 may be independent of the payer and payee, providing the service through a website, telephone, or in person. The payment processor 102 may also be the same entity as the payer 100 or payee 101, facilitating the financial transaction as well as sending or receiving currencies. They provide interfaces to the payer, payee, the crypto-currency exchanges 103, and the banking institutions 104. The payer and payee register with the payment processor to participate in financial transactions. The payment processor 102 coordinates with crypto-currency exchanges 103 to convert between fiat-currencies and crypto-currencies 107, and between different crypto-currencies. Banking institutions 104
may be used to accept payments from a payer in a fiat-currency of their choice 106 and to remit payments to a payee in the fiat-currency of their choice 108.

[0055] The transaction may not involve any good or service but may be a financial transfer to send funds from a payer 100 to a payee 101. The payer and payee may be in the same or different countries. The payer and the payee may use the same or different fiat-currencies, or may use one of a variety of crypto-currencies 107.

[0056] Referring to FIG. 2, transactions conducted using embodiments of the invention may involve the identities of one or both parties verified in compliance with Anti-Money Laundering (AML) policies and Know-Your-Customer (KYC) requirements or similar requirements in the jurisdiction of the payer or the payee or both jurisdictions. Transactions may also be compliant with similar international regulations. The payment processor classifies payees and payers as new, or naked customers 201, unprofiled customers 202, transacting customers 203, or authenticated members 204. A naked customer 201 is a payee or payer that has registered with the payment processor to make or receive a payment. The naked customers 201 have supplied only minimal, unverified information to identify themselves such as an e-mail address, name, telephone number, or other information or combination of information to allow the payment processor to contact them. Typically, the registration will be done on the payment processor's website involving a user name and password for authentication, though this could also be done via e-mail, telephone or other means. It may also be done on a third party website that the payment processor has access to, such as a bank, financial institution, credit card company, or the payee's or payer's website. The payment processor may provide APIs (application program interface) to enable these third parties to securely interface with the payment processor.

[0057] The process of registering as a naked customer 201 creates an account with the payment processor changing their classification to being an unprofiled customer 202. An unprofiled customer 202 is then prompted to enter additional identification, business, and banking information to enable the payment processor and banking institutions to access their financial accounts to withdraw or deposit money. This information may include their country of residence, bank account and routing information, crypto-currency wallet address, credit or debit card information, email address, home or business address, telephone number and other information as required to make a financial transaction. At this point the customer becomes a transacting customer 203 and may send or receive fiat-currency or crypto-currency transactions. Since the identity of the transacting customer 203 has not yet been verified, there may be limitations on the transaction they are permitted to do. They may be limited to
the number of transactions, the countries they can send or receive money with, be limited to transactions below a certain value, or may only be able to send or receive but not both. Restrictions on transactions below a certain value may be evaluated on a per transaction basis or based on the total value of transactions over a period of time. For example, a transacting customer 203 may be limited to transactions below $2,000 for each transaction and no more than $10,000 within a month.

[0058] Referring to FIG. 3, in order to comply with the relevant government AML, KYC, and other regulations the payment processor will be required to verify the identity of the payer or payee. For some transactions, especially for large amounts of money, both may have to be verified. Verification can be done in different levels depending on the amount of money involved or other criteria as set out in the regulations. For small amounts it may be sufficient to do a level 1 301 verification that verifies data such as the location of the IP address, address of the business, location of the phone number, business industry databases, OFAC (Office of Foreign Assets Control), and similar checks. These can be done through a variety of methods including manual review by payment processor staff, querying of industry websites, internet search engines (Google, Bing, etc.), phone number directories, and calling the customer for verbal confirmation. Referring to FIG. 4, if the amount of money to be transacted exceeds a specified amount, such as $2,000 then further level 2 401 verification can be done. This may include review of government issued photo ID, proof of address, articles of incorporation, a review of SEC filings for public companies, and similar documents required for regulatory compliance. Referring to FIG. 5, for larger transfers a level 3 501 verification may be required, for example greater than $10,000, credit references, bank statements, and even onsite visits by the payment processor or their agents may be required. The transfer of larger amounts or other special circumstances may be required even more stringent checks.

[0059] Once a payee or payer has been verified to a certain level, they become authenticated members 204 at that level. Authenticated members are payers 100 or payees 101 who have been verified for transactions up to a specified amount or for transactions that meet certain criteria that could include source and destination country, and number of payees and other criteria. Future transactions involving authenticated members may be streamlined in that they can be initiated and completed without additional verification. This simplifies repeat and reoccurring payments between parties. It also simplifies transactions between authenticated members 204 that have not previously transacted. For example, if payer A has transacted with payee B, then A and B are both authenticated members. If payer C has
transacted with payee D, then C and D are both authenticated members. Then if payer A wants to transfer money to payee D or payer C wants to transfer money to payee B, it can be done without account verification since all four parties are authenticated members. However, if any of the parties are only verified at level 1 and then want to make a larger, level 2 transaction, they may have to submit further information to be verified to the required level to complete the transaction.

[0060] FIG. 3 shows details of an example of level 1 verification 301 according to one embodiment of the invention. The level 1 verification starts with verification of the data input by an applicant (payer or payee) 302. The data can be verified through a variety of means including a Geo (IP) location, address verification, phone number verification, OFAC (Office of Foreign Assets Control) check, and a check of business or industry directories. (A Geo (IP) location is where the geographic location of an IP is queried from a public database.) The results of the check may raise flags 303 caused by results that meet predefined or dynamic criteria or exceed predefined or dynamic thresholds. Flags may also be raised when data is not available. If flags are raised, then a manual review 304 is required. This involves verifying the identity of the applicant on industry websites, Google searches, verifying a match of website registration with phone numbers and addresses, and any similar search to verify the identity of the applicant. Whether flags 303 are raised or not, often a customer agent working with or for the payment processor will call 308 the applicant to verify their telephone number or some of their contact or financial information. If the provided telephone number is not valid 309 the payment processor may attempt to confirm information by e-mailing the application or calling a telephone number listed on the website the applicant has provided 307. Based on the response of the applicant 306 a level 2 verification may be required 305. If the telephone number verification is completed a check is then done to determine if the application and transaction represents a valid use of funds 313 as determined by relevant government AML, KYC, and other regulations. If it is determined not to be a valid use of funds, then a check will be done to determine if the applicant has been banded from the service previously 311. If so, then the application will be declined 312 and the applicant rejected. If the applicant has not previously been banned, then the application will be escalated to compliance for a manual check 310. Should the use of funds be valid 313 then a check is made to verify if the transfer is a non-business-to-business use such as sending funds to the applicant themselves, to family, or to another individual 314. If this is the case a test will be done to verify is the applicant is a real customer 317. If not, the applicant will be declined 318. If so a gratuity test will be performed 316. Once it is
determined that this is a business transaction 314 then the value of the transaction will be
evaluated against a threshold 320, for example $2,500. The exact limit may be chosen for
business reasons by the payment processor or to ensure compliance with relevant government
AML, KYC, and other regulations. If the transaction amount is less than the limit, then level
1 verification is completed 319. If the amount exceeds the threshold 320, then level 2
verification is required.

[0061] FIG. 4 shows details of an example of level 2 verification 401 according to one
embodiment of the invention. The applicant (payer or payee) is required to upload or provide
more identification 402 such as government photo ID, proof of address, a list of beneficial
owners of the company, articles of incorporation, or other similar identification. The
payment processor may also request additional information 403 as required. A check of the
beneficial owners 407 will be done and the information will be verified for completeness 406.
If complete and the applicant is a public company 405 then a search will be done for the
directors of the company and the data recorded by the payment processor 404. If the data is
complete and the applicant is not a public company, then the ID and the address will be
verified 408 and if the verification of ID and the supplied address fails then the application
will be escalated to compliance 409. For transactions over a larger amount then for level 1
verification 320, for example, $100,000 410, as required for business reasons by the payment
processor or to ensure compliance with relevant government AML, KYC, and other
regulations, the transaction will be escalated to level 3 verification 413. If the transaction
amount is greater than a lesser amount, such as $10,000 411, then level 2 verification is
complete 414, otherwise more verification of applicant documents may be required.

[0062] FIG. 5 shows details of an example of level 3 verification 501 according to one
embodiment of the invention. The applicant (payer or payee) may be required to provide
further information 502 such as credit references and bank statements. Onsite visits may also
be required for large transactions or transactions to or from some countries. If the
verification of this information is successful 503 then level 3 verification 504 is complete.
Otherwise further authorization 505 may be required from the applicant which may lead to
the applicant being declined 506.

[0063] The payer initiates the transaction by accessing the payment processor as a naked
customer and registering. The payer uses a computer or mobile device to access the website
of the payment processor. This can be done by entering a URL in a web browser window, by
clicking on a link in an e-mail, or by a variety of other well-known means. The payer is
prompted to create an account by entering a minimal amount of information that allows the
payment processor to contact them. This could include a name, e-mail address, telephone number, and a password. The payer then becomes an unprofiled customer.

[0064] The payment processor will then send a confirmation e-mail to the e-mail address entered by the payer prompting them to enter further information about themselves and their company. The payer logs into the payment processor website and is presented with choices including to make a payment. This can be in response to an invoice being received or be unilaterally sending a payment to a payee.

[0065] The payer must then provide additional information concerning themselves or the business in order to verify their identify for regulatory compliance. This information may include the name of business, the address of their place of business as well as banking information such as the bank name, routing number, and account number from which payment will be received. It may also include a crypto currency wallet address, credit or debit card information, or other information to allow money to be transferred from the payer to the payment processor. This information may be verified to comply with regulations based on the amount of money to be transferred, the country of origin or destination, the frequency or number of transactions, or other parameters. At this point the payer is considered to be a transacting customer and can proceed with the payment.

[0066] The payer must also enter information regarding the payee. The information required may be similar or the same as for the payer. However, in embodiments of this invention the payer can input a minimal, but incomplete amount of information, complete information to verify the payee's identity, or any amount of information in between. Minimal information would be the minimum information required by the payment processor to be able to contact the payee to receive further information. Complete information is the information required to identify the payee and their business and comply will relevant government AML, KYC, and any other relevant regulations. Any information not provided by the payer will be provided by the payee afterwards and will be verified by the payment processor.

[0067] The payer, having provided partial or complete payee information, will then provide the amount to be paid, and whether they will pay in crypto-currency or fiat-currency. The amount to be paid in fiat-currency will often be the fiat-currency where the payer resides but may be another common fiat-currency such as US dollars or Euros.

[0068] Various options can also be made when making a payment that can be specified through a user interface at the payment processor's website. While individuals will likely only make a single payment at a time, business have more complex needs which could include paying multiple payees as part of the same transaction, making reoccurring payment
such as salaries, electronic interfaces to accounting and financial software, and extensive reporting for internal or to fulfill government regulations regarding financial reporting and money laundering. For very small transactions such as micropayments where the fees are considered by the payer or payee to be significant, the payer, payee, or payment processor may choose to aggregate transactions before initiating the transfer at a later time. The payer may choose to not initiate transfers until the amount to be transferred exceed an amount or other criteria. They payee may choose not to accept transfer until the amount to be transferred exceed an amount or other criteria. The payment processor may provide information on fees, time required to make the transaction, information tied to Service Level Agreements (SLAs) or any other information before the payer commits to the transaction.

[0069] The payment processor will than use the payment information provided by the payer to transfer the required funds from the payer's bank or other payment source as indicated by the payer. This can be done in a variety of ways as known in the art including Automated Clearing House (ACH) transfers, electronic transfer, credit card payments, debit transfers, or drawing from an exiting payer account with the payment processor. If the payer is providing funds in a crypto-currency the payer will provide information to allow the payment processor to receive the funds which may include digital wallet addresses. The payment processor has the option of initiating the transfer immediately or may delay the payment until they have received the funds from the payer. The payment processor may initiate the transactions immediately or may also delay payment until certain criteria have been met such as receiving payment from the payer, making payment on a specified date, when the total amount to be transferred exceeds a certain amount, or any other criteria set by the payer or the payment processor.

[0070] If the payer is paying in a fiat-currency, the payment processor will then select a crypto-currency or several crypto-currencies for the transaction. There are a variety of crypto-currencies and this variety is expected to grow over time. Depending on parameters of the transaction one crypto-currency may provide an advantage over others such as lower fees, increased security, faster transfer, extensive reporting, government approval, or others. Payers or payees may also insist on the use of a single or multiple approved crypto-currencies. Parameters are numerous but could include the location of the payer and payee, type of transfer, amount to be transferred and others. The payment processor may choose a default crypto-currency or use these parameters to choose one. They may also select multiple crypto-currencies and present these choices to the payer and allow them to make the choice. Once a crypto-currency is chosen it will have associated protocols that govern the transfer,
which may include information required, minimum and maximum amounts, and others.

[0071] Once the crypto-currency to be used for the transaction has been determined, the payment processor will select an exchange or multiple exchanges to convert the fiat-currency supplied by the payee to an equivalent amount of crypto-currency minus any fees that apply. The exchange may be a digital or cryptocurrency exchange, a private transaction, dark pool, or offline exchange. The exchange may report an exchange rate and any fees to be charged to the payment processor who may relay this information to the payer for approval or for informational purposes. The payment processor may use the exchange rate spread between buying and selling to receive a fee for the transaction. The payer may also supply a range of acceptable fees, a minimum amount of crypto-currency to be received by the payee after fees are paid, or other criteria and the payment processor may proceed without approval if the criteria are met.

[0072] The fiat-currency is successfully converted to crypto-currency by the exchange, which may be verified by a number of means including checking for errors, verifying success on the crypto-currency block chain, receiving an explicit indication of success from the exchange, or other means.

[0073] The crypto-currency amount is now converted by an exchange to an equivalent amount of the fiat-currency specified by or for the payee. Similarly, to the conversion from payer fiat-currency to crypto-currency, this conversion from crypto-currency to payee fiat-currency may have its own set of criteria. Depending on parameters of the transaction, some exchanges may provide an advantage such as lower fees, increased security, faster transfer, extensive reporting, government approval, or others. Payers or payees may also insist on the use of a single or multiple approved crypto-currencies. Parameters are numerous but could include the location of the payer and payee, type of transfer, amount to be transferred and others. A default exchange may be used or an exchange may be chosen based on these criteria.

[0074] In order for a transaction to complete, both the payer and the payee must be authorized members that have provided the required information and had the information verified by the payment processor. In the present embodiment of the invention a payee who in not an authorized member will receive an e-mail or similar communication such as SMS, from the payer either directly or through the payment processor. The payee will be prompted to log into the payment processor’s web site to supply additional information that hasn't been provided by the payer. This can include information regarding the business, the banking information of the payee, in fact, similar information required to identify the payee,
compliant with government AML, KYC or other relevant national or international regulations. The information will be verified by the payment processor as in the case of the payer. The payee may also provide additional parameters such as the fiat-currency or crypto-currency of choice. In the case of micro-payments, the payee may specify a minimum amount of payment to receive in order to aggregate payments to lessen the impact of any fees charged by the payment processor or their local bank. The amount of information that must be provided and the verification required depends on the level of verification required which is dictated by government or international regulations or the business relationship between the payer and payee. For very small transactions, verification may not be required.

[0075] Once the identity of the payee has been verified to the level required by the parameters of the transaction, the payment processor will initiate the conversion from crypto-currency to the payee's fiat-currency and may receive the fiat-currency and use the payee's banking or deposit information to pay the crypto-currency to the payee. Alternatively, the payment processor may initiate the transfer of the payee fiat-currency directly to the payee from the exchange or through a third party using information identifying the payee.

[0076] The payment processor may then report information to the payer and payee including confirmation of the transfer completing successfully, exchange rates, fees, previously completed transfers, future scheduled transfers, taxes due, and other relevant information. Reporting may also be made to government bodies as required.

[0077] Transactions may be initiated by either the payer or the payee. In other embodiments of the invention the payee may register and issue an invoice or a demand for a payment. If the payer is not an authenticated member the payee will input a minimum amount of information for the payment processor to contact the payer, complete information regarding the payer, or incomplete information regarding the payer. The payer will receive an e-mail or similar communication such as SMS, from the payee either directly or through the payment processor. The payer will be prompted to log into the payment processor's web site to supply additional information that hasn't been provided by the payer. This can include information regarding the business, the banking information of the payer, information required to identify the payer, compliant with government AML, KYC or other relevant national or international regulations. The information will be verified by the payment processor. The payee may also provide additional parameters such as the fiat-currency or crypto-currency of choice. In the case of micro-payments, the payer may specify a minimum amount of payment to pay in order to aggregate payments to lessen the impact of any fees charged by the payment processor or their local bank.
FIG. 6 shows details of an example of a system used to make a transaction made using a first embodiment of the invention. A transaction between a verified payer and a payee that has not previously used the payment processor starts when a payer wishes to pay a payee for a good or a service with the payer paying in a national, or fiat-currency of their choice and the payee receiving payment in a fiat-currency of their choice. The payer may be a shopper paying a merchant or a business that is paying a supplier, an employee, or a consultant. The payer and payee may be in the same or different countries. The transaction may not involve any good or service but may be a financial transfer to send funds from a payer to a payee.

A payer or sender, who has previously been verified and has conducted at least one transaction before starts the process by indicating through a user interface to pay an invoice 601. The invoice contains at least partial identification information for the payer and the payee and may include banking information to where the payment should be made. The process for a payee, or receiver is different for a new receiver 602 or an existing receiver 607 that has been verified. The payer initiates the paying of an invoice and indicates a payee or receiver of the funds. Typically, the payer will not know if the receiver is a new or existing client of the payment processor. If the receiver or payee 602 is new, then the payer is prompted to enter banking information 603 to the system to enable payment. The payer is then presented with a payment summary page 604 to enable them to verify the invoice payment details. The payer will then be informed that since the payee is new 606 that the transaction must wait until the payee or receiver is registered and verified. The payment processor will also be authorized to debit the payer's account as soon as the receiver registers and is verified 605. Similarly, if the receiver is an existing client 607 of the payment processor but has not been verified for the size or other characteristic of the transaction 611, the payer will still be presented with a payment summary page 612 but will then be informed that the receiver must be verified 650 and that the payment processor is authorized to debit the payer's account as soon as the receiver registers and is verified 613. Once the transaction is waiting for the receiver to be registered and verified or just verified, the status of the transaction is changed to "sent pay" 614. An email is sent to the receiver prompting them to complete their profile 615, to be registered and verified, in order to receive their payment. An email is also sent to the sender informing them that the payment processor is awaiting payee confirmation and that the payment will be processed 616. After receiving the email notification, the payee or receiver will log into the payment processor's website and be presented with a user interface 618 that allows them to confirm the information for their
account and to claim the invoice amount 617. A final check of the transaction will be made to determine if the payer and payee are verified against the threshold for the transaction parameters. If the threshold is exceeded 620 then an additional popup window 620 will be presented to allow input of further information. If the threshold is not exceeded 619 the payee is then presented with a success/confirmation page 622.

[0080] If the payee is an existing receiver and has been fully verified 609 then the payer is presented with a payment confirmation page 610. Another popup window confirming the decision and prompting for any additionally required bank details 626 is displayed. Once this happens or the success/confirmation page 622 is displayed then the status of the transaction is changed to "pull authorization" 624 and a confirmation email is sent to the sender 623 indicating that the payee will soon receive the funds, and to the receiver 625 informing them to expect to receive funds shortly.

[0081] An example of a payee sending an invoice 630 is similar in that the process differs for the case of an existing, new sender or payer 631, or an existing sender, or payer 632. The payee is presented with a user interface containing an invoice detail page from 633 that allows them to enter invoice data including the identity of the payer and banking information for both the payee or the payer. An invoice summary form 634 is then displayed to allow the sender or payee to review and confirm the information. The invoice is then sent 636 and any status updates to the payee 635 is also sent. A check is made as to whether a transaction threshold for is not exceeded 638 or is exceeded 637 and if the threshold is exceeded an additional form is displayed 639 to enable the upload and verification of additional documentation. An email is then sent to the payee 640 to prompt them to pay the invoice. The payee who created the invoice is also sent an email 641 as a receipt for the transaction. The payer may login to their existing account 643, or register for a regular or guest account 642. They are then presented with an interface to preview the invoice 644 and may then process and pay it 645. The status then changes to "push authorization" and the funds are transferred from the payer to the payee 649.

[0082] In a second embodiment of the present invention, a configurable software module referred to as an "exchange router" uses criteria to select a rail, including currency exchanges, to be used in a currency conversion transaction where funds are transferred from a sender to a receiver. The exchange router also administers how an exchange is going to be used on a crypto-network when the transaction is processed. The module gathers dynamically changing cost and criteria input in real time from a variety of exchanges in order to choose an optimal rail for the transaction.
The exchange router is configurable through inputs that provide the criteria to evaluate exchanges. The input may be provided by one or more of the sender, receiver, payment processor, businesses, governments, banks, consumers, or any other organization. There may be a single input criteria or several where the criteria will vary depending on the needs of the parties involved in the financial transaction. A variety of criteria may be used but common ones include the bid and ask price of the currency as is commonly used today. Other criteria may include the maximum number of transactions in during a day, month, or other time period, minimum or maximum currency amount per transaction or during a time period. Criteria may use only fiat-currencies, crypto-currencies, or it may be allowable to use a combination of the two. Criteria may be selected and grouped to provide the basis of service level agreements (SLAs) between the sender or receiver and the payment processor.

Due to the stateless nature of crypto-currency exchanges there may be criteria based on the fiat-currencies supported by the exchange as well as their liquidity for chosen fiat-currencies. The country where the exchange is located or registered in, what laws they operate under and what national or international regulations they abide by may also be of interest.

Other possible criteria may be the fees charged, cost per transaction, monthly fees, or other costs involved in the transaction. Additional criteria of interest may be related to payment types supported for payments in and out. Criteria related to exchange size and reliability may also be used, for example, size of the company that owns the exchange, amount of currency converted, number of conversions, and exchange uptime.

Referring to FIG. 7 an example of a crypto-currency financial transaction is the transfer of funds from a payer 701 in one country to a payee 713 in the same or another country using crypto-currency as a transport mechanism. In this type of transaction, a payer in a first country initiates a transfer using their home country fiat-currency 702 and specifying the payee's deposit destination information 703 such as a bank account and routing information. The payment processor will then convert the fiat-currency amount to an equivalent crypto-currency amount 707. Next the crypto-currency will be transferred to the payee's country using crypto-currency infrastructure as a transport mechanism. Finally, the crypto-currency is converted to a second fiat-currency 709, that is payee's home country fiat-currency, and paid to the payee. These steps are typically performed in the order above but could be done in any order given the level of trust and arrangements between the parties involved. In the above transaction there are two exchanges performed;
from a first fiat-currency to crypto-currency and from the crypto-currency to a second fiat-currency. Both of these conversions may utilize the exchange server of this embodiment with the same or different criteria defined. The criteria could be defined by either the sender or the receiver of the transfer, the company providing the transfer infrastructure, government regulations or other entities. Criteria may be combined and may be decided at the time of transfer or in advance. For similar transfers done at different times, the criteria may change as well. The transaction uses a rail that uses two exchanges; a first exchange to convert the payee fiat-currency to crypto-currency and a second exchange to convert the crypto-currency to an equivalent amount of the payee's fiat-currency.

Each exchange has a weighting in the exchange router where the weighting gives it a relative priority compared to other exchanges. This is defined as the exchange weighting. When a transaction is available for processing, the router determines the exchange to use based on the weighting allocated for the exchange.

Though the embodiment above describes currency exchanges between crypto-currency and fiat-currencies the same embodiment can be used to exchange between crypto-currencies and between two fiat-currencies or any two similar or dissimilar assets. Exchanges can be fiat-currency exchanges such as banks and foreign exchange markets as well as crypto-currency exchanges based on technology of which blockchain is one example.

With reference to FIG. 8 another embodiment of a complex rail that does not involve a straight path from payer to payee. This crypto-currency financial transaction illustrates the transfer of funds from a payer 801 in one country to a payee 813 in the same or another country using crypto-currency as a transport mechanism where the presence of sufficient reserve funds allows for a payment to a payee to be made before other currency exchanges have completed or been confirmed.

In this type of transaction, a payer in a first country initiates a transfer using their home country fiat-currency 803 and specifying the payee's deposit destination information 803 such as a bank account and routing information. The payment processor determines one or more exchanges to use for the fiat-currency to crypto-currency 806, crypto-currency to fiat-currency 808, and any crypto-currency to crypto-conversions required using criteria as defined. The criteria 805 could be defined by either the sender or the receiver of the transfer, the company providing the transfer infrastructure, government regulations or other entities. Criteria may be combined and may be decided at the time of transfer or in advance. For similar transfers done at different times, the criteria may change
as well, the will then convert the fiat-currency amount to an equivalent crypto-currency amount. The conversions form a chain and in this embodiment the presence of a reserve fund in the correct currency at any part of the chain allows for that transfer to be made before currency is received from the previous link in the chain. For example, a payee may receive their payment 809 in their local fiat-currency 811 should the local crypto-currency to fiat-currency exchange hold a reserve in the local currency and make the payout before receiving crypto-currency received from the payee's initiated transaction.

[0091] In general, the steps in the processes described herein may be performed in any order given reserve levels, contractual agreements, or other arrangements as agreed to by one of more of the parties involved.

[0092] FIG. 9 illustrates an embodiment of the invention as implemented on computer hardware by a payment processor to choose a rail for financial transaction. A transaction can be initiated by either a payer (sender) or a payee (receiver). A payer may have received an invoice to pay, may be required to make a payment in advance of a shipment, or may simply want to transfer funds to another party. A payee may want to initiate a transaction to request funds as in sending an invoice to another party. Both the sender and the receiver are registered with the payment processor or will be registered as part of the process and this will include information required to comply with KYC (know your customer) and AML (anti-money laundering) requirements as required by governments or by the sender or the receiver. KYC requirements may also be required by an exchange or a third party who may be guaranteeing the transaction or acting as an escrow agent.

[0093] In the present example, once the payment 901 is defined and information gathered the payment processor starts to collect key parameters of the transaction. This can be looking at the source 902 and the destination 903. In the example given the funds are being transferred from the United States and the payment processor reads in a first set of criteria that are relevant for transfers originating from the United States. These criteria may vary depending on the originating country and may vary depending on the information provided by the sender. The payment processor will also look at the destination of the transfer 903 and this will dictate a second set of criteria that is added to the first set. In the example given the destination may be Mexico or China. Assuming that China 904 does not permit crypto-currency transfers then a traditional wire transfer will be used to pay out the transfer to the receiver. Assuming the Mexico does permit both wire transfers and crypto-currency transfers then the receiving currency will be examined 905 and this lead to a third set of criteria being added. In this case if the payment is made from the United States to
Mexico in US dollars then crypto-currencies may not be used and a wire transfer is chosen 906. In this case, by making a transfer from the United States to Mexico where the payee receives funds in peso there exist rails that utilize both traditional wire transfer exchanges and crypto-currency exchanges and the payment processor. In this case, due to the large number of options in rails and the high volatility of both the exchange rate of crypto-currencies and the fees charged by the various exchanges the calculation of the cost 908 of the rails is non-trivial and is performed by the payment processor.

The calculation of the cost 908 of the available rails starts with the use of computer implemented API (application programming interfaces) to automatically query the banks and exchanges that make up the possible rails for the transfer. Each exchange and bank will return different data in different formats and this must be normalized by the payment processor in order to compare them. The costs will then be evaluated against the criteria. A variety of criteria may be used but common ones include the bid and ask price of the currency as is commonly used today. Other criteria may include the maximum number of transactions in during a day, month, or other time period, minimum or maximum currency amount per transaction or during a time period. Criteria may include the amount of time required to complete a transaction. Further criteria may include the amount, detail, and accuracy of the reporting provided by the rail. Criteria may be to use only fiat-currencies, crypto-currencies, or it may be allowable to use a combination of the two. Criteria may be selected and grouped to provide the basis of service level agreements (SLAs) between the sender or receiver and the payment processor. This may be combined with reporting in order to determine if the SLA conditions have been fulfilled. Due to the stateless nature of crypto-currency exchanges there may also be criteria based on the fiat-currencies supported by the exchange as well as their liquidity for chosen fiat-currencies. The country where the exchange is located or registered in, what laws they operate under and what national or international regulations they abide by may also be of interest. Other possible criteria may be the fees charged, cost per transaction, monthly fees, or other costs involved in the transaction. Additional criteria of interest may be related to payment types supported for payments in and out. Criteria related to exchange size and reliability may also be used, for example, size of the company that owns the exchange, amount of currency converted, number of conversions, and exchange uptime.

The querying of the banks and exchanges must be done in a timely manner as close to the time of the payment processor evaluating rails to ensure that highly volatile data is as up to date as possible. The payment processor may maintain a table of costs that
include when they were last updated and an indication of their volatility. Highly volatile

costs may have to be updated frequently while low volatility costs may be updated

infrequently.

[0096] The evaluation of the criteria will lead to a cost per rail for each possible rail

that can implement the transaction. Referring to FIG. 10, each source and destination, in

this illustrative example the United States 1002, Kenya 1005, Mexico 1003, and Italy 1004

has a number of rails that can be used to transfer funds from and to them. Rails may be bi-

directional or unidirectional. Unidirectional transfers are where currencies may be

transferred in or out using a particular exchange but not both. A country such as the United

States will have a large number of available rails 1007 while a smaller country such as

Kenya may have only one 1006. Rails may incorporate a single or multiple exchanges and

may be able to convert all or only some fiat-currencies and crypto-currencies.

[0097] FIG. 11 shows a geographical view of an embodiment of the invention. The

sender is located in the US 1101 and may initiate or respond to transactions using a

personal computer, mobile device, telephone or other means of communication. The

interface using a personal computer or mobile device may be a customized web page or a

local application that allows the use to register, authenticate with the payment processor,

provide identification for themselves and the receiver, and to communicate with the

payment processor to verify their identity in link with KYC criteria. The user interface also

allows them to specify general criteria to be used with all of their transactions as well as

specific criteria. Specific criteria may apply to sending payments, receiving payments, to

certain receivers or groups of receivers. Specific criteria may apply to receivers in certain

countries, or that use certain currencies, including crypto-currencies. For example; criteria

may apply to receivers in Mexico that want to receive payment in bitcoin and are in the

telecommunications industry. Other criteria may apply to receivers in Germany who want

to receive payment in Euro and have overdue payments due to the sender.

[0098] The sender 1101 interfaces to the payment processor 1102 who may be located

in the same country as the sender or the receiver, or somewhere where neither is located. If

the sender is sending in fiat-currency they will typically interface with one of the local

banks 1104, or another local bank 1105. If they are sending funds in a crypto-currency

they may use one located in their home country 1106, or one in the receiver's country 1109,

or one located elsewhere 1107 or 1108. Similar to the sender, the receiver 1103 may

initiate or respond to transactions using a personal computer, mobile device, telephone or

other means of communication. The interface using a personal computer or mobile device
may be a customized web page or a local application that allows the use to register, authenticate with the payment processor, provide identification for themselves and the receiver, and to communicate with the payment processor to verify their identity in link with KYC criteria. The user interface also allows them to specify general criteria to be used with all of their transactions as well as specific criteria.

[0099] The receiver 1103 may receive payout in the fiat-currency of their choice using a local bank 1111 from among a choice of local banks 1110. They may receive payment in a crypto-currency through a crypto-exchange that is local 1109, in the sender's country 1106, or located elsewhere 1107, 1108.

[0100] The payment processor will evaluate the transaction data and its associated criteria as well as criteria supplied by the sender and the receiver. The payment processor will determine the optimal rail for the transaction given the criteria. The payment processor may also determine redundant or back-up rails that could also be used to complete the transaction. These redundant rails may have the same cost, or the same overall cost but may have higher scores or lower costs in different criteria from the primary rail. The payment processor may have criteria to decide when to use a redundant rail or may give the choice to the sender or the receiver.

[0101] FIG. 12 illustrates how security policies 1201 can be implemented using a third embodiment of the invention. Multi-signature addresses 1202 provide security for access to crypto-currencies for secure storage or transactions. A multi-signature address is an address that is associated with more than one public-private key pair 1203. One of the simplest form of multi-signature address 1202 is an m-of-n address and is defined by the variables m and n, where n is the total number of public-private keys associated with generating a multi-signature address 1202 and m is the number of private keys that must be signed in order to unlock the address associated with the crypto-currency. In FIG. 12 it can be seen that n is 2. It can be seen that m is less than or equal to n. If sending crypto-currency from a wallet that is associated with n private keys, then sending crypto-currency from this address requires signatures from at least m keys. A multi-signature transaction is one that sends and receives funds from a multi-signature address.

[0102] Using an m-of-n multi-signature address 1202 allows the n keys to be kept in multiple location, on multiple computer systems, with multiple computer operating systems even in non-digital and offline locations such as in paper or in paper wallets. The key can be managed and administered using separate applications as well. Since m of the total keys must be compromised in order to unlock the value assigned to a transaction unlocking the multi-
signature address becomes more difficult than the case of a single signature which has only a single key.

[0103] M-of-n multi-signature addresses 1202 also provide redundancy. For example, with a 2-of-3 address, the crypto-currency owner can still unlock the value if they forget any single key provided they have at least 2 of the 3. Multi-signature addresses 1202 may also be shared among multiple people where a majority vote or a defined number of votes are required to unlock and use the funds. Another embodiment of multi-signature addresses involves a party such as a payment processor setting up, tearing down, configuring, and processing multi-signature addresses and transactions involving multi-signature addresses.

[0104] To set up a multi-signature address 1202 the payment processor creates the multi-signature address with a plurality of keys 1203. Each key 1203 may be labeled and named by the payment processor or user for reference. Each key 1203 is also programmed or configured by linking it to a script, software, or configuration 1206. Each script defines a number of conditions 1208, attributes 1209, and rules 1207. The script or the software 1206 can be resident on a payer's computer, server, digital storage, cloud locations or mobile device. The script 1206 could also be resident on servers, or computers or mobile devices operated by the payment processor or another third party. The script 1206 includes one or more rules 1207 that must trigger to enable a key 1203 to be signed. If the key 1203 is triggered, then it becomes "active" and is able to be signed in order to approve a transaction. Each rule 1207 defines a Boolean combination of conditions 1208 that must occur for the rule 1207 to be triggered. For example, given four conditions 1208 labeled A, B, C, and D, one rule 1207 may be triggered if conditions 1208 A, B, and D occur, whether C occurs or not. Another example would be to trigger the rule 1207 if B and C occurred but not D. A further example would be to trigger a rule 1207 if any 3 of conditions A, B, C, or D occur.

[0105] Referring to FIG. 13, conditions 1208 are comprised of one or more attributes 1209 such as if the price of bitcoins is greater than $500, the price of inventory is less than $200, a seller is located in a specific location such as San Francisco, or the age of a buyer over 18 years of age. or any number of other attributes 1209 agreed upon by the payment processor, the merchant, the consumer, the payer, the payee, or other involved parties. For rules 1207, conditions 1208, and attributes 1209 other combinations and combinations can be defined depending on the level of complexity desired and the level of security required. A "safety key" 1205 may also be defined which would allow for the unlocking of an escrow or a disputed transaction. It could also be used when private keys have been lost. Also part of the configuration script 1206 is that the payment processor can setup an "exit key" 1204; a time
based rules or any other type of rules to exit or cancel a multi-signature transaction and return the funds to their owner or another action. The attributes 1209, conditions 1208 and rules 1207 for the exit rule 1204 may be setup in situations where the triggering of the events that are designed to activate the keys have not occurred and where a time limit has expired. An example is that if the multi-signature address 1202 is configured where the private key 1203 is activated if the price of the good goes down by 5% for a period no more than 24 hours, then at the expiry of the time period, the transaction expires and the funds are returned to their owner. The exit rule 1204 conditions could be time based, event based, payer based, payee based, or enforced by the payment processor based on its policies or requests by banks, government agencies or any other entity that has the ability to force the address to expire.

Further examples of attributes 1209 include but are not limited to:

- Time field: Key is activated after midnight.
- Date: Key is activated after January 1, 2020.
- Location: The key is activated only if the payer is in California.
- Identity: The key is activated based on the identity of the payer on a national or state driver's license.
- Price of a good or service: The key is activated if the price of the good is over specified amount or the price of this service declines to below a specified price.
- Price of currency: The key is activated if the price of a crypto-currency is over a specified amount or the price of a fiat-currency is over a specified amount.
- Database entries: The key is activated if there is an entry in a database. For example, the key is activated if the payer is in the customer database.
- Any information that can be used as input to the script. For example, the key can be activated if the weather in New York is above 50 degrees Fahrenheit or if the result of the presidential election were in favor of candidate A.

Functions that scripts 1206 can be used for multiple aspects of a multi-signature key system including but not limited to the following.

- Creation of key pairs
  - Script that automates key pair generation or creation
- Storage location of keys
  - Script that auto routes key pairs to final management / storage destination
  - Routing to 3rd party management - key holders
  - Routing to payment processor server
  - Routing to Mobile devices
Routing to Local machine storage, including hard disks and solid-state drives
Routing to Web browser storage
Routing to other forms of online, digital storage such as flash drives
Routing to other forms of offline storage including automatically printing on paper wallets

- Management and Administration
  - Script that retrieves keys from various locations based on conditions
  - Script that returns unspent transactions to originator
  - Script that checks for unused or undocumented addresses with balances
  - Script that empties and deletes obsolete addresses

- Transaction Automation
  - Script that allows for automated remote signing. For example, through email or through a dashboard application,
  - Script that automates key importing from digital or offline locations either remotely or locally from the server executing the transaction,
  - Script that automates key pair raw extraction
  - Script that automates private key signing
  - Script that automates raw transaction creation
  - Script that automates transaction sending
  - Script that automates transaction sending

- Security
  - Script that automates backing up (redundancy) of keys

[0108] Keys may be generated by any number of electronic devices including servers, computer, tablets, cell phones. Keys may be supplied or partially supplied by the user, the payment processor, or by a financial institution such as a bank or currency exchange. The keys may be stored on a user's own device and may be stored in a database. When stored in a database, an application can be authorized to access the key from the database. Keys may be split and stored in a number of locations, for example partially on a user's device, with a payment processor, or with a financial institution such as a bank or currency exchange.

[0109] A multi-signature address 1202 can also function as a unique identifier that abstracts traditional payment types including: wallets, cash, cards, bank, prepaid cards, gift cards, voucher cards, voucher pins, or any other form of eMoney. When all the conditions 1208 are met and the payment is executed, the multi-signature address becomes the trigger for the payment action. For example, once conditions are met, credit cards are charged, funds pushed
or pulled from bank accounts, funds released from escrow, cash exchanged or moved into electronic wallets, gift cards exchanged for inventory, vouchers applied and executed. The same logic and actions that apply to crypto-currency are applicable for traditional payments and the address acts as a proxy, or a representation of the action required from traditional payments.

[0110] A set of rules 1207 on a network can define the behavior of payments inside the network. Therefore, it is feasible to setup operating policies 1201 on the network comprising of a set of rules 1207 and conditions 1208 administered on a set of multi-signature addresses 1202 thereby determining and influencing the behavior of transactions; what gets accepted and what gets declined.

[0111] E-Commerce and financial service providers can incorporate multi-signature keys for conducting currency exchanges within or between countries, to purchase items, issue invoices, to pay employees and a variety of other uses. Currency exchanges can be from a national or fiat currency to a crypto-currency such as Bitcoin or the reverse, from a crypto-currency to a fiat currency. The transfer of currencies can be between the same currency or between different currencies. Service providers may integrate multi-signature technology into a web-based user interface using APIs (application programming interfaces). A payment processor is a company or organization that provides the software and infrastructure to do currency exchanges using multi-signature keys. A plugin can be created by the payment processor to allow people to collect payments through their website in different crypto and fiat currencies. The plugin provided by the payment processor provides a payment gateway that may be branded by either the service provider or the payment processor. A user must enter identification and bank account information after which the payment proceeds in a similar way to paying online using a credit card or PayPal. The Payment processor is responsible for checking and verifying the user's identity including name, address and any other required information required to verify their identity.

[0112] One feature of this system is the service provider (merchant or financial institution) is not required to assume the risk of a fraudulent transaction. This is assumed by the payment processor. The plugin uses a software module called a "risk engine" that will confirm the user data and combine it with attributes of the transaction to evaluate the risk of the transaction to determine the complexity of the multi signature key to be used. Transaction attributes can include the identity and payment history of the payer and payee, the source and destination country of the transaction, the fiat or crypto currencies involved and their amount, the risk tolerance of merchants, financial institutions, currency exchanges, and governments.
involves, and a variety of other factors. The risk engine allows the user to enter the required information to evaluate the transaction and if it determines that it is a high-risk transaction may stop the transaction, and require additional information or require manual intervention.

[0113] The payment processor will evaluate the multi signature key and sign them, thereby assuming the risk for the transaction.

[0114] The merchant, financial exchange, currency exchange, or other involved party may configure the level of risk they are willing to accept using a software module referred to as the "business configuration engine". This can be used to specify the parameters of the multi signature key such as the number of keys, number of rules, scripts, conditions, and attributes.

[0115] Advanced currency exchange features may be implemented by the plugin such as creating queues for each source and destination currency exchange and only triggering the actual conversion when a predefined exchange rate is met. This can be implemented using multi-signature keys by defining an additional key where the rule includes a condition where the attribute is the desired exchange rate. Note that if the condition is never met some conversions may take a long time or may never trigger. In this case an exit key containing a rule with a condition using an attribute of the pendency of the transaction can be used to automatically cancel the transaction or notify the payee or payer.

[0116] Many international transactions will use a plurality of conversions such as from one fiat-currency to an intermediate crypto-currency, and another one from the crypto-currency to a second fiat-currency. For this type of two-leg or multi-legged transaction a different multi signature key can be used for each leg with each key having its own set of keys, rules, conditions, and attributes.

[0117] The payment processor has its own risk engine to determine the parameter of the multi signature key and therefore may assume the risk of the transaction. However, in some embodiments of the invention the evaluation by the risk engine and the responsibility may be bourn by third party insurance companies.

[0118] In another embodiment of the invention, companies, merchants, financial institutions, insurance companies and other parties may utilize multi signature keys to implement a manual authorization system for high risk or high value transactions. This can be done by defining a manual key in each multi signature address that must be entered by an individual in the organization to approve the transaction. The manual key may involve entering data through a user interface device such as a keyboard, a scanned signature, biometric information such as a finger print or iris scan, or inserting a specially prepared USB key, SD card, NFC device or similar non-volatile memory device. For example, in a company the
finance manager may be able to approve most transactions immediately but transactions over a specified amount are queued until the CEO or CFO inserts a USB key into a computer or terminal or accesses the payment processor's website using a specific laptop, computer, or mobile computing device. The private manual key stored on a USB key or electronic device does not have to be the actual key but may be a hash of the key. A similar setup may be used by police to release confiscated funds, a parent to approve purchases made by their children over a predefined amount, or customs officials when currency limits are exceeded. In larger organizations there may be a large number of private USB sticks containing private manual keys to approve large transactions. These may be distributed to the officers of the company and large transactions may be signed and approved by using a subset of the distributed keys. For example, a bank may have a special authorization key with 3 USB sticks required from a total of 10 officers of the bank to approve the transaction.

[0119] Although the algorithms described above including those with reference to the foregoing flow charts have been described separately, it should be understood that any two or more of the algorithms disclosed herein can be combined in any combination. Any of the methods, algorithms, implementations, or procedures described herein can include machine-readable instructions for execution by: (a) a processor, (b) a controller, and/or (c) any other suitable processing device. Any algorithm, software, or method disclosed herein can be embodied in software stored on a non-transitory tangible medium such as, for example, a flash memory, a CD-ROM, a floppy disk, a hard drive, a digital versatile disk (DVD), or other memory devices, but persons of ordinary skill in the art will readily appreciate that the entire algorithm and/or parts thereof could alternatively be executed by a device other than a controller and/or embodied in firmware or dedicated hardware in a well-known manner (e.g., it may be implemented by an application specific integrated circuit (ASIC), a programmable logic device (PLD), a field programmable logic device (FPLD), discrete logic, etc.). Also, some or all of the machine-readable instructions represented in any flowchart depicted herein can be implemented manually as opposed to automatically by a controller, processor, or similar computing device or machine. Further, although specific algorithms are described with reference to flowcharts depicted herein, persons of ordinary skill in the art will readily appreciate that many other methods of implementing the example machine readable instructions may alternatively be used. For example, the order of execution of the blocks may be changed, and/or some of the blocks described may be changed, eliminated, or combined.

[0120] It should be noted that the algorithms illustrated and discussed herein as having various modules which perform particular functions and interact with one another. It should
be understood that these modules are merely segregated based on their function for the sake of description and represent computer hardware and/or executable software code which is stored on a computer-readable medium for execution on appropriate computing hardware. The various functions of the different modules and units can be combined or segregated as hardware and/or software stored on a non-transitory computer-readable medium as above as modules in any manner, and can be used separately or in combination.

[0121] While particular implementations and applications of the present disclosure have been illustrated and described, it is to be understood that the present disclosure is not limited to the precise construction and compositions disclosed herein and that various modifications, changes, and variations can be apparent from the foregoing descriptions without departing from the spirit and scope of an invention as defined in the appended claims.
WHAT IS CLAIMED IS:

1. A method of electronic commerce payments comprising:
   a payment processor receiving currency information and identification information,
   said currency information comprising a payer fiat-currency and a payee fiat-currency,
   said identification information comprising information verifying the identify of a payer and a payee,
   said payment processor utilizing said currency information and said identification information to determine a transaction restriction level,
   said payment processor verifying that said identification information meets a threshold for said transaction restriction level,
   said payment processor receiving payment in said payer fiat-currency and initiating a transaction to convert said payer fiat-currency amount into a crypto-currency amount,
   said payment processor converting said crypto-currency amount into said payee fiat-currency, and
   said payment processor initiating a transfer of said payee fiat-currency amount to said payee.

2. The method of claim 1, further comprising said payment processor determining criteria to be used to select said crypto-currency and selecting said crypto-currency.

3. A method of electronic commerce payments comprising:
   a payment processor receiving currency information and identification information,
   said currency information comprising a payer fiat-currency and a payee fiat-currency,
   said identification information comprising information verifying the identify of a payer and a payee,
   said payment processor utilizing said currency information and said identification information to determine a transaction restriction level,
   said payment processor verifying that said identification information does not meet a threshold for said transaction restriction level and augmenting said identification information to meet said threshold for said transaction restriction level,
said payment processor receiving payment in said payer fiat-currency and initiating a transaction to convert said payer fiat-currency amount into a crypto-currency amount,
said payment processor converting said crypto-currency amount into said payee fiat-currency, and
said payment processor initiating a transfer of said payee fiat-currency amount to said payee.

4 The method of claim 3, further comprising said payment processor determining criteria to be used to select a crypto-currency and selecting said crypto-currency.

5. The method of claim 3, further comprising said payment processor augmenting said identification information comprises verifying the identity of said payer with a first portion of information provided by said payer and a second portion of information provided by said payee.

6. The method of claim 3, further comprising said payment processor augmenting said identification information comprises verifying the identity of said payee with a first portion of information provided by said payer and a second portion of information provided by said payee.

7. A method of electronic commerce payments comprising:
   a payment processor receiving currency information and identification information,
said currency information comprising a payer fiat-currency and a payee fiat-currency,
said identification information comprising information comprising a payer trusted level and a payee trusted level,
said payment processor utilizing said currency information and said identification information to determine a transaction restriction level,
said payment processor verifying that said payer trusted level and said payee trusted level meet a threshold for said transaction restriction level,
said payment processor receiving payment in said payer fiat-currency and initiating a transaction to convert said payer fiat-currency amount into a crypto-currency amount,
said payment processor converting said crypto-currency amount into said payee fiat-currency,
said payment processor initiating a transfer of said payee fiat-currency amount to said payee.

8. A method of currency transactions over a network using a payment processor server comprising:
providing a payer user interface to receive currency information and identification information, said currency information comprising a payer fiat-currency and a payee fiat-currency, said identification information comprising information verifying the identify of a payer and a payee,
utilizing said currency information and said identification information to determine a transaction restriction level,
verifying that said identification information meets a threshold for said transaction restriction level,
receiving payment in said payer fiat-currency and initiating a transaction to accessing a first exchange to convert said payer fiat-currency amount into a crypto-currency amount,
accessing a second exchange and converting said crypto-currency amount into said payee fiat-currency, and
initiating a transfer of said payee fiat-currency amount to said payee.

9. A method of currency transactions over a network using a payment processor server comprising:
providing a payer user interface to receive currency information and identification information, said currency information comprising a payer fiat-currency and a payee fiat-currency, said identification information comprising information verifying the identify of a payer and a payee,
receiving over said network said currency information and identification information by said payment processor server, said payment processor server comprising a processor and a memory that stores said currency information and identification information, wherein said processor compares said currency information and said identification information against a threshold to determine a transaction restriction level,
verifies that said identification information meets a threshold for said transaction restriction level,
receives payment in said payer fiat-currency and initiates a network transaction to access a first exchange to convert said payer fiat-currency amount into a crypto-currency amount,
accesses a second exchange and converting said crypto-currency amount into said payee fiat-currency, and
initiates a second network transfer of said payee fiat-currency amount to said payee.

10. A method of electronic commerce payments comprising:
   a payment processor receiving a first fiat-currency amount and information, said information comprising a payee deposit destination,
   said payment processor receiving a first plurality of criteria, evaluating a first plurality of exchanges against said first plurality of criteria, and selecting a first transaction exchange from said first plurality of exchanges to initiate a first conversion between a first fiat-currency amount and a crypto-currency amount,
   said payment processor receiving a second plurality of criteria, evaluating a second plurality of exchanges against said second plurality of criteria, and selecting a second transaction exchange from said second plurality of exchanges to perform a second conversion between the crypto-currency amount and a second fiat-currency amount,
   said payment processor initiating a transfer of said second fiat-currency amount to the payee deposit destination.

11. A process of selecting an exchange comprising:
   receiving a plurality of criteria,
   evaluating a plurality of exchanges against said plurality of criteria, and
   selecting an transaction exchange from said plurality of exchanges to perform a conversion between a first asset and a second asset.

12. A method of electronic commerce payments comprising:
   a payment processor receiving a first fiat-currency amount and information, said information comprising a payee deposit destination,
   said payment processor receiving a first plurality of criteria, assigning at least a first
weighting to at least one of said first plurality of criteria and using said first weighting to produce a first weighted criteria, evaluating a first plurality of exchanges against at least one of said first plurality of criteria and said first weighted criteria, and selecting a first transaction exchange from said first plurality of exchanges to initiate a first conversion between a first fiat-currency amount and a crypto-currency amount, said payment processor receiving a second plurality of criteria, assigning at least a second weighting to at least one of said second plurality of criteria and using said second weighting to produce a second weighted criteria, evaluating a second plurality of exchanges against at least one of said second plurality of criteria and said second weighted criteria, and selecting a second transaction exchange from said second plurality of exchanges to initiate a second conversion between the crypto-currency amount and a second fiat-currency amount, said payment processor initiating a transfer of said second fiat-currency amount to the payee deposit destination.

13. A process of selecting an exchange comprising:
receiving a plurality of criteria,
assigning at least one weighting to at least one of said plurality of criteria and using said weighting to produce a weighted criteria,
evaluating a plurality of exchanges against at least one of said plurality of criteria and said weighted criteria, and selecting an transaction exchange from said plurality of exchanges to perform a conversion between a first asset and a second asset.

14. A process for generating a multi-signature address comprising:
defining an address associated with said multi-signature address;
generating a plurality of keys and associating them with said address; for each of said plurality of keys, defining a rule that when triggered enable each of said corresponding plurality of keys to be signed, said rule being a logical combination of a plurality of conditions, said plurality of conditions each having an attribute that when true allow each of said plurality of conditions to be true; defining the number of said plurality of keys that must be signed in order to unlock said address.
15. The process of claim 14, further comprising determining one or more exit rules associated with said address wherein if not all of said plurality of keys have been signed before said exit rule is triggered then all of said plurality of keys are reset to an unsigned state.

16. A process for signing a multi-signature address comprising:
   receiving an address;
   determining a plurality of keys from said address;
   determining a number of said plurality of keys that must be signed in order to unlock said address;
   determining a rule associated with at least two of said plurality of keys;
   waiting until said a condition occurs before signing one of said at least two of said plurality of keys, said condition each having an attribute that when true allow said condition to be true;
   unlocking said address when said number of said plurality of keys are signed.

17. The process of claim 16, further comprising determining an exit rule from said address wherein if not all of said plurality of keys have been signed before said exit rule is triggered then all of said plurality of keys are reset to an unsigned state.

18. A method for implementing a policy for financial transactions involving a merchant, a consumer, and a payment processor comprising:
   defining a plurality of multi-signature addresses;
   defining addresses associated with each of said plurality of multi-signature addresses;
   generating a plurality of keys associated with each of said addresses;
   for each of said plurality of keys, defining a rule that when triggered enable each of said corresponding plurality of keys to be signed, said rule being a logical combination of a plurality of conditions, said plurality of conditions each having an attribute that when true allow each of said plurality of conditions to be true;
   defining the number of said plurality of keys that must be signed in order to unlock said address.

19. The method of claim 18, wherein the financial transaction utilizes
cryptocurrencies.

20. The method of claim 18, wherein at least one of said plurality of keys, said rules, said conditions, and said attributes are defined by said consumer.

21. The method of claim 18, wherein at least one of said plurality of keys, said rules, said conditions, and said attributes are defined by said merchant.

22. The method of claim 18, wherein at least one of said plurality of keys, said rules, said conditions, and said attributes are defined by said payment processor.

23. The method of claim 18, wherein said multi-signature address is an identifier for non-digital payment types.
FIG. 2

1. Account Creation
   - On Boarding Model
     - Inbound
       - eMail Verification
         - Naked customer
         - 201

2. Business Details
   - Profile
     - Initiator Verification
     - Unprofilled customer

3. Transaction Verification
   - Customer
     - Counter Party Verification

4. Trusted Parties
   - New Member Acquisition
   - 203

5. Authenticated Members
   - Processed Transaction
     - Align Network
     - Re-engagement cycle
     - 204
FIG. 5

Performing By Compliance

Compliance Level 3 Verification

Option for Enhanced Due Diligence:
- 2 credit references
- 3 months bank statements
- Onsite visit

Passed?

Yes
Level 3 Verified

No

Sign Authorization from Sender

Decline
Fiat-currency
Payee information
Payer

Payment Processor

Determine criteria for choosing exchange

Choose crypto-currency exchange

Initiate fiat-currency to crypto-currency conversion

Determine criteria for choosing exchange

Initiate crypto-currency to fiat-currency conversion

Initiate transfer of fiat-currency to payee

Send reports to payer and payee

Fiat-currency
Report
Payee

FIG. 7
Fiat-currency

Payee information

803

Payer

801

Payment Processor

804

Determine criteria for choosing exchange

805

Choose crypto-currency exchange

806

Reserve

807

Initiate fiat-currency to crypto-currency conversion

808

Determine criteria for choosing exchange

814

Reserve

Initiate crypto-currency to fiat-currency conversion

811

Fiat-currency

Report

Send reports to payer and payee

810

Initiate transfer of fiat-currency to payee

809

Reserve

813

Payee

812

FIG. 8
901 Payment Out

902 Coming from

US

Europe

903 Where to

China

Mexico

904 Wire transfer

905 Currency

USD

Wire transfer

907 External data (APIs)

908 Calculate cost

Exchange A

Bank (fixed cost)

909 Best rail

910 Use exchange A

FIG. 9
FIG. 10
1201 Policies

Transactions

1202 Multi-signature address

1203 Key

1206 Script, software, configuration

1207 Rules

1208 A B C D

1209 Attribute

Unlock m of n keys to unlock address

1204 1205

When rules trigger, key may be unlocked

Boolean or logical combination of some or all conditions

Time of day, month, price, locations, etc.

FIG. 12
<table>
<thead>
<tr>
<th>Conditions</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A:</td>
<td>Price of bitcoins &gt; $500</td>
</tr>
<tr>
<td>B:</td>
<td>Price of inventory &gt; $200</td>
</tr>
<tr>
<td>C:</td>
<td>Location of seller = San Francisco</td>
</tr>
<tr>
<td>D:</td>
<td>Age of buyer &gt; 18 years old</td>
</tr>
</tbody>
</table>

**Rules**

Rule 1: A and B and D
Rule 2: B and C not D
Rule 3: Any 3 of A, B, C, D
**INTERNATIONAL SEARCH REPORT**

**Box No. II** Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.: because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.: because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. III** Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Group I Claims 1-9; Group II Claims 10-13; Group III Claims 14-23

"*Continued in the Next Supplemental Box:*"*

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☑ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos. 1-9

**Remark on Protest**

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (2)) (January 2015)
INTERNATIONAL SEARCH REPORT

International application No.
PCT/US1 6/581 16

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) : G06Q 40/04, 20/12, 20/38, 20/40, 30/03 (2016.01)
CPC : G06Q 20/381, 20/363, 20/16, 20/12, 40/04

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) : G06Q 20/04, 20/08, 20/12, 20/38, 20/40, 30/03, 40/04 (2016.01)
CPC : G06Q 20/065, 20/0658, 20/16, 20/36, 20/363, 20/381, 20/382, 20/414, 40/04, 20/08, 20/12

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PatLeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, Other Countries (INPADOC), RU, AT, CH, TH, BR, PH); EBSCO; IEEE/IEEEexplore; Google/Google Scholar; Keywords: currency, cryptocurrency, fiat, conversion, exchange, ecommerce, buyer, seller, purchase, transaction, payer, payee, trust

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 2015/0262139 A1 (COINBASE, INC.) 17 September 2015; figures 26, 29, 40, 42; paragraphs [0090], [0094], [0144].</td>
<td>1-4, 8-9 *********</td>
</tr>
<tr>
<td>Y</td>
<td>US 2008/0091619 A1 (PERLMAN, J. et al.) 17 April 2008; claim 6.</td>
<td>5-6</td>
</tr>
<tr>
<td>Y</td>
<td>US 2013/0097056 A1 (SUN, T. et al.) 18 April 2U13; paragraph[1] [UU4b], [UU3b].</td>
<td>7</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

"T" later document published after the international filing date or priority date and not in conflict with the application but cited is understood to be of particular relevance

"Y" document of particular relevance; the claimed invention cannot be considered as interfering with the application

Authorised officer
Shane Thomas

Date of the actual completion of the international search

Date of mailing of the international search report
1 FEB 2017

Home and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-8300

Form PCT/ISA/2 10 (second sheet) (January 2015)
This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-9 are directed towards converting between a crypto-currency and a fiat-currency for electronic commerce payments.

Group II: Claims 10-13 are directed towards evaluating and selecting a transaction exchange to perform conversion between a crypto-currency and a fiat-currency.

Group III: Claims 14-23 are directed towards a process for generating a signing a multi-signature address.

The inventions listed as Groups I-III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical features of Group I include at least: method of currency transactions over a network using a payment processor server comprising: said payment processor server comprising a processor and a memory that stores said currency information and identification information providing a payer user interface to receive currency information and identification information, a payment processor receiving currency information and identification information, said currency information comprising a payer fiat-currency and a payee fiat-currency, said identification information comprising information comprising a payer trusted level and a payee trusted level, said identification information comprising information verifying the identity of a payer and a payee, said payment processor utilizing said currency information and said identification information to determine a transaction restriction level, said payment processor verifying that said identification information does not meet a threshold for said transaction restriction level, and augmenting said identification information to meet said threshold for said transaction restriction level, said payment processor receiving payment in said payer fiat-currency and initiating a transaction to convert said payer fiat-currency amount into a crypto-currency amount, said payment processor converting said crypto-currency amount into said payee fiat-currency, and said payment processor initiating a transfer of said payee fiat-currency amount to said payee, which are not present in Groups II-III.

The special technical features of Group II include at least said information comprising a payee deposit destination, said payment processor receiving a first plurality of criteria, assigning at least a first weighting to at least one of said first plurality of criteria and using said first weighting to produce a first weighted criteria, evaluating a first plurality of exchanges against at least one of said first plurality of criteria and said first weighted criteria, and selecting a first transaction exchange from said first plurality of exchanges to initiate a first conversion between a first fiat-currency amount and a crypto-currency amount, said payment processor receiving a second plurality of criteria, assigning at least a second weighting to at least one of said second plurality of criteria and using said second weighting to produce a second weighted criteria, evaluating a second plurality of exchanges against at least one of said second plurality of criteria and said second weighted criteria, and selecting a second transaction exchange from said second plurality of exchanges to initiate a second conversion between the crypto-currency amount and a second fiat-currency amount, which are not present in Groups I and III.

The special technical features of Group III include at least a process for signing a multi-signature address and method for implementing a policy for financial transactions involving a merchant, a consumer, and a payment processor comprising: receiving an address; determining a plurality of keys from said address; determining a number of said plurality of keys that must be signed in order to unlock said address; for each of the keys, defining a rule that when triggered enable each of said corresponding plurality of keys to be signed, said rule being a logical combination of a plurality of conditions, said plurality of conditions each having an attribute that when true allow each of said plurality of conditions to be true; determining a rule associated with at least two of said plurality of keys; waiting until said a condition occurs before signing one of said at least two of said plurality of keys, said condition each having an attribute that when true allow said condition to be true; unlocking said address when said number of said plurality of keys are signed, which are not present in Group III.

The common technical features shared by Groups I-II are a method of electronic commerce payments comprising: a payment processor receiving a first fiat-currency amount and information, said payment processor initiating a transfer of said second fiat-currency amount to the payee deposit destination.

However, these common features are previously disclosed by US 2015/0178693 A1 (SOLIS). SOLIS discloses a method of electronic commerce payments (electronic payments; paragraph [0037]) comprising: a payment processor receiving a first fiat-currency amount and information (the payment processor receives the destination payment account and the total amount to be transferred in a fiat currency; paragraphs [0060], [0076]), said payment processor initiating a transfer of said second fiat-currency amount to the payee deposit destination (transferring the funds in a fiat currency into the specified payment account (payee deposit destination); paragraphs [0062], [0076]).

Since the common technical features are previously disclosed by the SOLIS reference, these common features are not special and so Groups I-II lack unity.

Since none of the special technical features of the Group III invention are found in more than one of the inventions, unity is lacking.