



CipherTrace Sentry API

Version 1.31 July 9, 2021

This document details the CipherTrace API, which provides data access to CipherTrace customers, which allows organizations to integrate CipherTrace REST APIs into their platform for real-time transaction monitoring and other forms of analysis. Today, the CipherTrace API service supports BTC, ETH, BCH, LTC, BNB, RSK, and ERC-20/721. It represents itself as an HTTPS based query service with JSON encoded data.

CipherTrace Sentry contains a Core API and an AML Risk Classification API, both of which can be used when assessing the risk and behavior of a specific address (see the FAQ for more details).

The Core API is an address and CipherTrace Cluster (wallet) query service providing attribution and transaction details.

The AML Risk Classification API provides risk classifications for addresses and transactions, based on the nature and transactional behavior of that address.

Since the Sentry API is an active project with many new features in development, CipherTrace reserves the right to perform minor non-breaking updates to the API, such as potentially adding additional fields to existing information structures.

If you have any questions or need assistance, please contact support@ciphetrace.com or your CipherTrace representative.

Table of Contents

History	7
Authentication	8
Wallet (Cluster) Queries	9
Wallet Data Structures	10
Owner	10
Wallet	10
Transaction Queries	11
Transaction Data Structures	11
Transaction History	11
TxInput	11
TxOutput	11
Transaction Detail	12
AddressInfo	13
Transactions	13
Address Queries	14
Address Data Structures	14
Address Tx	14
IP Info	15
Address Results	15
Queries	17
Wallet (Cluster) By Address	17
Wallet By Wallet Id	17
Wallet Addresses	18
Transaction History for Address	20
Details for transaction list	21
Address Search	25

Query Count for Account User	26
BCH Queries	27
BCH Wallet By Address	27
BCH Wallet By Wallet Id	27
BCH Wallet Addresses	28
BCH Transaction History for Address	28
Details for BCH transaction list	29
BCH Address Search	31
LTC Queries	32
LTC Wallet By Address	32
LTC Wallet By Wallet Id	32
LTC Wallet Addresses	33
LTC Transaction History for Address	33
Details for LTC transaction list	34
LTC Address Search	36
ETH Queries	38
ETH Wallet By Address	38
ETH Wallet By Wallet Id	38
ETH Wallet Addresses	39
ETH Transaction History for Address	39
Details for ETH transaction list	40
ETH Address Search	41
BNB Queries	42
BNB Wallet By Address	42
BNB Wallet By Wallet Id	43
BNB Wallet Addresses	43
BNB Transaction History for Address	44

Details for BNB transaction list	44
BNB Address Search	46
RSK Queries	48
RSK Wallet By Address	48
RSK Wallet By Wallet Id	49
RSK Wallet Addresses	49
RSK Transaction History for Address	50
Details for RSK transaction list	50
RSK Address Search	54
IP Queries	58
IP Result	58
Address Match	59
IP Address Search	59
AML Risk Scoring API	61
Risk Scores	61
Call Back	62
Bitcoin Risk Scoring API	62
Transaction Risk Score Info	62
AddressRisks Info	63
Address Risk Score Info	66
Ethereum Risk Scoring API	68
ETH Transaction Risk Score Info	68
ETH Address Risk Info	68
ETH AddressRisks Map Info	69
Bitcoin Cash Risk Scoring API	71
Transaction Risk Score Info	71
Bitcoin Cash Address Risks Info	71

Address Risk Score Info	73
Litecoin Risk Scoring API	74
Transaction Risk Score Info	74
Litecoin Address Risks Info	74
Address Risk Score Info	76
Binance Chain Risk Scoring API	77
Transaction Risk Score Info	77
BNB Address Risks Info	77
Address Risk Score Info	79
RSK Risk Scoring API	80
Transaction Risk Score Info	80
RSK Address Risks Info	80
Address Risk Score Info	82
BTC Watch List for Alerts	83
Changing and Inspecting the Watch List	83
Adding a BTC Address to watch	83
Removing a BTC Address from the watch list	83
Inspecting the entire watch list, use GET:	83
Clear the entire watch list	84
Updating User Preference for Webhook and Email Delivery	84
Receiving Webhook notifications	84
API FAQs (Frequently Asked Questions)	86
Wallet Address Queries	86
What do you mean by count and offset in regard to the Wallet Addresses Query?	86
What does it mean if I receive the message “404 Not Found - getAddressWallet: error address=<Crypto Address> not found” while performing an Address specific API call?	86
Ethereum	86

How do you gather information on an Ethereum address's balance?	86
Risk Scoring/Classification	87
Using Risk Classification and Attribution for AML/Transaction Monitoring	87
Can you please explain the callbackSeconds in the AML Risk Scoring API?	88
Attribution	88
What are all the Attributed entity types that you support?	88
Is an owner of a wallet (cluster) always an actual individual?	89
Do you have some example queries for entity type returns?	90

History

Date	Version	Changes	Author
March 26, 2019	1.12	Updated AML with additional risk scores	Jake Tarnow
April 11, 2019	1.13	Added breaking changes disclaimer	Jake Tarnow
May 17, 2019	1.14	Restructured, Added TOC	Frank Steegmans
May 30, 2019	1.15	Added Ethereum endpoints	David Wheeler
July 1, 2019	1.16	Updated 8 and 9 risk scores as well as updated risk explanations	Frank Steegmans
July 19, 2019	1.17	Updated descriptions, no more levels	Frank Steegmans
August 5, 2019	1.18	Update risk descriptions to match new classification algorithm	Frank Steegmans
September 19, 2019	1.19	Added BTC Watch List Alerts Added BCH queries	Rudi Cilibrasi David Wheeler
October 2, 2019	1.20	Added IP endpoint	David Wheeler
October 21, 2019	1.21	Added LTC queries	David Wheeler
November 4, 2019	1.22	Added BNB queries	David Wheeler
November 21, 2019	1.23		David Wheeler
April 20, 2020	1.24	Added Webhooks for Alerts	Frank Steegmans
May 11, 2020	1.24.1	Alerting Rest Hostname typo correction	David Wheeler
May 14, 2020	1.25	Added RSK queries	David Wheeler
June 2, 2020	1.25.1	Added minor clarifications	Catherine Woneis
June 9, 2020	1.25.2	Added minor url updates and RSK AML	Jake Tarnow
July 10, 2020	1.26b	Added Realtime BTC Beta	David Wheeler
July 10, 2020	1.26	Realtime BTC GA	Catherine Woneis
January 4, 2021	1.27	Ethereum Wallet id's updated	David Wheeler
March 24, 2021	1.28	Additions to data structures documentation and FAQs	Catherine Woneis
April 15, 2021	1.29	Additions to data structures documentation and FAQs	Catherine Woneis
May 17, 2021	1.30	Additions to IP data structure documentation	Catherine Woneis
July 9, 2021	1.31	Additional Implementation Recommendations	Catherine Woneis

Authentication

You will receive your Authorization Value via a CipherTrace One-time Share (CTOS) link. Click on the link to obtain the CipherTrace Authorization Value.

NOTE: the CTOS link is only accessible one time. Be sure to copy the Authorization Value when you click on the link. CTOS link example: <<https://secret.ciphertrace.com/...>>

For client authentication, the Authorization Value is provided with the following format:

<API VERSION>:<KEY ID>:<KEY SECRET>

An example value for the version 1 API might be:

ctv1:testkey:a12d6e87fada12

Wallet (Cluster) Queries

The CipherTrace wallet clustering implementation is an asynchronous process to the main blockchain import mechanism. This has the side effect of potential lag between the two databases. As a result, addresses not yet available in the main blockchain database might be included in a cluster, or, addresses available in the blockchain might not yet be clustered. Over time, this implementation will change to provide tighter synchronization.

Wallets are identified by a string encoded wallet id number, for example: 0000f42e6000. The format of this identifier can change in the future, so it's important not to make assumptions about the nature of its content.

Clustering is a highly dynamic operation. As a consequence, for every transaction processed, it is likely that wallets are merged. This can leave some input wallets to the transaction orphaned as all addresses are moved to the final wallet. For example, if addresses from wallets A, B, C and D are all used as inputs to a single transaction then all of these wallets will be merged. One of the Id's will be selected as the final Id and the others orphaned (so the final wallet might be given the Id of "B"). If queries are made to the orphaned wallet ids, they will return information regarding the new wallet.

Also, the ordering of addresses within a wallet is currently not constant – as wallets are merged the ordering of addresses within that wallet will change. Therefore, when queries are made for the address list for a given wallet it is important that the entire wallet is fetched rather than just a subset.

To help the client manage this, a wallet structure includes a revision number. This number is incremented when updates to the wallet are made.

Note that in CipherTrace Inspector (The Console Application), references to "Wallet" and "Wallet ID" are displayed as "Cluster" and "Cluster ID". A Bitcoin wallet is a collection of private keys, whereas the ID referred to here is actually a collection of addresses associated with an Input Cluster. The ID associated with a "cluster" is an internal CipherTrace ID.

The Cluster ID is a way of grouping Bitcoin addresses into one group that is likely to be controlled by a single user or by a service.

Note that one entity may control more than one cluster. Therefore, users should not equate the "Cluster ID" with all addresses likely to be controlled by an attributed or unattributed private key holder.

Note that although Inspector terminology has changed, the API terminology has not changed so as not to break implementations.

Wallet Data Structures

The wallet API uses the following data structures:

Owner

Field	Type	Description
name	String	Name of the owning entity (Coinbase, Locky, etc.)
url	String	URL of the owning entity (if available)
country	String	Abbreviated country code of residence (if known)
subpoenable	Boolean	Set to true if the entity is subpoenaable by US courts
type	String	Entity type if known (criminal, exchange, etc)

The owner of a wallet is the entity that we have identified through attribution and clustering, not an actual individual. If there is no attribution on the owner of the wallet, then this object will be empty.

Wallet

Field	Type	Description
walletId	String	CipherTrace Wallet Identifier
owner	Owner	Owner data structure
totalAddressCount	Integer	Total number of addresses in the wallet
revision	Integer	Incrementing revision number for the wallet. If the revision changes the wallet should be re-fetched.
walletIdChanged	Boolean (Optional field)	Set to true if the wallet id has changed. In this case the wallet should be re-fetched with the new wallet id.
addresses	Array[String]	List of addresses in the wallet. The set of addresses returned depends on query parameters.

Transaction Queries

Two forms of transaction queries are supported: transaction history for an address over a given date range, and details for a list of transactions.

Transaction Data Structures

Transaction History

This structure includes a list of transaction hashes that include the search address over a date range.

Field	Type	Description
address	String	Address that was queried
startDate	Int	Start date of the query range (Unix epoch time)
endDate	Int	End date of the query range (Unix epoch time)
transactions	Array of String	Array of transactions that included the searched address as an input or output

TxInput

A structure detailing an input to a transaction.

Field	Type	Description
pos	Int	Position of this input
address	String	Address used in this input
value	Long	Total coin spent for this input

TxOutput

A structure detailing an output from a transaction.

Field	Type	Description
pos	Int	Position of this output
address	String	Address used in this output
value	Long	Total coin deposited for this output

Transaction Detail

This structure represents details for a single transaction.

Field	Type	Description
txHash	String	Hash of the specified transaction
date	Int	Date of the transaction (Unix epoch time)
blockHeight	Long	The block height that this transaction was a part of
total	Long	Total value of the transaction (including fees)
fee	Long	Transaction fee
inputs	Array TxInput	Transaction inputs
outputs	Array of TxOutput	Transaction outputs
Error	String	Optional field that is populated if there was an error querying this transaction

These fields are only applicable to Ethereum

Field	Type	Description
txType	String	The transaction type (for example, transfer, call, internal, etc)
children	Vector	List of child transactions
nonce	Long	The number of transactions sent from a given address
toAddress	String	Address funds have been sent to
fromAddressBalance	BigDecimal	Balance of the sent from address
gasPrice	BigInt	The fee required to successfully

		conduct the transaction, expressed in Wei
fromAddress	String	Address funds were sent from
gasLimit	BigInt	The maximum price the user is willing to pay when sending a transaction, or performing a smart contract function
gasUsed	BigInt	The gas used in the transaction. The difference between gasLimit and gasUsed is returned to the user.
toAddressBalance	BigDecimal	Balance of the sent to address

These fields are applicable only to Binance Network (BNB)

Field	Type	Description
items	Vector	A list of items involved in the transaction
asset	String	Asset being exchanged
feeAsset	String	Asset in which the fee was paid

AddressInfo

A structure detailing attribution information about an address.

Field	Type	Description
wallet	Wallet	Wallet details for this address

Transactions

A structure detailing a list of transactions.

Field	Type	Description
transactions	Array of TxDetail	Details of the queried transactions.

addresses	Map of address to AddressInfo	Hash table detailing AddressInfo structures for all input and output addresses in the transactions array.
ipHistory	Map of Vector of IPInfo	Hash map of IP Address information for all addresses and transactions contained in this structure. Indexed by address or transaction hash with the key only specified if there is IP information.

Address Queries

The address queries allow for address balance, transaction history, and IP address searches. This new service supersedes the address transaction search functionality.

Address Data Structures

Address Tx

This structure details the balance of an address at the specified transaction.

Field	Type	Description
txHash	String	Transaction hash for this balance
blockHeight	Long	The block height that this transaction was a part of. Will not be set for mempool Transactions
mempool	Boolean	True for transactions in mempool and not set for transactions that have a blockHeight
balance	Double	Address balance after this transaction is applied.
spent	Double	How much this address contributed to the transaction if it was an input
received	Double	How much this address received from this transaction if it was an output

IP Info

This structure details an IP address hit against an address or transaction.

Field	Type	Description
ipAddress	String	IP address
Country	Optional String	Country in which this IP is located
City	Optional String	City location of this IP
Latitude	Optional Double	Latitude of this IP
Longitude	Optional Double	Longitude of this IP
Date	Int	Epoch time this IP address match was collected
ClientVersion	String	The BTC client version that was used

Address Results

This structure details the balance of an address at the specified transaction.

Field	Type	Description
address	String	Bitcoin Address
startDate	Int	Start Date for query
endDate	Int	End Date for query
wallet	Wallet	Wallet (cluster) information for this address
balance	Double	Current balance for this address (for all time)
totalDepositCount	Int	Number of deposits (transaction output to this address) for all time
totalSpendCount	Int	Number of spends (transaction inputs from this address) for all time
totalDeposits	Double	Total amount deposited to this address for all time
totalSpent	Double	Total amount spent by this address for all time
lastUsedBlockHeight	Int	Blockheight of last transaction involving this address

inCase	Boolean	True if this address is referenced in any case
txHistory	Optional Vector of AddressTx	Transaction history (within specified date range) for this address
ipHistory	Optional Vector of IPInfo	IP Address history (within specified date range) for this address
queryEndingBalance	Int	Balance at time of endDate. This is either the final tx balance in the returned results or the balance at the time of the last tx before the date range
querySpent	Int	How much address spent in the returned tx results
queryDeposits	Int	How much address deposited in the returned tx results
queryDepositCount	Int	Number of deposits in the returned tx results
querySpendCount	Int	Number of spends in the returned tx results

Fields for Binance Network (BNB) only

Field	Type	Description
querySummary	Vector	Query summary information
locked	Double	Amount that has been locked
frozen	Double	Amount that can not be transferred, spent in orders or any other transaction until unfrozen.
free	Double	Amount that is free
summary	Vector	Summary information

Queries

Queries can be performed through any API GUI such as Postman or via customized scripts and simple curl commands. Please note that the HTTPS certificate verification is on a self-signed cert, so you may want to ignore the cert verification.

For Postman:

- Go to settings and select option to ignore SSL certificate verification
- Set Authorization Tab as “No Authorization”
- Set Headers Tab to:
 - Key = “Authorization”
 - Value = “ctv1:username:secretkey”
- Place in the url for the given GET query and press Send

For Curl:

- `curl -i -H "Authorization:ctv1:username:secretkey" "https://rest.ciphertrace.com/api/v1/tx/search?address=17aaJMZqArjH3eufDaEJ3HZg74BJT7Gmgz&startdate=1459363904&enddate=1459373001"`

Wallet (Cluster) By Address

This query returns wallet (cluster) information for a specified address.

<https://rest.ciphertrace.com/api/v1/wallet?address=17aaJMZqArjH3eufDaEJ3HZg74BJT7Gmgz>

This returns a Wallet Response. For example, the above query returns:

```
{
  "walletId": "08045fcb",
  "owner": {
    "name": "Locky",
    "subpoenable": false,
    "url": "",
    "country": "RU",
    "type": "criminal"
  },
  "totalAddressCount": 7093,
  "revision": 1
}
```

A single address can be provided for the “address” parameter.

Wallet By Wallet Id

This query returns wallet information for a specified wallet id (CipherTrace cluster id).

https://rest.ciphertrace.com/api/v1/wallet?wallet_id=08045fcb

This returns a Wallet Response. For example, the above query returns:

```
{
  "walletId": "08045fcb",
  "owner": {
    "name": "Locky",
    "subpoenable": false,
    "url": "",
    "country": "RU",
    "type": "criminal"
  },
  "totalAddressCount": 7093,
  "revision": 1
}
```

A single wallet id can be provided for the “wallet_id” parameter. If the wallet state has changed the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id which has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

Wallet Addresses

This query returns wallet addresses for a specified wallet id.

https://rest.ciphertrace.com/api/v1/wallet/addresses?wallet_id=08045fcb&count=100&offset=100

This returns a Wallet Response with addresses included. For example, the above query returns:

```
{
  "addressOffset": 100,
  "walletId": "08045fcb",
  "revision": 1,
  "owner": {
    "name": "Locky ",
    "subpoenable": false,
    "url": "",
    "country": "RU",
    "type": "criminal"
  },
  "totalAddressCount": 7093,
  "addresses": [
    "1EktpvcfCPpyqbuRGyL6UkDgJHWDJQAScQ",
    "1Fr8xcEe9LkqN8Kgnr5dqj4cnyU7KJLNpb",
    "1PP1x2d42HL6vFy7XA5haUewuD67FpwxRa",
    "1DRPAA6m6gLez77PureMFiXhxS6rMg5Q3",
    "1HzEKvHPYHUnvCMzAndjLpJnMwvUDL5nd5",
    "1FrrQ67wcpDLisYaGshw54f2veHDzZTTQe",
    "1GXMT15AQXsgr2fHEqkUUitU6vR6SxucQd",
    "14hczTzPoa8cxbLSWmxutX4os6Vzs3QH5M",
    "1L7xBY9uq22V3UHtEdPp3DCbWL45TYE6XW",
    "1F5YcKGiT5i2wvKNwdxDWbbgzYzz2Hf36h",
    "1ELcjKDtgnlzp4zccnmvy2MwMzvlJWvPlE",
    "1FUKHd3moVYTMFYpHggERjYp7HrzccMPPa",
    "1Agkv6bWdeE7t1UH72vDdFtLsiGkNdgAPU",
    "1GiFtyKRfbSTX6xJoQ6X2ABkizhcMmQF3Z",
    "1HcUBeADVWJPJ8DtSVbjPpowWBMtcF8shv",
    "1DnSnGfbCiLjRQSPS9pf6utGjJ9XbMD6ta",
    "1JPQQlTrjXrqRqEofEDoC2ZzfP9KvyG1FH",
    "1QLH65j7zcZePNBhs5YyD5diG4kZVTXZre",
  ]
}
```

"1GYURtbqcnF9H3fvu7PgD3yopQWWA1GGQA",
"1AjxCSfAwpgTCLcGbKxCZTVZ7AxDo2CUFb",
"1Jv2h3YxtdMC7Y1D24qn8psympebzXMeCZ",
"1DvomEXpbmw1Z37RiwY653N1dfS1UZCXC3",
"1H7dwK3VCK6RqoRc7FmcZDiiEFKJboxesXr",
"1GusLDqkL1ShHDgSyRGPskS7haGogxCYRU",
"1Fv1fK1JsacJ1fVCHfoU3fJDyMHxNhCmjL",
"123zTvJw931gKezq4bMwaBS45YBQjJh3pZ",
"1EyfeFpyJFrr5ahb56PJSmFRYajGFHqey",
"16Pd7Rgz2t45LTpgYqpeLG3VgVrb8KwPK",
"1Cy8AbHkMzWTBSJhJtnUCXrvdfV9wCjcd",
"1CwxcDazTJk7h1BJwpABMLBqVajxCrP41c",
"1J2KmDQyQCQJebuzdS5RFk3CSjyMZw8A28",
"1PyPvKT4XQcLwoCUwi9FVNVjRWj86oQya",
"1GRMuB5KsLRjSDnyP7NjXohLFmpxktFWSJ",
"15JouskM1UHmZ2M2kUtNWNUGDwiQVtmoGA",
"17FANmXhwoDjUy276dskQwt3imejgYxwq4",
"183pjpcdni3SgK5yZYCNdtz8TmsiZYxYQ",
"1MWrS2P9HUdUtsDzNAkUQXy9ZTwALwYaH1",
"1AoG69yW5yrnKqKMcR1mbGvqCvLxwDAqQs",
"1PerzYxYd4ukRqMAHMcA1DuMU3aP5bPdeg",
"19A9tWsdB68KZgcKYcxHYtqn2sA9HR2ZZU",
"12mPlrBBdQNu6M2FmCx5WQpawsbzGH5AL4",
"13fbQ3WeYtTwFYcQuvmYaZmMH4Sn7iFmUo",
"1CFL9jYjs48Nv5nHgEMhXiqz5JKvU2kvTv",
"18uYMTeZxNLoANKv483CQUtVqx7g46fZ18",
"12LyHDCEGkxdVGygfSintzKhXeNiKXCMFt",
"1h5Nx6jA4aLdj2Qn8NydX7bCAxi3HQkSU",
"19A4thzhK8Eq6PHbR6eik1cDqH9HVjryA5",
"1Mip4rxtheHqkREe9mzGZGXzNTBbrShkiu",
"19HP4WhwUc3Hy6pqfNZiJfYPrhBD2xvtNA",
"1DPQiNFfn3L5ZGVdzVCQuSRkUhhXhmDSay",
"12GM2RDDWLCpAAzLDNadnvegBgZBiHMHun",
"1BAi9bB9PKpNiGMhQVVhYo4D2ioj7hgfpA",
"16EDTPCBUAtrNRjzSB9v3PRrUMHjZMQ3v",
"1QEhETnNBJeQbwi2HW37Xu4Nh3fMSVXn9R",
"17JxnAGqBnq5Zg3qKhVVXymNyNrpBxZrAA",
"19SspSUHzzGBFMavW3hZppxZtdo66cNG4F",
"1EexlfZZBPwkHj9bZGT4QZTegajqoYQbEY",
"1PqXDoWQerCSfj2ummFUV88sdFCnbzvV57",
"1japUvvpdz4uT49CSMUjqm4n8qsJhrKu",
"12FQZBebt7nQgA7VubbGHQzKbUTjk9Avny",
"1Eru7ozyAjVmA4URtmwGNUMff5fNxKneJPL",
"1H8KjbPsPSGCvRLj68vF3VoYzYzMhP9nuK",
"1HuLrXAKN9QiQW5e6a7q1p4bkhAQ5tjHtn",
"1JLdDwCbh2uyPiQMBBn9SJBodKcy1uqUo",
"1K4UUqnnq9R2vUufoDECegokgdGfBNjYRj",
"1Jta5JwTgtDBjW86tnEJmJRYj9LAmX2jjP",
"1FW9xGDLs7Qrkr7fWCCZFJfM98v2WL61eg",
"18QTYUJiBRuEah4RXnGZgHsey6DEhzcio",
"1Pkts269uSb3nbt9EYcQpT1jGuQfviEMN6",
"19LZB5QkGQXbWB5zAxSDy3p6WkfsSvdFbB",
"1LBd2Ddm9iYBBYvYGgb6wwJjVsujAHbcEY",
"1DvrGU3HGfBRp6Wb8wiAds53bSPUtYSjMc",
"1EVN8Kq6gX6QM4dC7bRgid9jhJLpVaQqER",
"14g2MB8QVT8nE7uhcRPV6X8cjvpjs3Ezx",
"1Fs1T2RESrAT44zovp473H5F8NpMCXdwct",
"17t2tsxe8wWo8o1YG5CnRAujitRfv2n6Bi",
"16rUr5Sx5eFF7LK5mprgdeESZYHthi52og",
"18cyCdZ38d7xHKHCpjB61xKdAzerdwoF7",
"1PGRubz4R6CEa41kKjdr4p1sknAWhKbCE",
"15GTDsWZHvFxnfnHxFQbRHFfFqEe2Nqos8",
"1QBGGwGFRrFLvzxx3kojQYUczuEbUne6Xd",
"1kjChGREPEJtKAim4Ebvrc3mwl1QrEq8h",
"15UheiezGRMGh2DsJv1JSKXYSugJcb2NnP"

```

    "1A4gemYhncwf78krmXxPgUK7fNV836GNR",
    "1L8Ksxr3zYXncLPzxFEHj2F8GZLhnJfPeD",
    "1E4nbMYzgBZG5PwfjuaiTqGHAbD3Ye4aG8",
    "1FzNEXoi85QpwNVhNkwUGx5qK2jYrPBeY8",
    "1FwGLgBQ8YpjjgH6VuoTjYyV7bFCpVCTZS2",
    "1GkYNcCCkTxckim7cV7hMCy5kRFwnh3uUc",
    "16S4jvoMttnnigCyBEzRoWTMnxbihWkg3w",
    "18gGwoyKzegNz4QZxE1TJDtKLgs38Xsjn9",
    "1HPNjrrjDtm14zrrJHZ2dmYyfjviV2acyPK",
    "1PW9KS8TlySvfoiS7KnwPDjQCkDi8SQDbk",
    "14eMZx6wiU3wsfk9sbFbepbiQrUJokDuv7",
    "19Pe7r8WFzyEMBZVMxgehCQzk36VTvcqz6",
    "1BgRb5VQ4aetvqmVCsTUBkEJ3sg9Y6QmZL",
    "1PpBWFijScRfFT3gF5iwZSulvFhKyhQ7BY",
    "1FzkKdTTMZQLMazzhn7oLz8hBUcFJkZh1x",
    "1Q8rVutEc2BTeBexsXTFr1WnD9rPUxEAkS",
    "1B4wuXbhNRsf7H6MuqWWu2FG3jRwVBwQn"
  ]
}

```

A single wallet id can be provided for the “wallet_id” parameter. A starting address offset is provided with the “offset” parameter. The count parameter must be between 1 and 10000.

Offset and count are used to page through the address list. For example, if your first query is offset=100 and count=1000, then your next query would be offset=1100 and count=1000 (or whatever count value you prefer).

If the wallet state has changed, the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id that has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

Transaction History for Address

NOTE: This query is largely superseded by the new Address Search query (which returns address balance, balance history and IP Address information).

This query returns a list of transactions that have included a specified address within a date range.

<https://rest.ciphertrace.com/api/v1/tx/search?address=17aaJMzqAriH3eufDaEJ3HZg74BJT7Gmgz&startdate=1459363904&enddate=1459373001&mempool=true>

In this query, the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. The mempool flag can be used to include transactions that are still in mempool (defaults to false)

As an example, the above query returns the following JSON:

```

{
  "address": "17aaJMzqAriH3eufDaEJ3HZg74BJT7Gmgz",
  "startDate": 1459363904,
  "endDate": 1459373001,
  "transactions": [
    "19e0886e6c6bdade6eb6fbae8aa0e83929cd4c6cf31fc442ff596af5c7f3035a",
    "e4bb4a6c82592be5e981b8551d97456bb508e6662d5524aacb837137b66f0543"
  ]
}

```

20

```
]
}
```

Details for transaction list

This query returns details on a specified list of transaction hashes (maximum of 10 hashes) as well as attribution data for all addresses used in the transactions.

<https://rest.ciphertrace.com/api/v1/tx?txhashes=19e0886e6c6bdade6eb6fbae8aa0e83929cd4c6cf31fc442ff596af5c7f3035a,3ea7b3067066c22cc58f577ed6aaf7fbac39c3202a05e70899bf5622e5e6afaf>

The txhashes parameter specifies an array of comma separated transaction hashes to search on (no white space allowed). Please limit the query to a maximum of 10 transactions at present.

NOTE: This query has been updated to include an ipHistory map which details any IP address matches for all transaction and address hashes included in the response. Only hashes that have IP Information are included in the map.

The above query returns the following JSON:

```
{
  "transactions": [
    {
      "txHash": "19e0886e6c6bdade6eb6fbae8aa0e83929cd4c6cf31fc442ff596af5c7f3035a",
      "outputs": [
        {
          "pos": 0,
          "address": "18hoczynjLg3hMdAduhDig3hh5vrnEvyB8",
          "value": 5.84995069
        },
        {
          "pos": 1,
          "address": "1VrUhJEuaMP3GPWL3ZbSxx6a3TTRwchNY",
          "value": 0.01773592
        }
      ],
      "total": 5.86818045,
      "inputs": [
        {
          "pos": 0,
          "address": "1QEF4yDuRZGgRLcn4R5oyZ5PuwgwRxSiyK",
          "value": 0.09858045
        },
        {
          "pos": 1,
          "address": "14rGFdBqksi932Tpq6K56isQL2MxUHdWeg",
          "value": 0.0297
        },
        {
          "pos": 2,
          "address": "1Fafr9D6zzQdNJB3mswRWpGjyR6LbDtPtz",
          "value": 5.1
        },
        {
          "pos": 3,
          "address": "17aaJMZqArjH3eufDaeJ3HZg74BJT7Gmgz",
          "value": 0.5
        }
      ]
    }
  ]
}
```

```

        "pos": 4,
        "address": "17bVoAYWqUhQ91qG7RbkEtLXVNjJKB71W",
        "value": 0.1
    },
    {
        "pos": 5,
        "address": "1M6piyCpJdRgZzswChBoi3E8ijyg8Dfgmx",
        "value": 0.0399
    }
],
"date": 1459373001,
"blockHeight": 405041,
"fee": 0.0004938399999998566
},
{
    "txHash": "3ea7b3067066c22cc58f577ed6aaf7fbac39c3202a05e70899bf5622e5e6afaf",
    "outputs": [
        {
            "pos": 0,
            "address": "1A3jaFQQYrGqZqubrcAfWUH4eiX1AevQCV",
            "value": 0.0304381
        },
        {
            "pos": 1,
            "address": "133uy6u2VuYWNwyrNnUhYJj3GkoeTtzpcg",
            "value": 1.90684622
        }
    ],
    "total": 1.93786898,
    "inputs": [
        {
            "pos": 0,
            "address": "1M8MSttZPzuuRmpcccNptPKKf5k3s3qq7H",
            "value": 1.93786898
        }
    ],
    "date": 1513127119,
    "blockHeight": 498980,
    "fee": 0.0005846599999999036
}
],
"addresses": {
    "1A3jaFQQYrGqZqubrcAfWUH4eiX1AevQCV": {
        "wallet": {
            "walletId": "148121e7",
            "owner": {},
            "totalAddressCount": 1,
            "revision": 0
        }
    },
    "1M6piyCpJdRgZzswChBoi3E8ijyg8Dfgmx": {
        "wallet": {
            "walletId": "08045fcb",
            "owner": {
                "name": "Locky",
                "subpoenable": false,
                "url": "",
                "country": "RU",
                "type": "criminal"
            },
            "totalAddressCount": 7093,
            "revision": 1
        }
    },
    "1M8MSttZPzuuRmpcccNptPKKf5k3s3qq7H": {

```

```

    "wallet": {
      "walletId": "148121e6",
      "owner": {},
      "totalAddressCount": 1,
      "revision": 0
    }
  },
  "1Fafr9D6zzQdNJB3mswRWpGjyR6LbDtPtz": {
    "wallet": {
      "walletId": "08045fcb",
      "owner": {
        "name": "Locky",
        "subpoenable": false,
        "url": "",
        "country": "RU",
        "type": "criminal"
      },
      "totalAddressCount": 7093,
      "revision": 1
    }
  },
  "1VrUhJEuaMP3GPWL3ZbSxx6a3TTRwchNY": {
    "wallet": {
      "walletId": "08045fcb",
      "owner": {
        "name": "Locky",
        "subpoenable": false,
        "url": "",
        "country": "RU",
        "type": "criminal"
      },
      "totalAddressCount": 7093,
      "revision": 1
    }
  },
  "17bVoAYWqUhQ91qG7RbkEtLXVNjJKB71W": {
    "wallet": {
      "walletId": "0000f42e8000",
      "owner": {
        "name": "Locky Ransomware 1",
        "subpoenable": false,
        "url": "",
        "country": "RU",
        "type": "criminal"
      },
      "totalAddressCount": 7093,
      "revision": 1
    }
  },
  "18hoczynjLg3hMdAduhDig3hh5vrnEvyB8": {
    "wallet": {
      "walletId": "0839285b",
      "owner": {},
      "totalAddressCount": 6,
      "revision": 0
    }
  },
  "133uy6u2VuYWNwyrNnUhYJj3GkoeTtzpcg": {
    "wallet": {
      "walletId": "148121e8",
      "owner": {},
      "totalAddressCount": 1,
      "revision": 0
    }
  },
},

```

```

"1QEF4yDuRZGgRLcn4R5oyZ5PuwgwRxSiyK": {
  "wallet": {
    "walletId": "08045fcb",
    "owner": {
      "name": "Locky",
      "subpoenable": false,
      "url": "",
      "country": "RU",
      "type": "criminal"
    },
    "totalAddressCount": 7093,
    "revision": 1
  }
},
"14rGFdBqysi932Tpq6K56isQL2MxUHdWeg": {
  "wallet": {
    "walletId": "08045fcb",
    "owner": {
      "name": "Locky",
      "subpoenable": false,
      "url": "",
      "country": "RU",
      "type": "criminal"
    },
    "totalAddressCount": 7093,
    "revision": 1
  }
},
"17aaJMzqArjH3eufDaEJ3HZg74BJT7Gmgz": {
  "wallet": {
    "walletId": "08045fcb",
    "owner": {
      "name": "Locky",
      "subpoenable": false,
      "url": "",
      "country": "RU",
      "type": "criminal"
    },
    "totalAddressCount": 7093,
    "revision": 1
  }
},
"ipHistory": {
  "133uy6u2VuYWNwyrNnUhYJj3GkoeTtzpcg": [
    {
      "city": "Tottenham",
      "latitude": 51.6,
      "country": "United Kingdom",
      "longitude": -0.0667,
      "date": 1513108830,
      "ipAddress": "77.102.83.142",
    }
  ],
  "1A3jaFQQYrGqZqubrcAfWUH4eiX1AevQCV": [
    {
      "city": "Tottenham",
      "latitude": 51.6,
      "country": "United Kingdom",
      "longitude": -0.0667,
      "date": 1513108830,
      "ipAddress": "77.102.83.142",
      "clientVersion": "/breadwallet:0.6.2/"
    }
  ]
}
]

```

```
}  
}
```

Address Search

This query returns all information regarding an Address. Current balance information as well as (optional) balance history with transaction hashes and IP Address match history.

<https://rest.ciphertrace.com/api/v1/address/search?features=tx,ip&address=133uy6u2VuYWNwyrNnUhYj3GkoeTtzpcg&startdate=1513108829&enddate=1513127120 &mempool=true>

In this query the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. Features is also an optional parameter that details which type of optional information the requester wishes (as a comma separated list). "tx" requests a transaction history within the date range. "ip" requests IP Information within the date range. The "mempool" flag enables the inclusion of transactions that are still in mempool

As an example, the above query returns the following JSON:

```
{  
  "lastUsedBlockHeight": 498980,  
  "querySpent": 1.90684622,  
  "queryEndingBalance": 0,  
  "endDate": 1513127120,  
  "totalSpendCount": 1,  
  "totalSpent": 1.90684622,  
  "totalDepositCount": 1,  
  "queryDeposits": 1.90684622,  
  "currentBalance": 0,  
  "queryDepositCount": 1,  
  "ipHistory": [  
    {  
      "city": "Tottenham",  
      "latitude": 51.6,  
      "country": "United Kingdom",  
      "longitude": -0.0667,  
      "date": 1513108830,  
      "ipAddress": "77.102.83.142"  
      "clientVersion": "/breadwallet:0.6.2/"  
    }  
  ],  
  "querySpendCount": 1,  
  "address": "133uy6u2VuYWNwyrNnUhYj3GkoeTtzpcg",  
  "txHistory": [  
    {  
      "txHash": "3ea7b3067066c22cc58f577ed6aaf7fbac39c3202a05e708999bf5622e5e6afaf",  
      "txIndex": 281267556,  
      "balance": 1.90684622,  
      "date": 1513127119,  
      "received": 1.90684622,  
      "spent": 0  
    },  
    {  
      "txHash": "ca67ba5cad5b9bd767893b3c8ba110c5a41ab5f5026861bbf9d7cbd17fe704bf",  
      "txIndex": 281267557,  
      "balance": 0,  
      "date": 1513127119,  
      "received": 0,  
    }  
  ]  
}
```

```

        "spent": 1.90684622
    }
  ],
  "inCase": false,
  "startDate": 1513108829,
  "wallet": {
    "walletId": "148121e8",
    "owner": {},
    "totalAddressCount": 1,
    "revision": 0
  },
  "totalDeposits": 1.90684622
}

```

Query Count for Account User

This query returns all query count information for the given user.

https://rest.ciphertrace.com/api/v1/account/query_count

This query uses the supplied Authentication header to query results for the associated user. The response will return with a breakdown by month of all counts for both API and AML queries respectively. As an example, the above query returns the following JSON:

```

{
  "userName": "someUserName",
  "history": {
    "aml": [
      {
        "year": 2017,
        "month": 9,
        "queryCount": 9
      },
      {
        "year": 2017,
        "month": 12,
        "queryCount": 12
      },
      {
        "year": 2018,
        "month": 1,
        "queryCount": 13
      },
      {
        "year": 2018,
        "month": 12,
        "queryCount": 8
      }
    ],
    "api": [
      {
        "year": 2018,
        "month": 12,
        "queryCount": 251
      }
    ]
  },
  "allTime": {
    "aml": 42,
    "api": 251
  }
}

```

BCH Queries

Bitcoin Cash queries vary from their standard bitcoin queries in two ways. First, they require prepending “bch_” to endpoint URL after the API version. Second, they require the use of bitcoin cash formatted address hashes. Legacy addresses should be converted to the “q” style cash addresses. The “bitcoincash:” prefix should be omitted.

BCH Wallet By Address

This query returns wallet information for a specified Bitcoin Cash address.

https://rest.ciphertrace.com/api/v1/bch_wallet/?address=pzt7ezr9gpdph6n283j657fc4qscrdwx3c9hdpaldy

This returns a Wallet Response. For example, the above query returns:

```
{
  "walletId": "03a2c629",
  "owner": {
    "name": "Bitstamp.net",
    "subpoenable": false,
    "url": "http://www.bitstamp.net",
    "country": "LU",
    "type": "exchange"
  },
  "totalAddressCount": 217394,
  "revision": 0
}
```

A single address can be provided for the “address” parameter.

BCH Wallet By Wallet Id

This query returns wallet information for a specified wallet id.

https://rest.ciphertrace.com/api/v1/bch_wallet/?wallet_id=03a2c629

This returns a Wallet Response. For example, the above query returns:

```
{
  "walletId": "03a2c629",
  "owner": {
    "name": "Bitstamp.net",
    "subpoenable": false,
    "url": "http://www.bitstamp.net",
    "country": "LU",
    "type": "exchange"
  },
  "totalAddressCount": 217394,
  "revision": 0
}
```

A single wallet id can be provided for the “wallet_id” parameter. If the wallet state has changed the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id which has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

BCH Wallet Addresses

This query returns wallet addresses for a specified wallet id.

https://rest.ciphertrace.com/api/v1/bch_wallet/addresses?wallet_id=03a2c629

This returns a Wallet Response with addresses included. For example, the above query returns:

```
{
  "addressOffset": 0,
  "walletId": "03a2c629",
  "revision": 0,
  "walletIdChanged": false,
  "owner": {
    "name": "Bitstamp.net",
    "subpoenable": false,
    "url": http://www.bitstamp.net,
    "country": "LU",
    "type": "exchange"
  },
  "totalAddressCount": 217394,
  "addresses": [
    "pzt7ezr9gpdph6n283j657fc4qscrdwx3c9hdpaldy",
    "pqrpjhtr29egkdlf93rztkhw4y6crk6r2yj8k2rjpe",
    "pqmud4zkyjqyd7cdvgzcp5dux37npflrhg0u8k6uqg",
    ...
  ]
}
```

A single wallet id can be provided for the “wallet_id” parameter. A starting address offset is provided with the “offset” parameter. The count parameter must be between 1 and 10000.

Offset and count are used to page through the address list. For example, if your first query is offset=100 and count=1000, then your next query would be offset=1100 and count=1000 (or whatever count value you prefer).

If the wallet state has changed, the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id that has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

BCH Transaction History for Address

This query returns a list of transactions that have included a specified address within a date range.

https://rest.ciphertrace.com/api/v1/bch_tx/search?address=qrlfsgth5nq6sx0478q5puml2g5d65rcsv5h35yc5n

In this query, the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. As an example, the above query returns the following JSON:

```
{
  "address": "qrlfsgth5nq6sx0478q5pum12g5d65rcsv5h35yc5n",
  "startDate": 0,
  "endDate": 1913732049,
  "transactions": [
    "94f6db2afade837114fed493c69273edbc1e9933d58350c633b4550c3bfd4159",
    "743dcb0efc5bd90367dc39c7faedf224399338f7b6757c9c0ea44a7ea9cc7cd4"
  ]
}
```

Details for BCH transaction list

This query returns details on a specified list of transaction hashes (maximum of 10 hashes) as well as attribution data for all addresses used in the transactions.

https://rest.ciphertrace.com/api/v1/bch_tx?txhashes=1111002bbe965ba181da0c63db4c255dd1e81eca9c10a1578a6a490c065f21d4,f96b6f05faf74f1c3e33d365cc83203cf31bd67b756321db4ab54c0a0f66aaf8

The txhashes parameter specifies an array of comma separated transactions hashes to search on (no white space allowed). Please limit the query to a maximum of 10 transactions at present.

NOTE: This query has been updated to include an ipHistory map which details any IP address matches for all transaction and address hashes included in the response. Only hashes that have IP Information are included in the map.

The above query returns the following JSON:

```
{
  "transactions": [
    {
      "txHash": "1111002bbe965ba181da0c63db4c255dd1e81eca9c10a1578a6a490c065f21d4",
      "outputs": [
        {
          "pos": 0,
          "address": "qqqfv026xdaqdru0zcynd6819qn4kqhv6s7rtwxflg",
          "value": 0.3
        },
        {
          "pos": 1,
          "address": "qq3vpr7hyeaphsf515asmz7qww3fjj3v0q9atekxah",
          "value": 2.66584708
        },
        {
          "pos": 2,
          "address": "qr5m999harx1phgv2g5ntpel7hndqn9p4q2y8ee0cq",
          "value": 0.00788939
        }
      ]
    },
    {
      "total": 2.97373647,
      "inputs": [
        {
          "pos": 0,
```

```

        "address": "qrmf7ymjy4rkp20qv8cwfpxs5qxczkr9lcl3w73xry",
        "value": 2.96584708
    },
    {
        "pos": 1,
        "address": "qz7jhxx75fs4a5zp22mqrkyh288gtepqq5mfxvsfv2",
        "value": 0.00838939
    }
],
"date": 1381345912,
"fee": 0.00050
},
{
    "txHash": "f96b6f05faf74f1c3e33d365cc83203cf31bd67b756321db4ab54c0a0f66aaf8",
    "outputs": [
        {
            "pos": 0,
            "address": "qqnh7j4254qclfy3uzk0r3c5gtgzhwvugqr1tekdza",
            "value": 0.3
        },
        {
            "pos": 1,
            "address": "qz62e6pdhxxtl90xdlgczktac7lz4ws4p5updfqq8n",
            "value": 0.0042922
        }
    ],
    "total": 0.3042922,
    "inputs": [
        {
            "pos": 0,
            "address": "qqqfv026xdaqdru0zcynd6819qn4kqhv6s7rtwxflg",
            "value": 0.3
        },
        {
            "pos": 1,
            "address": "qprrp3pua775jfnwv3n9pyr07p10cgpnhgcvwte88t",
            "value": 0.0047922
        }
    ],
    "date": 1381345912,
    "fee": 0.00050
}
],
"addresses": {
    "qrmf7ymjy4rkp20qv8cwfpxs5qxczkr9lcl3w73xry": {
        "wallet": {
            "walletId": "0131025c",
            "owner": {},
            "totalAddressCount": 2,
            "revision": 0
        }
    },
    "qz62e6pdhxxtl90xdlgczktac7lz4ws4p5updfqq8n": {
        "wallet": {
            "walletId": "01310b02",
            "owner": {},
            "totalAddressCount": 2,
            "revision": 0
        }
    }
},
...
},
"ipHistory": {}
}

```

BCH Address Search

This query returns all information regarding an Address. Current balance information as well as (optional) balance history with transaction hashes and IP Address match history.

https://rest.ciphertrace.com/api/v1/bch_address/search?startdate=0&features=tx,ip&address=qrlfsgth5nq6sx0478q5puml2g5d65rcsv5h35yc5n

In this query the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. Features is also an optional parameter that details which type of optional information the requester wishes (as a comma separated list). "tx" requests a transaction history within the date range. "ip" requests IP Information within the date range.

As an example, the above query returns the following JSON:

```
{
  "lastUsedBlockHeight": 599115,
  "querySpent": 23.424921529999999,
  "queryEndingBalance": 0.03935368,
  "endDate": 1913732049,
  "totalSpendCount": 665,
  "totalSpent": 23.42492153,
  "totalDepositCount": 802,
  "queryDeposits": 23.46423642,
  "currentBalance": 0.03935368,
  "queryDepositCount": 620,
  "ipHistory": [],
  "querySpendCount": 533,
  "address": "qrlfsgth5nq6sx0478q5puml2g5d65rcsv5h35yc5n",
  "txHistory": [
    {
      "txHash": "0f6aee950e9cb7122c85884b928ba3b7f3024918a80384f4df48f6e53c99dcac",
      "txIndex": 275619031,
      "balance": 0.00003438,
      "date": 1564334608,
      "received": 0.00003438,
      "spent": 0.0
    },
    {
      "txHash": "bc87e98ef01941f6c51278a1135cfa4c61d7165f88ec262821a668ffa6578c8f",
      "txIndex": 275619032,
      "balance": 0.00003438,
      "date": 1564334608,
      "received": 0.0,
      "spent": 0.00003879
    },
    ...
  ],
  "inCase": false,
  "startDate": 0,
  "wallet": {
    "walletId": "118ad3de",
    "owner": {},
    "totalAddressCount": 206,
    "revision": 0
  },
  "totalDeposits": 23.46427521
}
```

LTC Queries

Litecoin queries are nearly identical to the standard Bitcoin queries other than operating on LTC addresses. The API accepts Litecoin addresses in the L, ltc, and M formats. Legacy '3' addresses are not supported and should be converted to the P2SH 'M' format before being used in a query.

LTC Wallet By Address

This query returns wallet information for a specified Litecoin address.

https://rest.ciphertrace.com/api/v1/ltc_wallet/?address=LQcctH7yCV1qh97ktAHWHAAbDHtc5hgCdAF

This returns a Wallet Response. For example, the above query returns:

```
{
  "walletId": "002ddcc3",
  "owner": {
    "name": "Kraken.com",
    "subpoenable": true,
    "url": "https://www.kraken.com",
    "country": "US",
    "type": "exchange"
  },
  "totalAddressCount": 209394,
  "revision": 0
}
```

A single address can be provided for the “address” parameter.

LTC Wallet By Wallet Id

This query returns wallet information for a specified wallet id.

https://rest.ciphertrace.com/api/v1/ltc_wallet/?wallet_id=002ddcc3

This returns a Wallet Response. For example, the above query returns:

```
{
  "walletId": "002ddcc3",
  "owner": {
    "name": "Kraken.com",
    "subpoenable": true,
    "url": "https://www.kraken.com",
    "country": "US",
    "type": "exchange"
  },
  "totalAddressCount": 209394,
  "revision": 0
}
```

A single wallet id can be provided for the “wallet_id” parameter. If the wallet state has changed the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id which has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

LTC Wallet Addresses

This query returns wallet addresses for a specified wallet id.

https://rest.ciphertrace.com/api/v1/ltc_wallet/addresses?wallet_id=002ddcc3&count=100&offset=100

This returns a Wallet Response with addresses included. For example, the above query returns:

```
{
  "addressOffset": 0,
  "walletId": "002ddcc3",
  "revision": 0,
  "walletIdChanged": false,
  "owner": {
    "name": "Kraken.com",
    "subpoenable": true,
    "url": "https://www.kraken.com",
    "country": "US",
    "type": "exchange"
  },
  "totalAddressCount": 209394,
  "addresses": [
    "LLMQrWWkNBy2Q1rtpuvKNNZXxzphPXFfvV",
    "LSUgaiHycDuALdBdzVAB4D77R396mUPMo3",
    "LL9X5GF4C5xBTwaCuSbzEizWuvxNC98J5q",
    "LeSdLNPdWPSJ6ZVjXH4dvKtk4c7edut1ER",
    "LdRftC3oK3RjnrLGKaiTPW7KHFTytXM2mZ",
    ...
  ]
}
```

A single wallet id can be provided for the “wallet_id” parameter. A starting address offset is provided with the “offset” parameter. The count parameter must be between 1 and 10000.

Offset and count are used to page through the address list. For example, if your first query is offset=100 and count=1000, then your next query would be offset=1100 and count=1000 (or whatever count value you prefer).

If the wallet state has changed, the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id that has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

LTC Transaction History for Address

This query returns a list of transactions that have included a specified address within a date range.

https://rest.ciphertrace.com/api/v1/ltc_tx/search?address=MJRSgZ3UUFcTBTBAaN38XAXvZLwRe8WVw7

In this query, the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range

searched is inclusive of the starting and ending date. As an example, the above query returns the following JSON:

```
{
  "address": "MJRSgZ3UUFcTBTBAaN38XAXvZLwRe8WVw7",
  "startDate": 0,
  "endDate": 1913732049,
  "transactions": [
    "6560188e641999b05ce0f10b4fc0c0703f6d7b107dfd5b0914c8a778e410336b",
    "d76157133bcc3f4b300511d4bd82e3ce7962cc853aca3fcc0d45c4325e2fdf10",
    "f354585871aacc128f7a27b179fd0bed4807dafbc640b2b5719035222bf2d0d",
    ...
  ]
}
```

Details for LTC transaction list

This query returns details on a specified list of transaction hashes (maximum of 10 hashes) as well as attribution data for all addresses used in the transactions.

https://rest.ciphertrace.com/api/v1/ltc_tx?txhashes=A58F941AEE0AAA32B8123452D2717CA532DB63DB54A786BE365CAB0F29922023,28A301ABFE1F1CD72DF36020FCC34D09AFE024A2CF67A987837498F656ECA01

The txhashes parameter specifies an array of comma separated transactions hashes to search on (no white space allowed). Please limit the query to a maximum of 10 transactions at present.

NOTE: This query has been updated to include an ipHistory map which details any IP address matches for all transaction and address hashes included in the response. Only hashes that have IP Information are included in the map.

The above query returns the following JSON:

```
{
  "transactions": [
    {
      "txHash": "A58F941AEE0AAA32B8123452D2717CA532DB63DB54A786BE365CAB0F29922023",
      "outputs": [
        {
          "pos": 0,
          "address": "LcdMyJY6TJiopCkEE44bSCDEP6or2UUbJd",
          "value": 0.47439948
        },
        ...
        {
          "pos": 6,
          "address": "LhyLNfBkoKshT7R8Pce6vkb9T2cP2o84hx",
          "value": 48.94904913
        }
      ]
    },
    "total": 60.13341973,
    "inputs": [
      {
        "pos": 0,
        "address": "LNgs6vGiG4de5nssV29CQLi28jeJiSLHe5",
        "value": 32.3935363
      },
      ...
    ]
  ]
}
```

```

    {
      "pos": 50,
      "address": "LNtA2kZnX7cwnzFXfnaMTLGcCyjyepmcA",
      "value": 3.41281029
    }
  ],
  "date": 1518653907,
  "fee": 0.05072998
},
{
  "txHash": "28A301ABFE1F1CD72DF36020FCC34D09AFE024A2CF67A987837498F656ECO0A01",
  "outputs": [
    {
      "pos": 0,
      "address": "Lcp1dUUeYpNctkqGh8GKPLDms6hqKmxnwy",
      "value": 1.99
    },
    ...
    {
      "pos": 16,
      "address": "LhyLNfBkoKshT7R8Pce6vkB9T2cP2o84hx",
      "value": 10.0452332
    }
  ],
  "total": 85.84806672,
  "inputs": [
    {
      "pos": 0,
      "address": "LMBBDPvxQBhTPNxQPfqbMutfBGsiUxJRUn",
      "value": 85.85201447
    }
  ],
  "date": 1517347032,
  "fee": 0.00394775
}
],
"addresses": {
  "LQMUfjgFfkiqAKoN6Rz7T7xiGmGeGr23w7": {
    "wallet": {
      "walletId": "004b4184",
      "owner": {
        "name": "Bittrex.com",
        "subpoenable": true,
        "url": "https://bittrex.com",
        "country": "US",
        "type": "exchange"
      }
    },
    "totalAddressCount": 416075,
    "revision": 0
  }
},
  "LRpNnkAqX7sb7pWmscHu4pJw6L1GjhtCKT": {
    "wallet": {
      "walletId": "004b4184",
      "owner": {
        "name": "Bittrex.com",
        "subpoenable": true,
        "url": "https://bittrex.com",
        "country": "US",
        "type": "exchange"
      }
    },
    "totalAddressCount": 416075,
    "revision": 0
  }
}
},

```

```

    ...
  },
  "ipHistory": {}
}

```

LTC Address Search

This query returns all information regarding an Address. Current balance information as well as (optional) balance history with transaction hashes and IP Address match history.

https://rest.ciphertrace.com/api/v1/ltc_address/search?features=tx,ip&address=LPHsPRmK81eR2UJ5AHp9n82bSHGsrzZwHP

In this query the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. Features is also an optional parameter that details which type of optional information the requester wishes (as a comma separated list). "tx" requests a transaction history within the date range. "ip" requests IP Information within the date range.

As an example, the above query returns the following JSON:

```

{
  "lastUsedBlockHeight": 1376686,
  "querySpent": 0.46167006,
  "queryEndingBalance": 0.0,
  "endDate": 1913732049,
  "totalSpendCount": 2,
  "totalSpent": 0.46167006,
  "totalDepositCount": 2,
  "queryDeposits": 0.46167006,
  "currentBalance": 0.0,
  "queryDepositCount": 2,
  "ipHistory": [],
  "querySpendCount": 2,
  "address": "LPHsPRmK81eR2UJ5AHp9n82bSHGsrzZwHP",
  "txHistory": [
    {
      "txHash": "28a301abfe1f1cd72df36020fcc34d09afe024a2cf67a987837498f656ec0a01",
      "txIndex": 20458836,
      "balance": 0.29426917,
      "date": 1517347032,
      "received": 0.29426917,
      "spent": 0.0
    },
    {
      "txHash": "a58f941aee0aaa32b8123452d2717ca532db63db54a786be365cab0f29922023",
      "txIndex": 21219299,
      "balance": 0.46167006,
      "date": 1518653907,
      "received": 0.16740089,
      "spent": 0.0
    },
    {
      "txHash": "48aa5eda0c56b94f5bf342a2b38a91f8813811a60bab392d2e88e99f16c3927a",
      "txIndex": 21442022,
      "balance": 0.16740089,
      "date": 1518970432,
      "received": 0.0,
      "spent": 0.29426917
    },
    {

```

```
    "txHash": "4bdee3cc6c30c95f090d7a46b3600c9ddee6f76e5be210936e1a8049dc38eefd",
    "txIndex": 21904272,
    "balance": 0.0,
    "date": 1519811452,
    "received": 0.0,
    "spent": 0.16740089
  }
},
"inCase": true,
"startDate": 0,
"wallet": {
  "walletId": "00d77a29",
  "owner": {
    "name": "KuCoin",
    "subpoenable": false,
    "url": "https://www.kucoin.com/#/",
    "country": "CN",
    "type": "exchange"
  },
  "totalAddressCount": 192445,
  "revision": 0
},
"totalDeposits": 0.46167006
}
```

ETH Queries

Ethereum queries are very similar to the BTC set with some minor differences in response structure due to the differences in the currencies themselves. The request URLs generally map the BTC URL's with an eth_ prefix after the API version.

ETH Wallet By Address

This query returns wallet information for a specified Ethereum address.

https://rest.ciphertrace.com/api/v1/eth_wallet?address=0x8d12a197cb00d4747a1fe03395095ce2a5cc6819

This returns a Wallet Response. For example, the above query returns:

```
{
  "walletId": "0x8d12a197cb00d4747a1fe03395095ce2a5cc6819",
  "owner": {
    "name": "EtherDelta",
    "subpoenable": false,
    "url": "http://etherdelta.com",
    "country": "US",
    "type": "exchange"
  },
  "totalAddressCount": 1,
  "revision": 0
}
```

A single address can be provided for the “address” parameter.

ETH Wallet By Wallet Id

This query returns wallet information for a specified wallet id.

https://rest.ciphertrace.com/api/v1/eth_wallet?wallet_id=0x8d12a197cb00d4747a1fe03395095ce2a5cc6819

This returns a Wallet Response. For example, the above query returns:

```
{
  "walletId": "0x8d12a197cb00d4747a1fe03395095ce2a5cc6819",
  "owner": {
    "name": "EtherDelta",
    "subpoenable": false,
    "url": "http://etherdelta.com",
    "country": "US",
    "type": "exchange"
  },
  "totalAddressCount": 1,
  "revision": 0
}
```

A single wallet id can be provided for the “wallet_id” parameter. If the wallet state has changed the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id which has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

ETH Wallet Addresses

This query returns wallet addresses for a specified wallet id.

https://rest.ciphertrace.com/api/v1/eth_wallet/addresses?wallet_id=0x8d12a197cb00d4747a1fe03395095ce2a5cc6819&count=100&offset=0

This returns a Wallet Response with addresses included. For example, the above query returns:

```
{
  "addressOffset": 0,
  "walletId": "0x8d12a197cb00d4747a1fe03395095ce2a5cc6819",
  "revision": 0,
  "walletIdChanged": false,
  "owner": {
    "name": "EtherDelta",
    "subpoenable": false,
    "url": "http://etherdelta.com",
    "country": "US",
    "type": "exchange"
  },
  "totalAddressCount": 1,
  "addresses": [
    "0x8d12a197cb00d4747a1fe03395095ce2a5cc6819"
  ]
}
```

A single wallet id can be provided for the “wallet_id” parameter. A starting address offset is provided with the “offset” parameter. The count parameter must be between 1 and 10000.

Offset and count are used to page through the address list. For example, if your first query is offset=100 and count=1000, then your next query would be offset=1100 and count=1000 (or whatever count value you prefer).

If the wallet state has changed, the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id that has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

ETH Transaction History for Address

This query returns a list of transactions that have included a specified address within a date range.

https://rest.ciphertrace.com/api/v1/eth_tx/search?address=0x37f5b1dcf6649a3ea6888f745e618ce996dc313b&startdate=1470000000&enddate=1477550206&offset=0&limit=10000

In this query, the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. The default limit is 1000 transactions per page. As an example, the above query returns the following JSON:

```

{
  "address": "0x37f5b1dcf6649a3ea6888f745e618ce996dc313b",
  "startDate": 1470000000,
  "endDate": 1477550206,
  "transactions": [
    "0x3d35360d536a4b2f0ebb99bd68d54b4a14f2fc9c47d5639f43ad76b1656a300c",
    "0xba0005b953a61b0733baa026c8665c0b132392ac1e6935924016eaac72ccef49",
    "0x228ed7644b96b4e80861db8971f08c4b59bac151e09d562eadb201f42659e5ed",
    "0x289de8a1b28b73f07b76f651d3f35ad084b2c61c9226a29bb16027cbe170339a",
    "0x52562b5678cae1b5e9fd28c964613450dea84570b8e68e5c3db6d43c7cf0fcba",
    "0xbc6f3e826c0983a5277d269acdca76061444cebd210fa45046c374f7709cf48c",
    "0xd95f1fb4924be74b4a36f4ff7111dc84253e4c2d0b5bbbf5a1d67a0f468894c2",
    "0xf5f453acfd9a203054b23d936efee0d0fb93b364ccd0879bd5df4c194c8e0356"
  ]
}

```

Details for ETH transaction list

This query returns details on a specified list of transaction hashes (maximum of 10 hashes) as well as attribution data for all addresses used in the transactions.

https://rest.ciphertrace.com/api/v1/eth_tx?txhashes=0x3d35360d536a4b2f0ebb99bd68d54b4a14f2fc9c47d5639f43ad76b1656a300c,0xba0005b953a61b0733baa026c8665c0b132392ac1e6935924016eaac72ccef49

The txhashes parameter specifies an array of comma separated transactions hashes to search on (no white space allowed). Please limit the query to a maximum of 10 transactions at present.

The above query returns the following JSON:

```

{
  "transactions": [
    {
      "txType": 1,
      "children": [],
      "txHash": "0x3d35360d536a4b2f0ebb99bd68d54b4a14f2fc9c47d5639f43ad76b1656a300c",
      "nonce": 47,
      "toAddress": "0x209c4784ab1e8183cf58ca33cb740efbf3fc18ef",
      "fromAddressBalance": 0.000699419263702382,
      "gasPrice": 20000000000,
      "date": 1477550206,
      "fromAddress": "0x37f5b1dcf6649a3ea6888f745e618ce996dc313b",
      "blockHeight": 2515807,
      "gasLimit": 40000,
      "value": 35.09901917,
      "gasUsed": 30376,
      "toAddressBalance": 0
    },
    {
      "txType": 1,
      "children": [],
      "txHash": "0xba0005b953a61b0733baa026c8665c0b132392ac1e6935924016eaac72ccef49",
      "nonce": 46,
      "toAddress": "0xbfc39b6f805a9e40e77291aff27aee3c96915bdd",
      "fromAddressBalance": 0.000326109263702382,
      "gasPrice": 30000000000,
      "date": 1473654476,
      "fromAddress": "0x37f5b1dcf6649a3ea6888f745e618ce996dc313b",
      "blockHeight": 2243718,
      "gasLimit": 40000,
      "value": 21.04919043,
    }
  ]
}

```

```

        "gasUsed": 29130,
        "toAddressBalance": 0
    }
  ],
  "addresses": {
    "0xbfc39b6f805a9e40e77291aff27aee3c96915bdd": {
      "wallet": {
        "walletId": "N/A",
        "owner": {},
        "revision": 0
      }
    },
    "0x37f5b1dcf6649a3ea6888f745e618ce996dc313b": {
      "wallet": {
        "walletId": "N/A",
        "owner": {},
        "revision": 0
      }
    },
    "0x209c4784able8183cf58ca33cb740efbf3fc18ef": {
      "wallet": {
        "walletId": "N/A",
        "owner": {},
        "revision": 0
      }
    }
  },
  "ipHistory": {}
}

```

ETH Address Search

This query returns all information regarding an Address. Current balance information as well as (optional) balance history with transaction hashes and IP Address match history.

https://rest.ciphertrace.com/api/v1/eth_address/search?features=tx,ip&address=0x37f5b1dcf6649a3ea6888f745e618ce996dc313b&startdate=0&enddate=1440178493&offset=0&limit=10000

In this query the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. The default limit is 1000 transactions per page

As an example, the above query returns the following JSON:

```

{
  "address": "0x37f5b1dcf6649a3ea6888f745e618ce996dc313b",
  "currentBalance": 0.000699419263702382,
  "endDate": 1440178493,
  "inCase": true,
  "ipHistory": [],
  "lastUsedBlockHeight": 2515807,
  "queryDepositCount": 1,
  "queryDeposits": 0.25,
  "queryEndingBalance": 0,
  "querySpendCount": 1,
  "querySpent": 0.24895,
  "startDate": 0,
  "totalDepositCount": 0,
  "totalDeposits": 14958.15,
  "totalSpendCount": 47,
  "totalSpent": 14958.11072059,
}

```

```

"txHistory": [
  {
    "txHash": "0x5441f4df0806c6070a1955318c3709dc3409d41c4fcb873a04764eb7cf081bae",
    "txIndex": 38608,
    "balance": 0.25,
    "date": 1440178183,
    "received": 0.25,
    "spent": 0
  },
  {
    "txHash": "0xda77b0e030e5d9c20f671bc2c072b773a1fc59cdf15b5caee59cca6390e52bb3",
    "txIndex": 38616,
    "balance": 0,
    "date": 1440178493,
    "received": 0,
    "spent": 0.24895
  }
],
"wallet": {
  "walletId": "0x37f5b1dcf6649a3ea6888f745e618ce996dc313b",
  "owner": {},
  "totalAddressCount": 1,
  "revision": 0
}
}

```

BNB Queries

BNB (Binance Network) queries differ from both Ethereum and Bitcoin in that each send transaction is made up of one or more asset types with each asset type in a transaction having a set of inputs and a set of outputs. Because of this, all addresses will have separate balances and summaries for each asset they hold or have transacted with. Each transaction also contains a set of data for each asset as well as an indicator for what asset was used to pay the transaction fee.

BNB Wallet By Address

This query returns wallet information for a specified BNB address.

https://rest.ciphertrace.com/api/v1/bnb_wallet/?address=bnb12wpk84anfltnwj9l7l9xazur4u70yxmdyj8glk

This returns a Wallet Response. For example, the above query returns:

```

{
  "walletId": "bnb12wpk84anfltnwj9l7l9xazur4u70yxmdyj8glk",
  "owner": {
    "name": "AtomicWallet",
    "subpoenable": false,
    "url": "https://atomicwallet.io/",
    "country": "UN",
    "type": "wallet"
  },
  "totalAddressCount": 1,
  "revision": 0
}

```

A single address can be provided for the “address” parameter.

BNB Wallet By Wallet Id

This query returns wallet information for a specified wallet id.

https://rest.ciphertrace.com/api/v1/bnb_wallet/?wallet_id=bnb1f69utnu7stm6kd84j0d7y2520hjq3ak8khczj

This returns a Wallet Response. For example, the above query returns:

```
{
  "walletId": "bnb1f69utnu7stm6kd84j0d7y2520hjq3ak8khczj",
  "owner": {
    "name": "Binance.com",
    "subpoenable": false,
    "url": "https://www.binance.com",
    "country": "HK",
    "type": "exchange"
  },
  "totalAddressCount": 1,
  "revision": 0
}
```

A single wallet id can be provided for the “wallet_id” parameter. If the wallet state has changed the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id which has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

BNB Wallet Addresses

This query returns wallet addresses for a specified wallet id.

https://rest.ciphertrace.com/api/v1/bnb_wallet/addresses?wallet_id=bnb12wpk84anfltnwj9l7l9xazur4u70yxmdyj8glk&count=100

This returns a Wallet Response with addresses included. For example, the above query returns:

```
{
  "addressOffset": 0,
  "walletId": "bnb12wpk84anfltnwj9l7l9xazur4u70yxmdyj8glk",
  "revision": 0,
  "walletIdChanged": false,
  "owner": {
    "name": "AtomicWallet",
    "subpoenable": false,
    "url": "https://atomicwallet.io/",
    "country": "UN",
    "type": "wallet"
  },
  "totalAddressCount": 1,
  "addresses": [
    "bnb12wpk84anfltnwj9l7l9xazur4u70yxmdyj8glk"
  ]
}
```

A single wallet id can be provided for the “wallet_id” parameter. A starting address offset is provided with the “offset” parameter. The count parameter must be between 1 and 10000.

Offset and count are used to page through the address list. For example, if your first query is offset=100 and count=1000, then your next query would be offset=1100 and count=1000 (or whatever count value you prefer).

If the wallet state has changed, the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id that has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

BNB Transaction History for Address

This query returns a list of transactions that have included a specified address within a date range.

https://rest.ciphertrace.com/api/v1/bnb_tx/search?address=bnb1000exsx2fy58zve825nerr6v605m6v626yd2yp&limit=10&offset=0&startdate=1546329600&enddate=1572897821

In this query, the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. The default limit is 1000 transactions per page. As an example, the above query returns the following JSON:

```
{
  "address": "bnb1000exsx2fy58zve825nerr6v605m6v626yd2yp",
  "startDate": 1546329600,
  "endDate": 1572897821,
  "transactions": [
    "19E05304C0327959ADD4D270B589454EC7580179080C26ACCAEE80D10B43C5B0",
    "D5ED106A1ED9BA237166BB0886A1504B7FBF738BBFA6DF6429F70D8A6790D138",
    "43AE6D7129A84A89BD63F67773A4BA5414793ACB2094E2F3D33495E0D88E94A8",
    "7CE11B99D6463FEAD025797D08A734C02B265158745D95D3DCBC41B4E991034D",
    "57BB2B21E9F4AA0DC8E4FDF833F4A9423112470BA8EC99A0A6BC294E853E3BC7",
    "2BD1F6B22A2FF345070C953D8B6B8944FFC230DBAE60568386E3425104B56514"
  ]
}
```

Details for BNB transaction list

This query returns details on a specified list of transaction hashes (maximum of 10 hashes) as well as attribution data for all addresses used in the transactions.

https://rest.ciphertrace.com/api/v1/bnb_tx?txhashes=2F82A60CCBBFE74ED74A357A9453A8056959E51DFD8EF9F0581A9ACDA3B56E5F,19E05304C0327959ADD4D270B589454EC7580179080C26ACCAEE80D10B43C5B0&includedetails=1

The txhashes parameter specifies an array of comma separated transactions hashes to search on (no white space allowed). Please limit the query to a maximum of 10 transactions at present. The includedetails parameter controls if related address information should be included as well

The above query returns the following JSON:

```
{
  "transactions": [
    {
      "txHash": "19E05304C0327959ADD4D270B589454EC7580179080C26ACCAEE80D10B43C5B0",
      "items": [
        {
          "asset": "NEW-09E",
          "total": 5.0,
          "inputs": [
            {
              "address": "bnb12cvjxjrqw6lz092pvzsealsrl7g90pkx25n7mc",
              "value": 5.0
            }
          ],
          "outputs": [
            {
              "address": "bnb1000exsx2fy58zve825nerr6v605m6v626yd2yp",
              "value": 5.0
            }
          ]
        }
      ],
      "feeAsset": "BNB",
      "date": 1566568400,
      "fee": 0.000375
    },
    {
      "txHash": "2F82A60CCBBFE74ED74A357A9453A8056959E51DFD8EF9F0581A9ACDA3B56E5F",
      "items": [
        {
          "asset": "BNB",
          "total": 1.5,
          "inputs": [
            {
              "address": "bnb12wpk84anfltnwj9l7l9xazur4u70yxmdyj8g1k",
              "value": 1.5
            }
          ],
          "outputs": [
            {
              "address": "bnb119whj8d4vjwt6jwkj6h260eu5xr6lkt067zhumu",
              "value": 1.5
            }
          ]
        }
      ],
      "feeAsset": "BNB",
      "date": 1572634618,
      "fee": 0.000375
    }
  ],
  "addresses": {
    "bnb12cvjxjrqw6lz092pvzsealsrl7g90pkx25n7mc": {
      "wallet": {
        "walletId": "bnb12cvjxjrqw6lz092pvzsealsrl7g90pkx25n7mc",
        "owner": {},
        "totalAddressCount": 1,
        "revision": 0
      }
    },
    "bnb1000exsx2fy58zve825nerr6v605m6v626yd2yp": {
      "wallet": {
        "walletId": "bnb1000exsx2fy58zve825nerr6v605m6v626yd2yp",

```



```

    "type": "exchange"
  },
  "totalAddressCount": 1,
  "revision": 0
}
"summary": [
  {
    "lastUsedBlockHeight": 45438035,
    "totalSpendCount": 5,
    "totalSpent": 591.80310239,
    "totalDepositCount": 12,
    "locked": 0.0,
    "currentBalance": 1474.65939761,
    "frozen": 0.0,
    "asset": "ARN-71B",
    "free": 1474.65939761,
    "totalDeposits": 2061.4625
  },
  {
    "lastUsedBlockHeight": 45438035,
    "totalSpendCount": 11,
    "totalSpent": 33.84093502,
    "totalDepositCount": 17,
    "locked": 0.0,
    "currentBalance": 26.39711677,
    "frozen": 0.0,
    "asset": "BNB",
    "free": 26.39711677,
    "totalDeposits": 60.28105858
  }
],
"querySummary": [
  {
    "lastUsedBlockHeight": 0,
    "totalSpendCount": 5,
    "totalSpent": 591.80310239,
    "totalDepositCount": 12,
    "locked": 0.0,
    "currentBalance": 0.0,
    "frozen": 0.0,
    "asset": "ARN-71B",
    "free": 0.0,
    "totalDeposits": 2061.4625
  },
  {
    "lastUsedBlockHeight": 0,
    "totalSpendCount": 11,
    "totalSpent": 33.84093502,
    "totalDepositCount": 17,
    "locked": 0.0,
    "currentBalance": 0.0,
    "frozen": 0.0,
    "asset": "BNB",
    "free": 0.0,
    "totalDeposits": 60.28105858
  }
],
"txHistory": [
  {
    "txHash": "2F82A60CCBBFE74ED74A357A9453A8056959E51DFD8EF9F0581A9ACDA3B56E5F",
    "balance": 26.39711677,
    "date": 1572634618,
    "asset": "BNB",
    "received": 1.5,
    "spent": 0.0
  }
]

```

```

    },
    {
      "txHash": "E1DF991E3E0AB027037DBBA9A944941383EA7CF76D7EFBB61E43F876E07312A2",
      "balance": 1474.65939761,
      "date": 1571298620,
      "asset": "ARN-71B",
      "received": 0.1,
      "spent": 0.0
    },
    {
      "txHash": "2F6B25D8A1CE84FB69D22E8A89E3B49BFD34E75AD728C5B7F09B54A727A98647",
      "balance": 24.58376677,
      "date": 1570967694,
      "asset": "BNB",
      "received": 0.0,
      "spent": 1.0431
    },
    {
      "txHash": "252B60709B093BC9834DCF2A3072FF0D5E22ED3C3467227AFC50AE7BBA061FFD",
      "balance": 1.0,
      "date": 1565615693,
      "asset": "BNB",
      "received": 1.0,
      "spent": 0.0
    }
  ]
}

```

RSK Queries

RSK queries are very similar to the ETH set with the major difference being that addresses are considered a part of a transaction if they are involved in a contract call that was a part of that transaction (token transfer, internal transfer, etc)

RSK Wallet By Address

This query returns wallet information for a specified Rootstock address.

https://rest.ciphertrace.com/api/v1/rsk_wallet?address=0x0d391f1a15bac22afa8db1ad4b009e6c68ec11ca

This returns a Wallet Response. For example, the above query returns:

```

{
  "walletId": "0x0d391f1a15bac22afa8db1ad4b009e6c68ec11ca",
  "owner": {
    "name": "HuobiGlobal",
    "subpoenable": false,
    "url": "https://www.hbg.com/en-us/",
    "country": "SG",
    "type": "exchange"
  },
  "totalAddressCount": 1,
  "revision": 0
}

```

A single address can be provided for the “address” parameter.

RSK Wallet By Wallet Id

This query returns wallet information for a specified wallet id.

https://rest.ciphertrace.com/api/v1/rsk_wallet?wallet_id=0xffac89640a75adb6184bdae717eb3e03c78566c4

This returns a Wallet Response. For example, the above query returns:

```
{
  "walletId": "0xffac89640a75adb6184bdae717eb3e03c78566c4",
  "owner": {
    "name": "CoinAll",
    "subpoenable": false,
    "url": "https://www.coinall.com",
    "country": "MT",
    "type": "exchange"
  },
  "totalAddressCount": 1,
  "revision": 0
}
```

A single wallet id can be provided as the “wallet_id” parameter. If the wallet state has changed the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id which has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

RSK Wallet Addresses

This query returns wallet addresses for a specified wallet id.

https://rest.ciphertrace.com/api/v1/rsk_wallet/addresses?wallet_id=0xffac89640a75adb6184bdae717eb3e03c78566c4&count=100&offset=100

This returns a Wallet Response with addresses included. For example, the above query returns:

```
{
  "addressOffset": 100,
  "walletId": "0xffac89640a75adb6184bdae717eb3e03c78566c4",
  "revision": 0,
  "walletIdChanged": false,
  "owner": {
    "name": "CoinAll",
    "subpoenable": false,
    "url": "https://www.coinall.com",
    "country": "MT",
    "type": "exchange"
  },
  "totalAddressCount": 1,
  "addresses": [
    "0xffac89640a75adb6184bdae717eb3e03c78566c4"
  ]
}
```

A single wallet id can be provided for the “wallet_id” parameter. A starting address offset is provided with the “offset” parameter. The count parameter must be between 1 and 10000.

Offset and count are used to page through the address list. For example, if your first query is offset=100 and count=100, then your next query would be offset=200 and count=100 (or whatever count value you prefer).

If the wallet state has changed, the revision field will be incremented. In this case if the client is tracking addresses, they should proceed to re-retrieve the entire address list.

Similarly, if the provided wallet id is an older id that has been merged with other wallets, the new walletId will be returned and the optional walletIdChanged will be provided with a value of true.

RSK Transaction History for Address

This query returns a list of transactions that have included a specified address within a date range. An address is considered included if it is the sender, receiver, or involved in contract execution or token transfer.

https://rest.ciphertrace.com/api/v1/rsk_tx/search?address=0xfe05ee3d651670f807db7dd56e1e0fcba29b234a&startdate=1514833200&enddate=1584041822&offset=0&limit=10000

In this query, the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. The default limit is 1000 transactions per page. As an example, the above query returns the following JSON:

```
{
  "address": "0xfe05ee3d651670f807db7dd56e1e0fcba29b234a",
  "startDate": 1514833200,
  "endDate": 1584041822,
  "transactions": [
    "0x9aa7c3dfb871868fd7991be659f3551ec07c2262f0f829b9c27a5c700ce6a267",
    "0xf184ec863b79ecb8613468421074cc580c9317e8fa4e0c4dec08610bb25d93b0",
    "0xf4247f0ac6a67edac9f7908565c176600319caa67bd7dc6b28016f49f0f68b6e ",
    "0x8a66d77feef86d729817e6ee6051c51ecae096cfeaf59a9dc132bc711ea2f5aa ",
    "0xa7157b44eece715d2e7a154ef7dbe64dc59832722a936c43648ec0e58347610b ",
    "0xe6a7001dde57ffd8be1c40fc5c61a6802f303d9848b9c6546f0f44d8dd9d5ab4",
    "0x83ca60a53fccd70507169d82dac1004ab42c5098bf8cd68675142b37dfd82696",
    "0x1a1eca8160e292e9a3092cf5cf7dde16e7e8cc22becd960b56094018e73cc299"
  ]
}
```

Details for RSK transaction list

This query returns details on a specified list of transaction hashes (maximum of 10 hashes) as well as attribution data for all addresses used in the transactions.

https://rest.ciphertrace.com/api/v1/rsk_tx?txhashes=0x9f97f9cf73dc477f9034ed533fb98bb7d6e314774dcac67ba96d711e7a66b2c0,0xb1ebc3069ee382b19eb355eb82a3dfa25411e6bbf9df0169d41b2efa20081b3e

The txhashes parameter specifies an array of comma separated transaction hashes to search on (no white space allowed). Please limit the query to a maximum of 10 transactions at present.


```

    "date": 1565144250,
    "fromAddress": "0x3f9abbd4e51332c197352771782286573588d7cd",
    "blockHeight": 1606418,
    "gasLimit": 250000,
    "value": 0.000018,
    "gasUsed": 21000
  }
],
"addresses": {
  "0x3f9abbd4e51332c197352771782286573588d7cd": {
    "wallet": {
      "walletId": "0x3f9abbd4e51332c197352771782286573588d7cd",
      "owner": {},
      "totalAddressCount": 1,
      "revision": 0
    }
  },
  "0xe4aa0f414725c9322a1a9d80d469c5e234786653": {
    "wallet": {
      "walletId": "0xe4aa0f414725c9322a1a9d80d469c5e234786653",
      "owner": {},
      "totalAddressCount": 1,
      "revision": 0
    }
  },
  "0xe700691da7b9851f2f35f8b8182c69c53ccad9db": {
    "wallet": {
      "walletId": "0xe700691da7b9851f2f35f8b8182c69c53ccad9db",
      "owner": {},
      "totalAddressCount": 1,
      "revision": 0
    }
  },
  "0x2c272443010f13509df3bbc55e0e74435d56fd56": {
    "wallet": {
      "walletId": "0x2c272443010f13509df3bbc55e0e74435d56fd56",
      "owner": {},
      "totalAddressCount": 1,
      "revision": 0
    }
  },
  "0x6921ea54320fd8f6999a1b68ae8f2dda9340f4a7": {
    "wallet": {
      "walletId": "0x6921ea54320fd8f6999a1b68ae8f2dda9340f4a7",
      "owner": {},
      "totalAddressCount": 1,
      "revision": 0
    }
  },
  "0x9d11937e2179dc5270aa86a3f8143232d6da0e69": {
    "wallet": {
      "walletId": "0x9d11937e2179dc5270aa86a3f8143232d6da0e69",
      "owner": {},
      "totalAddressCount": 1,
      "revision": 0
    }
  }
}
}

```

RSK Address Search

This query returns all information regarding an Address. Current balance information as well as (optional) balance history with transaction hashes.

https://rest.ciphertrace.com/api/v1/rsk_address/search?features=tx&address=0x821afc1b371bb546f03be9d959ab0240d44836f9&startdate=1591712927&enddate=1591810131&offset=0&limit=10000

In this query the address parameter specifies the address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. The default limit is 1000 transactions per page. As an example, the above query returns the following JSON:

```
{
  "endDate": 1591810131,
  "address": "0x821afc1b371bb546f03be9d959ab0240d44836f9",
  "txHistory": [
    {
      "txHash": "0x8aa785af0a4bd67737df65e2c26a0ade61389dda59241656258f5849607d9a6f",
      "balance": 0.217312123630729376,
      "messageIndex": 0,
      "date": 1591809481,
      "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
      "received": 0.0,
      "spent": 0
    },
    {
      "txHash": "0x0d913d73785753f45b52874e6ef7fa0cd197bdc55ec4c74e259a55853e6076f7",
      "balance": 0.21732440597431598,
      "messageIndex": 0,
      "date": 1591805474,
      "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
      "received": 0.0,
      "spent": 0
    },
    {
      "txHash": "0xba7e81c45489f2c188c25581d62959b2f67212d7e5dd93d4b3a6feaa748ed4c7",
      "balance": 0.217336812381760271,
      "messageIndex": 0,
      "date": 1591801938,
      "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
      "received": 0.0,
      "spent": 0
    },
    {
      "txHash": "0x2ca9dcb734825888d32364a5ab206c39a163d51bdb1187b44720d640a66ddf00",
      "balance": 0.217349218788680997,
      "messageIndex": 0,
      "date": 1591798230,
      "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
      "received": 0.0,
      "spent": 0
    },
    {
      "txHash": "0x5b3943f7d68681becc588bfad52d111deb3bd81be4379d69b5e50c1584ec02a",
      "balance": 0.217361625195915862,
      "messageIndex": 0,
      "date": 1591794366,
      "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
      "received": 0.0,
      "spent": 0
    }
  ]
}
```

```

},
{
  "txHash": "0x8d7ae007e2f3d3561ee04ff15c69c8c0f2f6e4adaeae47e395e0b764c97e5240",
  "balance": 0.217374031603464866,
  "messageIndex": 0,
  "date": 1591790775,
  "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
  "received": 0.0,
  "spent": 0
},
{
  "txHash": "0xd7ac78eca5044486302f50513de09810967c8824040b65fe39223a7a9f7e2e99",
  "balance": 0.217386438010909157,
  "messageIndex": 0,
  "date": 1591786889,
  "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
  "received": 0.0,
  "spent": 0
},
{
  "txHash": "0x112639523c210f5ba10141ade9b7ab2bba27c9d41495cd85c5de56060bc50af1",
  "balance": 0.21739859753064942,
  "messageIndex": 0,
  "date": 1591782631,
  "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
  "received": 0.0,
  "spent": 0
},
{
  "txHash": "0x084a0a624ae91987d980ac01153f41ab92550ebcd9b05c49a9af467275e18b63",
  "balance": 0.217410879873921885,
  "messageIndex": 0,
  "date": 1591779134,
  "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
  "received": 0.0,
  "spent": 0
},
{
  "txHash": "0x713c0eded64145010a08606ff17c974b70cca5adc2e71e4a8443ab72a2374b0e",
  "balance": 0.21742328628115675,
  "messageIndex": 0,
  "date": 1591775261,
  "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
  "received": 0.0,
  "spent": 0
},
{
  "txHash": "0x0f960720966b241b73262f6de6d9140e968ff27b69928f6993aa6c6dfe8ee339",
  "balance": 0.217435692688601041,
  "messageIndex": 0,
  "date": 1591771086,
  "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
  "received": 0.0,
  "spent": 0
},
{
  "txHash": "0x2811778b47f9342e425ed61ec2e8eada9aee9eb3b2f72fcf3f4de58ba26cc07b",
  "balance": 0.217448099095521767,
  "messageIndex": 0,
  "date": 1591767426,
  "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
  "received": 0.0,
  "spent": 0
},
{

```

```

"txHash": "0xd6f50db1d3e22a77976c2750c8159015ffbbdf2ff2d93356dc636ec21269ab54",
"balance": 0.217460505502442493,
"messageIndex": 0,
"date": 1591763515,
"contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
"received": 0.0,
"spent": 0
},
{
"txHash": "0xc0c068d331468e1d35374b866fe9b12983eca57b2e5fe4ddf280e2558ae9ffad",
"balance": 0.217472911909886784,
"messageIndex": 0,
"date": 1591759709,
"contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
"received": 0.0,
"spent": 0
},
{
"txHash": "0x61d1af6cdfc6c21fde0f13fb31ce9b8a269b819f65f682353c8aaf56b8cc6ca1",
"balance": 0.217485318316912223,
"messageIndex": 0,
"date": 1591756217,
"contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
"received": 0.0,
"spent": 0
},
{
"txHash": "0xad5a9b453d418dcc745d7160ba7d969ee5572d4534b82de9bd534c9dfa4493d6",
"balance": 0.217497724724251801,
"messageIndex": 0,
"date": 1591752786,
"contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
"received": 0.0,
"spent": 0
},
{
"txHash": "0xf5485ee35d8b18e5b542a7348139b715317639a67ccb9c86765d041672ff85f6",
"balance": 0.217510131131696092,
"messageIndex": 0,
"date": 1591749053,
"contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
"received": 0.0,
"spent": 0
},
{
"txHash": "0x7e8756afc3751e8b09023c21e31e628087ba2effc0f793e351c8959cd32b732f",
"balance": 0.217524272213661154,
"messageIndex": 0,
"date": 1591745453,
"contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
"received": 0.0,
"spent": 0
},
{
"txHash": "0x6b8b91f6901f4da15695a722a07fda84f332f41e7b8afad123f50f4a648a9ca6",
"balance": 0.217536523825041454,
"messageIndex": 0,
"date": 1591741830,
"contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
"received": 0.0,
"spent": 0
},
{
"txHash": "0x52d14fd5e83ed32f0d553fb761b7f6c9e4456e235f0f1585d30245866a6ddfb0",
"balance": 0.21754889919059326,

```

```

    "messageIndex": 0,
    "date": 1591738022,
    "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
    "received": 0.0,
    "spent": 0
  },
  {
    "txHash": "0x4a07efadd52ca4a6d3ef29cb136c4991092d55636ca6f20929eeaa0850d6fd9a",
    "balance": 0.217561273318296265,
    "messageIndex": 0,
    "date": 1591734284,
    "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
    "received": 0.0,
    "spent": 0
  },
  {
    "txHash": "0x3dafaf5546c69b7df67b2050d19c002324eed68a01dee6aaa033c7c96bb21853",
    "balance": 0.217573523705301943,
    "messageIndex": 0,
    "date": 1591730551,
    "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
    "received": 0.0,
    "spent": 0
  },
  {
    "txHash": "0x3f3a66d3b236d0798244eb62ab78dc4e0577b1d7711d867084aa28f1b48cf5da",
    "balance": 0.217587216035729463,
    "messageIndex": 0,
    "date": 1591726943,
    "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
    "received": 0.0,
    "spent": 0
  },
  {
    "txHash": "0x08eb492ef01fa35bea6fe5a4f57c0f665f94101db1dd1ee30180c8969caa9cc0",
    "balance": 0.217599591400863465,
    "messageIndex": 0,
    "date": 1591723506,
    "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
    "received": 0.0,
    "spent": 0
  },
  {
    "txHash": "0x084dfef018b6c92345449469f9377217ae5405e21aeb5ba4d26bc647d753472e",
    "balance": 0.217611841787869143,
    "messageIndex": 0,
    "date": 1591719794,
    "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
    "received": 0.0,
    "spent": 0
  },
  {
    "txHash": "0xfe8a361bb96edcf7c20071918be95acf3b60c9c006d432198fa0440ef5d8b204",
    "balance": 0.2176242171535254,
    "messageIndex": 0,
    "date": 1591715983,
    "contractAddress": "0xd89fd1010c9b3b0cafc3fb51ee661d89e256d8ef",
    "received": 0.0,
    "spent": 0
  }
],
"inCase": false,
"startDate": 1591712927,
"wallet": {
  "walletId": "0x821afc1b371bb546f03be9d959ab0240d44836f9",

```

```

    "owner": {},
    "totalAddressCount": 1,
    "revision": 0
  },
  "summary": {
    "lastUsedBlockHeight": 2431706,
    "totalSpendCount": 1216,
    "totalSpent": 0,
    "totalDepositCount": 0,
    "currentBalance": 0.217312123630729376,
    "totalDeposits": 0
  }
}

```

IP Queries

Information on crypto assets associated with IP addresses can be retrieved using the IP query endpoint. The endpoint uses two data structures, IP Result and Address Match.

IP Result

This structure details an IP address and the associated crypto assets

Field	Type	Description
ip	String	IP address
records	Array[Address Match]	The set of matching crypto asset addresses.
country	Optional String	Country in which this IP is located
city	Optional String	City location of this IP
latitude	Optional Double	Latitude of this IP
longitude	Optional Double	Longitude of this IP
nextOffset	Int	Offset value that should be used to get the next page of results. -1 indicates no further results.
startDate	Int	The lower bound timestamp filter applied to the query.
endDate	Int	The upper bound timestamp filter applied to the query.

Address Match

This structure details an IP address and the associated crypto address

Field	Type	Description
address	String	Crypto address
addressType	String	Crypto address type (BTC, BCH)
firstSeen	Int	First timestamp this IP was associated with this crypto address.
lastSeen	Int	Most recent timestamp this IP was associated with this crypto address
risk	Optional AddressRisks Info	Risks associated with this address
balance	Double	The current balance of this crypto address
walletId	String	CipherTrace Wallet Identifier
entity	Optional Owner	Owner data structure
country	Optional String	Country code of associated owner if known

IP Address Search

This query returns all information regarding an IP Address. Geo information as well as all associated crypto addresses.

<https://rest.ciphertrace.com/api/v1/ip/search?address=182.253.14.193&limit=5&offset=0&startdate=1451665358&enddate=1704126158>

In this example request the address parameter specifies the ip address to search on. startdate and enddate are optional fields which limit the date range searched (values are in Unix epoch time). The date range searched is inclusive of the starting and ending date. The default limit is 100 addresses per page. Limit and offset are used to paginate through the results

As an example, the above query returns the following JSON:

```
{
  "city": "Bandung",
  "ip": "182.253.14.193",
  "endDate": 1549764527,
  "latitude": -6.9217000007629395,
  "country": "ID",
  "longitude": 107.60710144042969,
  "nextOffset": 5,
  "records": [
    {
      "lastSeen": 1549359083,
      "walletId": "1d18aed7",
      "risk": {
        "callbackSeconds": 86400,
        "risk": 1.0,
        "sanctionsRisk": 1.0,
        "gamblingOkRisk": 1.0,
        "address": "17heHDg362VGEiZA57XBmwTLuhdvXVjJ21",
        "updatedToBlock": 597584
      },
      "balance": 0.0,
      "firstSeen": 1549359083,
      "addressType": "BTC",
      "entity": {
        "type": "unknown",
        "name": "unknown"
      },
      "address": "17heHDg362VGEiZA57XBmwTLuhdvXVjJ21"
    },
    {
      "lastSeen": 1549359083,
      "walletId": "0c20eaf8",
      "risk": {
        "callbackSeconds": 86400,
        "risk": 1.0,
        "sanctionsRisk": 1.0,
        "gamblingOkRisk": 1.0,
        "address": "17jGidyv49AwsxF54b7fxjhn6tpvcJFBZS",
        "updatedToBlock": 597584
      },
      "balance": 0.0,
      "firstSeen": 1549359083,
      "addressType": "BTC",
      "entity": {
        "type": "unknown",
        "name": "unknown"
      },
      "address": "17jGidyv49AwsxF54b7fxjhn6tpvcJFBZS"
    },
    ...
  ],
  "startDate": 1549359083
}
```

AML Risk Scoring API

The CipherTrace Risk Scoring API allows customers to test addresses and transactions for risk in order to comply with anti-money laundering requirements.

The API allows you to specify the currency and either an address or a transaction hash.

Risk Scores

CipherTrace determines risk for an address 3 ways:

1. Direct attribution data related to that address
2. Based on the risk of the addresses directly interacting with the address (1 hop)
3. Based on the risk of the addresses directly interacting with an address that the address under evaluation has been directly interacting with (2 hops)

Notes:

A transaction is the receiving or sending of value between 2 addresses.

We currently classify risk for a target address by looking at its direct attribution and at transactions that are one hop away and two hops away. A “hop” is one portion of the path between the source and destination. If Susan sends money to Bob, that transaction is “one hop away” from Susan. If Susan sends money to Bob and Bob sends money to Fred, then the Bob-Fred transaction is “two hops” away from Susan.

Risk classification levels are:

Risk Score	Description
0	No attribution exists for this address or the address has no transactions.
1	No known transactions with any level 9 or 10 addresses within one hop. Note that if this is a new address for which CipherTrace is still in the process of calculating its risk classification, the address will show up as a “1” until the updated risk classification is made. (in this situation, the updated risk classification should appear within a few hours).
2	This address is controlled by a trusted exchange that has not been labelled ‘High Risk Exchange’ and that has transacted with level 9 or 10 addresses one or more times within one hop.
4	This address has transacted with a level 9 address once within one hop. Does not propagate further.
5	This address has transacted with a level 10 address once within one hop. Does not propagate further.

8	This address has transacted with level 9 addresses two or more times, or with a level 10 address once and level 9 addresses one or more times, within one hop. Does not propagate further.
9	This address has transacted with level 10 addresses two or more times within one hop.
10	Attribution data exists for this address that attributes it to a sanctioned entity or labels it as Criminal, Dark Market, Gambling, Malware, Ransomware, or Mixer. (When using the gamblingOkRisk parameter in the API, gambling is whitelisted.)

Criminal type activities are:

- Money laundering mixers, tumblers, foggers
- Stolen coins
- Ransomware or malware
- Gambling sites and Ponzi Schemes
- Dark markets

In the current version of the API all values will be whole numbers, although the return value is a floating-point number allowing expansion of subcategories in future versions.

Call Back

The callback allows the API to return data quickly back to the caller, but requests that the caller make another call in **call_back_seconds** seconds in order to possibly get more information about the transaction or address. This may be used when querying an address or transaction with thousands or even hundreds of thousands of related addresses or transactions that must be queried in order to generate a risk score.

Bitcoin Risk Scoring API

Transaction Risk Score Info

This structure details information gathered when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the transaction.

risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted
txhash	String	Transaction hash supplied for the given query
addressRisks	Map of address to addressRisks	Details address information within the searched transaction (all inputs and outputs)
updatedToBlock	Int	Our current block height

The following fields are present for the Ethereum network only

Field	Type	Description
timestamp	Int	Time stamp of the risk calculation

AddressRisks Info

This structure details information gathered for each address when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the address.
outputValue	Int	Value of the given output, or zero if the address is an input.

inputValue	Int	Value of the given input, or zero if the address is an output.
address	String	Bitcoin address
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted

This query returns a risk score for a transaction. The risk score is the highest risk score of all the addresses, both input and output, for the transaction. The addressRisks object is a mapping of each address in the transaction. These will include details on the input and output values as well as individual risk scores per address. Per query, we research all addresses for you instead of having you individually query them. Each address will also return a callbackSeconds. Below are some examples.

<https://rest.ciphertrace.com/aml/v1/btc/risk?txhash=49315ba6b8ffbd16d68b2fdcd75fa52beddec2a2a325569ebaccb698068c3250>

```
{
  "callbackSeconds": 86400,
  "risk": 10,
  "sanctionsRisk": 1,
  "gamblingOkRisk": 10,
  "txhash": "49315ba6b8ffbd16d68b2fdcd75fa52beddec2a2a325569ebaccb698068c3250",
  "addressRisks": {
    "14cN2pTimACRJ4dqitFLuhtrmKQL6xxAoY": {
      "outputValue": 0.022,
      "callbackSeconds": 86400,
      "risk": 10,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 10,
      "address": "14cN2pTimACRJ4dqitFLuhtrmKQL6xxAoY",
      "inputValue": 0
    },
    "1NSBWAZgiByeyHuNw19NnBtbyLDarj5naF": {
      "outputValue": 0.002434,
      "callbackSeconds": 86400,
      "risk": 4,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 4,
      "address": "1NSBWAZgiByeyHuNw19NnBtbyLDarj5naF",
      "inputValue": 0
    },
    "1K6fKeSpKCfnEMGzmxsdWmw3YExLgXAqyi": {
      "outputValue": 0,
      "callbackSeconds": 86400,
      "risk": 5,
      "sanctionsRisk": 1,

```

```

        "gamblingOkRisk": 5,
        "address": "1K6fKeSpKCfnEMGzmxsdWmw3YExLgXAqyi",
        "inputValue": 0.025562
    }
},
"updatedToBlock": 568908
}

```

<https://rest.ciphertrace.com/aml/v1/btc/risk?txhash=4c97b52c13b6a42ed949d57d0b4e88bbee13e591c14f123de615799b34b8abc5>

```

{
  "callBackSeconds": 86400,
  "risk": 4,
  "sanctionsRisk": 1,
  "gamblingOkRisk": 4,
  "txhash": "4c97b52c13b6a42ed949d57d0b4e88bbee13e591c14f123de615799b34b8abc5",
  "addressRisks": {
    "16c9L88NBAQiqySKjkwpnAc97HAY2qK5x2": {
      "outputValue": 0,
      "callBackSeconds": 86400,
      "risk": 1,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 1,
      "address": "16c9L88NBAQiqySKjkwpnAc97HAY2qK5x2",
      "inputValue": 0.21558796
    },
    "17MxK2QaNWqo4kVKdkPjL55UTpAtfmQBmp": {
      "outputValue": 0.02838796,
      "callBackSeconds": 86400,
      "risk": 1,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 1,
      "address": "17MxK2QaNWqo4kVKdkPjL55UTpAtfmQBmp",
      "inputValue": 0
    },
    "1GMU7qLotnVlytirt9qcdqAFzgZoHpoDcZ": {
      "outputValue": 0.00234029,
      "callBackSeconds": 86400,
      "risk": 1,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 1,
      "address": "1GMU7qLotnVlytirt9qcdqAFzgZoHpoDcZ",
      "inputValue": 0
    },
    "12ZLAeRJ6P2Wcx4PerEgo4tJxN6KiJdoaQ": {
      "outputValue": 0.1872,
      "callBackSeconds": 86400,
      "risk": 1,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 1,
      "address": "12ZLAeRJ6P2Wcx4PerEgo4tJxN6KiJdoaQ",
      "inputValue": 0
    },
    "1EbpEqxyobP4kXy3p2tPLybWd63LVTmbX": {
      "outputValue": 0.00234029,
      "callBackSeconds": 86400,
      "risk": 1,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 1,
      "address": "1EbpEqxyobP4kXy3p2tPLybWd63LVTmbX",
      "inputValue": 0
    }
  }
}

```

```

    },
    "1GeTxbEJUguDYNb7EtXkwrtVH1wCndjA6f": {
      "outputValue": 0.00234029,
      "callbackSeconds": 86400,
      "risk": 1,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 1,
      "address": "1GeTxbEJUguDYNb7EtXkwrtVH1wCndjA6f",
      "inputValue": 0
    },
    "1NESvXTRKUdghesh7Z22qYHoJqpnWukd64": {
      "outputValue": 0,
      "callbackSeconds": 86400,
      "risk": 1,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 1,
      "address": "1NESvXTRKUdghesh7Z22qYHoJqpnWukd64",
      "inputValue": 0.00966075
    },
    "13uTmsHSZENT54WTnExHheg3yPaq8K25Ta": {
      "outputValue": 0.00233988,
      "callbackSeconds": 86400,
      "risk": 4,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 4,
      "address": "13uTmsHSZENT54WTnExHheg3yPaq8K25Ta",
      "inputValue": 0
    }
  },
  "updatedToBlock": 568908
}

```

Address Risk Score Info

This structure details information gathered for when performing a deep research on a given address to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the address.
address	String	Bitcoin address
risk	Int	Default CipherTrace risk score given to this address

sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted
updatedToBlock	Int	Our current block height

This query returns a risk score for a specified address.

<https://rest.ciphertrace.com/aml/v1/btc/risk?address=1DoZNZyDZV6RAgqZvbXbf8ESiyD59gWJwE>

```
{
  "callBackSeconds": 86400,
  "risk": 10,
  "sanctionsRisk": 1,
  "gamblingOkRisk": 10,
  "address": "1DoZNZyDZV6RAgqZvbXbf8ESiyD59gWJwE",
  "updatedToBlock": 568908
}
```

Ethereum Risk Scoring API

The Ethereum Risk Scoring API is modeled after the Bitcoin version, however there are some different data structures to be aware of. We have outlined the following data structures for our Ethereum Risk Scoring API responses.

ETH Transaction Risk Score Info

This structure details information gathered when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the transaction.
risk	Double	Default CipherTrace risk score given to this address
sanctionsRisk	Double	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Double	Same as default risk, except that gambling is whitelisted
txhash	String	Transaction hash supplied for the given query
addressRisks	Map of address to ETHAddressRisk	Details address information within the searched transaction (all addresses)
updatedToBlock	Int	Our current block height

ETH Address Risk Info

This structure details information gathered for each address when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the address.

address	String	Ethereum address
risk	Double	Default CipherTrace risk score given to this address
sanctionsRisk	Double	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Double	Same as default risk, except that gambling is whitelisted
updateToBlock	Int	Our current block height
balance	Long	Balance as of transaction

ETH Address Risks Map Info

This structure details information gathered for each address when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
address	String	Ethereum address
inputValue	String	Value in Wei of the given input, or zero if the address is the from address.
outputValue	String	Value in Wei of the given output, or zero if the address is the to address.
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the address.
risk	Double	Default CipherTrace risk score given to this address
sanctionsRisk	Double	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Double	Same as default risk, except that gambling is whitelisted

balance	String	The current balance of the address, represented in Wei
---------	--------	--

This query returns a risk score for a transaction. Each address will return a callbackSeconds for further research as well as contain the address's risk score. If the address was in the "from" field, then it is the input for the transaction thus, inputValue will contain a value that is represented in Wei (Ether's lowest denomination). If the address was in the "to" field, then the outputValue will contain the value.

<https://rest.ciphertrace.com/aml/v1/eth/risk?txhash=0xb49dacefcf067c4f2a9b885442b6f8753a8fc7b78c2563ca70b8576eb34159a>

```
{
  "callbackSeconds": 86400,
  "timestamp": 1538536805,
  "risk": 1,
  "sanctionsRisk": 1,
  "gamblingOkRisk": 1,
  "txhash": "0xb49dacefcf067c4f2a9b885442b6f8753a8fc7b78c2563ca70b8576eb34159a",
  "addressRisks": {
    "0x0795106c86d78ae929760bce4d3182f3a667acce": {
      "outputValue": "0",
      "callbackSeconds": 86400,
      "risk": 1,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 1,
      "address": "0x0795106c86d78ae929760bce4d3182f3a667acce",
      "inputValue": "4413700000000000000000"
    },
    "0x339aca055908d787fe300deb49db67f271fdd242": {
      "outputValue": "4413700000000000000000",
      "callbackSeconds": 86400,
      "risk": 1,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 1,
      "address": "0x339aca055908d787fe300deb49db67f271fdd242",
      "inputValue": "0"
    }
  },
  "gasLimit": "21000",
  "updatedToBlock": 7448044
}
```

<https://rest.ciphertrace.com/aml/v1/eth/risk?address=0x5fe87e186d8019e9ecea20e8106c6271a031fdc9>

The query to return a risk score for an address is below. This will return the current balance of the address (represented in Wei – the lowest denomination of Ether) as well as the callbackSeconds similar to the previous AML queries.

```
{
  "callbackSeconds": 86400,
  "risk": 5,
  "balance": "19400000000",
  "sanctionsRisk": 5,
  "gamblingOkRisk": 5,
  "address": "0x5fe87e186d8019e9ecea20e8106c6271a031fdc9",
  "updatedToBlock": 7448043
}
```

Bitcoin Cash Risk Scoring API

The Bitcoin Cash risk scoring API should be structurally identical to the BTC Risk Scoring API.

Transaction Risk Score Info

This structure details information gathered when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callBackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the transaction.
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted
txhash	String	Transaction hash supplied for the given query
addressRisks	Map of address to addressRisks	Details address information within the searched transaction (all inputs and outputs)
updatedToBlock	Int	Our current block height

Bitcoin Cash Address Risks Info

This structure details information gathered for each address when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callBackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the address.

outputValue	Int	Value of the given output, or zero if the address is an input.
inputValue	Int	Value of the given input, or zero if the address is an output.
address	String	BitcoinCash address
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted

This query returns a risk score for a transaction. The risk score is the highest risk score of all the addresses, both input and output, for the transaction. The addressRisks object is a mapping of each address in the transaction. These will include details on the input and output values as well as individual risk scores per address. Per query, we research all addresses for you instead of having you individually query them. Each address will also return a callbackSeconds. Example below.

<https://rest.ciphertrace.com/aml/v1/bch/risk?txhash=7f9a91d12c7eeaab9023d989dbb631e64d3272d942562dd5eb79798a19915903>

```
{
  "callbackSeconds": 86400,
  "risk": 9.0,
  "sanctionsRisk": 1.0,
  "gamblingOkRisk": 9.0,
  "txhash": "7f9a91d12c7eeaab9023d989dbb631e64d3272d942562dd5eb79798a19915903",
  "addressRisks": {
    "qpqpd0cxn5jgl78x9uznx14yx5h6xevz5heqmfant": {
      "outputValue": 0.0,
      "callbackSeconds": 86400,
      "risk": 1.0,
      "sanctionsRisk": 1.0,
      "gamblingOkRisk": 1.0,
      "address": "qpqpd0cxn5jgl78x9uznx14yx5h6xevz5heqmfant",
      "inputValue": 4.0
    },
    "qqvqptrmtnap48hk2m25n3wng9g5lryxs36ftpl9a": {
      "outputValue": 0.0,
      "callbackSeconds": 86400,
      "risk": 1.0,
      "sanctionsRisk": 1.0,
      "gamblingOkRisk": 1.0,
      "address": "qqvqptrmtnap48hk2m25n3wng9g5lryxs36ftpl9a",
      "inputValue": 0.04191527
    },
    ...
  },
  "updatedToBlock": 605714
}
```

}

Address Risk Score Info

This structure details information gathered for when performing a deep research on a given address to return a risk score.

Field	Type	Description
callBackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the address.
address	String	BitcoinCash address
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted
updatedToBlock	Int	Our current block height

This query returns a risk score for a specified address.

<https://rest.ciphertrace.com/aml/v1/bch/risk?address=qrlfsgth5nq6sx0478q5pum12g5d65rcsv5h35yc5n>

```
{
  "callBackSeconds": 86400,
  "risk": 1.0,
  "sanctionsRisk": 1.0,
  "gamblingOkRisk": 1.0,
  "address": "qrlfsgth5nq6sx0478q5pum12g5d65rcsv5h35yc5n",
  "updatedToBlock": 605714
}
```

Litecoin Risk Scoring API

The Litecoin risk scoring API should be structurally identical to the BTC Risk Scoring API.

Transaction Risk Score Info

This structure details information gathered when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the transaction.
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted
txhash	String	Transaction hash supplied for the given query
addressRisks	Map of address to addressRisks	Details address information within the searched transaction (all inputs and outputs)
updatedToBlock	Int	Our current block height

Litecoin Address Risks Info

This structure details information gathered for each address when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the address.

outputValue	Int	Value of the given output, or zero if the address is an input.
inputValue	Int	Value of the given input, or zero if the address is an output.
address	String	Litecoin address
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted

This query returns a risk score for a transaction. The risk score is the highest risk score of all the addresses, both input and output, for the transaction. The addressRisks object is a mapping of each address in the transaction. These will include details on the input and output values as well as individual risk scores per address. Per query, we research all addresses for you instead of having you individually query them. Each address will also return a callbackSeconds. Example below.

<https://rest.ciphertrace.com/aml/v1/ltc/risk?txhash=eca234a041edaef3bfd353fdf99d5b2fb54bccab9837a7aade8038cfdd404fe>

```
{
  "callbackSeconds": 86400,
  "risk": 10.0,
  "sanctionsRisk": 8.0,
  "gamblingOkRisk": 8.0,
  "txhash": "eca234a041edaef3bfd353fdf99d5b2fb54bccab9837a7aade8038cfdd404fe",
  "addressRisks": {
    "LPEgGLVaXZz7632SUrBJKybiHyBR9MNSXQ": {
      "outputValue": 0.0,
      "callbackSeconds": 86400,
      "risk": 8.0,
      "sanctionsRisk": 8.0,
      "gamblingOkRisk": 8.0,
      "address": "LPEgGLVaXZz7632SUrBJKybiHyBR9MNSXQ",
      "inputValue": 0.0331319
    },
    "ltc1q25ajd0w2dh3yeqwrft2usnfzn4f8yzt0t5mny": {
      "outputValue": 0.00029783,
      "callbackSeconds": 86400,
      "risk": 1.0,
      "sanctionsRisk": 1.0,
      "gamblingOkRisk": 1.0,
      "address": "ltc1q25ajd0w2dh3yeqwrft2usnfzn4f8yzt0t5mny",
      "inputValue": 0.0
    },
    "MNciG9DNPbiJvGGHYVGqfPYPnYmX8K8vcz": {
      "outputValue": 0.03261243,

```

```

    "callbackSeconds": 86400,
    "risk": 10.0,
    "sanctionsRisk": 1.0,
    "gamblingOkRisk": 1.0,
    "address": "MNciG9DNPbiJvGGHYVGqfPYPnYmX8K8vcz",
    "inputValue": 0.0
  }
},
"updatedToBlock": 1723771
}

```

Address Risk Score Info

This structure details information gathered for when performing a deep research on a given address to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the address.
address	String	Litecoin address
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted
updatedToBlock	Int	Our current block height

This query returns a risk score for a specified address.

<https://rest.ciphertrace.com/aml/v1/ltc/risk?address=MNciG9DNPbiJvGGHYVGqfPYPnYmX8K8vcz>

```

{
  "callbackSeconds": 86400,
  "risk": 10.0,
  "sanctionsRisk": 1.0,
  "gamblingOkRisk": 1.0,
  "address": "MNciG9DNPbiJvGGHYVGqfPYPnYmX8K8vcz",
  "updatedToBlock": 1723771
}

```

Binance Chain Risk Scoring API

The BNB risk scoring API is similar to the BTC risk scoring API except in the structure of the transaction risk details. Because a single BNB transaction can involve multiple asset types, the per address contributing values are grouped by asset.

Transaction Risk Score Info

This structure details information gathered when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the transaction.
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted
txhash	String	Transaction hash supplied for the given query
addressRisks	Map of address to addressRisks	Details address information within the searched transaction (all inputs and outputs)
updatedToBlock	Int	Our current block height

BNB Address Risks Info

This structure details information gathered for each address when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly

		get more information about the address.
assetValues	Map of assets to input and output values	Input and Output values for a given asset for this address
inputValue	Int	Value of the given input, or zero if the address is an output.
address	String	BNB address
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted

This query returns a risk score for a transaction. The risk score is the highest risk score of all the addresses, both input and output, for the transaction. The addressRisks object is a mapping of each address in the transaction. These will include details on the input and output values as well as individual risk scores per address. Per query, we research all addresses for you instead of having you individually query them. Each address will also return a callbackSeconds. Example below.

<https://rest.ciphertrace.com/aml/v1/bnb/risk?txhash=D5ED106A1ED9BA237166BB0886A1504B7FBF738BBFA6DF6429F70D8A6790D138>

```
{
  "callbackSeconds": 0,
  "risk": 1.0,
  "sanctionsRisk": 1.0,
  "gamblingOkRisk": 1.0,
  "txhash": "D5ED106A1ED9BA237166BB0886A1504B7FBF738BBFA6DF6429F70D8A6790D138",
  "addressRisks": {
    "bnb1000exsx2fy58zve825nerr6v605m6v626yd2yp": {
      "callbackSeconds": 0,
      "risk": 1.0,
      "sanctionsRisk": 1.0,
      "gamblingOkRisk": 1.0,
      "address": "bnb1000exsx2fy58zve825nerr6v605m6v626yd2yp",
      "assetValues": {
        "BNB": {
          "input": 0.0925,
          "output": 0.0
        }
      }
    },
    "bnb1ze53x0drn746w887mkqz4z43dpkjqrh3t3q8kc": {
      "callbackSeconds": 0,
      "risk": 1.0,

```

```

    "sanctionsRisk": 1.0,
    "gamblingOkRisk": 1.0,
    "address": "bnb1ze53x0drn746w887mkqz4z43dpkjqrh3t3q8kc",
    "assetValues": {
      "BNB": {
        "input": 0.0,
        "output": 0.0925
      }
    }
  },
  "updatedToBlock": 46143347
}

```

Address Risk Score Info

This structure details information gathered for when performing a deep research on a given address to return a risk score.

Field	Type	Description
callBackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the address.
address	String	BNB address
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted
updatedToBlock	Int	Our current block height

This query returns a risk score for a specified address.

<https://rest.ciphertrace.com/aml/v1/bnb/risk?address=bnb1I9whj8d4vjlw6jwkj6h260eu5xr6lkt067zhumu>

```

{
  "callBackSeconds": 0,
  "risk": 1.0,
  "sanctionsRisk": 1.0,
  "gamblingOkRisk": 1.0,
  "address": "bnb1I9whj8d4vjlw6jwkj6h260eu5xr6lkt067zhumu",
  "updatedToBlock": 46143578
}

```

RSK Risk Scoring API

The RSK risk scoring API is similar to the BTC risk scoring API except in the structure of the transaction risk details.

Transaction Risk Score Info

This structure details information gathered when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the transaction.
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted
txhash	String	Transaction hash supplied for the given query
addressRisks	Map of address to addressRisks	Details address information within the searched transaction (all inputs and outputs)
updatedToBlock	Int	Our current block height

RSK Address Risks Info

This structure details information gathered for each address when performing a deep research on a given transaction to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount in seconds until caller should ask again to possibly get more information about the address.

inputValue	Int	Value of the given input, or zero if the address is an output.
address	String	RSK address
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted

This query returns a risk score for a transaction. The risk score is the highest risk score of all the addresses, both input and output, for the transaction. The addressRisks object is a mapping of each address in the transaction. These will include details on the input and output values as well as individual risk scores per address. Per query, we research all addresses for you instead of having you individually query them. Each address will also return a callbackSeconds. Example below.

<https://rest.ciphertrace.com/aml/v1/rsk/risk?txhash=0x6db2bdf4e3f0a1d4c1ab68a007af24407efa19e0430b95444f1408ad32c25988>

```
{
  "callbackSeconds": 86400,
  "timestamp": 1591631431,
  "risk": 1.0,
  "sanctionsRisk": 1.0,
  "gamblingOkRisk": 1.0,
  "txhash": "0x6db2bdf4e3f0a1d4c1ab68a007af24407efa19e0430b95444f1408ad32c25988",
  "addressRisks": {
    "0x1af42dc99974d68024cb876d4591311f6a82dbe0": {
      "outputValue": 0,
      "callbackSeconds": 86400,
      "risk": 1.0,
      "sanctionsRisk": 1.0,
      "gamblingOkRisk": 1.0,
      "address": "0x1af42dc99974d68024cb876d4591311f6a82dbe0",
      "inputValue": 0
    },
    "0xe700691da7b9851f2f35f8b8182c69c53ccad9db": {
      "outputValue": 0,
      "callbackSeconds": 86400,
      "risk": 1.0,
      "sanctionsRisk": 1.0,
      "gamblingOkRisk": 1.0,
      "address": "0xe700691da7b9851f2f35f8b8182c69c53ccad9db",
      "inputValue": 0
    },
    "0xf1d5c9a337d78dfe63b4f6c5f52de2487cdb4b35": {
      "outputValue": 0,
      "callbackSeconds": 86400,
      "risk": 1.0,
      "sanctionsRisk": 1.0,

```

```

    "gamblingOkRisk": 1.0,
    "address": "0xf1d5c9a337d78dfe63b4f6c5f52de2487cdb4b35",
    "inputValue": 0
  }
},
"updatedToBlock": 2431619
}

```

Address Risk Score Info

This structure details information gathered for when performing a deep research on a given address to return a risk score.

Field	Type	Description
callbackSeconds	Int	Amount of time in seconds until the caller should ask again to possibly get more information about the address.
address	String	RSK address
risk	Int	Default CipherTrace risk score given to this address
sanctionsRisk	Int	Risk score that's based entirely on interaction with sanctioned entities
gamblingOkRisk	Int	Same as default risk, except that gambling is whitelisted
updatedToBlock	Int	Our current block height

This query returns a risk score for a specified address.

<https://rest.ciphertrace.com/aml/v1/rsk/risk?address=0x821afc1b371bb546f03be9d959ab0240d44836f9>

```

{
  "callbackSeconds": 86400,
  "risk": 1.0,
  "balance": 0.217312123630729376,
  "sanctionsRisk": 1.0,
  "gamblingOkRisk": 1.0,
  "address": "0x821afc1b371bb546f03be9d959ab0240d44836f9",
  "updatedToBlock": 2431714
}

```


curl -X GET <https://rest.ciphertrace.com/v1/alerting/subscriptions/me/btc>

Clear the entire watch list

To clear all entries from the watch list (full unsubscribe) use DELETE on the base subscription URL:

curl -X DELETE <https://rest.ciphertrace.com/v1/alerting/subscriptions/me/btc>

Several times a day alerts will be sent out via email for all changed addresses on users' watch lists. If there is a new transaction or changed risk score the alert will trigger.

Currently, there is no way to subscribe or unsubscribe from email alerts in the Inspector UI. However besides the API, every email includes links to unsubscribe from the specific alert address or all addresses.

Updating User Preference for Webhook and Email Delivery

To update the alerting preferences POST to the following URL with the following JSON data structure:

curl -X POST <https://rest.ciphertrace.com/v1/alerting/users/me/preferences>

```
{
  "webhookURL": "https://myurl.com:9021/hook?foo=var",
  "webhookEnabled": true,
  "emailEnabled": false
}
```

Please make sure to set the usual HTTP headers (user key in Authorization, Content-Type: application/json) .

Field	Type	Description
webhookURL	String	URL to deliver alerts to
webhookEnabled	Boolean	Webhook alerts enabled. Set to true to deliver webhook alerts
emailEnabled	Boolean	Email alerts enabled. Set to false to not receive emails

NOTE: Webhooks are delivered in a best effort way with no retries. Since the webhook caller cannot be authenticated, the receiving system should always use API callbacks to verify any webhook data.

Receiving Webhook notifications

When the webhookEnabled flag is set to true and a webhookURL is configured in the user preferences, CipherTrace will attempt to make 1 HTTP POST call to the specified URL whenever an alert is triggered on a configured address. The body of the message will look like to this example:

```
{
  "currency": "BTC",
  "address": "1Hn9ErTCPRP6j5UDBeuXPGuq5RtRjFJxJQ",
  "newRisk": true,
  "newTransaction": true
}
```

The content-type in the header will be application/json. The following table describes the fields that will be passed in the body of the HTTP call.

Field	Type	Description
currency	String	Chain that generated the alert; Currently only "BTC" is supported
address	String	Crypto currency address for which the alert was triggered
newRisk	Boolean	Boolean indicating that the risk classification changed
newTransaction	Boolean	Boolean indicating that there was a new transaction

Since webhook alerts cannot be authenticated, the receiving system should only use the webhook content as an indicator and use API callbacks to CipherTrace to check the addresses new risk or transactions.

Furthermore, CipherTrace advises that the customer's alert management system keeps a list of configured addresses and regularly (once a day, once a week, a few times a week) checks the current status of those addresses in case alert webhooks were missed due to intermittent network or other issues.

API FAQs (Frequently Asked Questions)

The following are some frequently asked questions. If you have any questions not addressed by this section, please contact support@ciphertrace.com -- we're here to help!

Wallet Address Queries

What do you mean by count and offset in regard to the Wallet Addresses Query?

Count is the number of addresses to return in the addresses list for that wallet. The count parameter must be between 1 and 10000. Both the count and offset are used to index through the addresses list. If the totalAddressCount for a wallet is 20,000, then you could proceed with first doing a query with count=10000 and offset=0. The following query could be count=10000 and offset=10000. Thus, you will have now indexed through the addresses list.

What does it mean if I receive the message "404 Not Found - getAddressWallet: error address=<Crypto Address> not found" while performing an Address specific API call?

The 404 response is the expected behavior for the "Wallet by Address" API call, when the address has never been used on the blockchain before. The reason for this response is that the address does not exist on the blockchain (or in the mempool, for currencies where we support it) and has no attribution, including Unknown, as it has not yet been added to our dataset or had the clustering attribution added in our system yet.

When you receive this response we recommend performing a callback after the transaction is added to the blockchain, which will often be within ten minutes, but may take much longer.

On currencies with mempool support, you may wish to monitor the blockchain for those transactions and addresses to leave the mempool before querying for the address, or use the "Address Search" API call that includes the mempool flag that enables the inclusion of transactions that are still in mempool and will also provide the address' Entity Name and Entity Type data.

Ethereum

How do you gather information on an Ethereum address's balance?

When performing a risk score query for a given Ethereum address, we will return the address's current balance. The balance will be represented in Wei which is the lowest denomination of Ether. 1 Ether = 10^{18} Wei.

Risk Scoring/Classification

Using Risk Classification and Attribution for AML/Transaction Monitoring

There are three main factors that can be taken into account when designing a system to flag, accept, or reject a transaction based on risk: Risk Classification, Entity Type, and Entity.

One way to determine whether to flag, accept, or reject a transaction is to look at the address' parent entity type (who the address belongs to). By using this information as a guide, you can choose to flag, accept, or reject a transaction that is attributable to one or more specific *entity types*.

As described earlier, there is some flexibility in defining a "high risk entity" in the risk classification system:

- By default, CipherTrace automatically classifies these entity types as "high risk entity types" (therefore earning an automatic risk classification of 10): Criminal, Dark Market, Gambling, HYIP, malware-associated, mixer, or ransomware-associated.
- If you don't want to block gambling entities, but want to block all other "10s" you can utilize the gamblingOkRisk score.
- OFAC sanctioned entities and addresses will have a 'sanctionsRisk' score 10 in the Sentry AML API and will have the following notation in Inspector "THIS IS A SANCTIONED ADDRESS OR ENTITY." So if you are only looking to identify direct transactions with OFAC sanctioned entities, you can utilize the sanctionsRisk score. You can also utilize the sanctionsRisk score to identify transactions with addresses that are one hop away from a sanctioned entity address.

However, your organization may have different standards that would be served by using entity types instead. For example, you may decide you want to automatically approve any transaction that doesn't belong to an identified "Criminal". If your policy is to allow interactions with mixers, you can "turn off" the mixer flag.

By using the entity type returned by the API, you can design a system to do so by simply ignoring the risk classification returned and using the entity type instead.

You may decide you only want to reject or accept transactions going to or from addresses associated with specific entities (an internal "blacklist"). For example, perhaps your organization generally allows transactions with gambling entities, but knows that "CryptoCasino" as been an AML risk in the past, in which case your system can use the "name" field to block.

Finally, you may wish to block or allow transactions coming to or from a specific country, such as to exchanges domiciled in Iran (ISO 3166-2: IR). By using the "country" field, you can block only those countries.

If you are unsure which method(s) would work best for you, contact support@ciphertrace.com. They can walk you through some examples of current clients and use cases that have implemented different systems.

Can you please explain the callBackSeconds in the AML Risk Scoring API?

The callBackSeconds in the AML Risk Scoring API delivers the number of seconds until we will have completed deep research on that transaction and addresses. During deep research, we may find interactions with addresses that have higher risk scores which could alter the given risk score of the address/transaction that you are searching on. The initial query on an address or transaction will show you immediate results. Subsequent requests will display a callBackSeconds of 604800. Most of our deep research will complete sooner than the callback amount, yet in order to be certain in the updates we specify the given seconds.

Attribution

What are all the Attributed entity types that you support?

ATM: A business who operates physical kiosks that allow a person to purchase Bitcoin by using cash or debit card. Some Bitcoin ATMs offer bi-directional functionality enabling both the purchase of Bitcoin as well as the sale of Bitcoin for cash. In some cases, Bitcoin ATM providers require users to have an existing account to transact on the machine. There are two main types of Bitcoin machines: cash kiosks and ATMs. Both types are connected to the Internet, allowing for cash or debit card payment, respectively, in exchange for bitcoins given as a paper receipt or by moving money to a public key on the blockchain. Bitcoin cash kiosks look like traditional ATMs, but do not connect to a bank account and instead connect the user directly to a Bitcoin exchange. Bitcoin-enabled ATMs are traditional ATMs and connect to a bank account to allow for a cashless purchase of bitcoin.

Criminal: An entity associated with a known crime. Criminals can be pseudonymous, such as in the case of crypto-thefts, or named (such as someone on a watchlist).

Dark Market: An entity associated with a darknet market or cryptomarket is a commercial website on the web that operates via darknets such as Tor or I2P. They function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods as well as the sale of legal products.

Enterprise: A business or company.

Exchange: A business that allows customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money or other digital currencies. Does not include businesses with a significant physical ATM presence that makes up the bulk of their business.

Faucet: A website or app that dispenses cryptocurrency rewards for visitors to claim in exchange for completing a task as described by the website.

Gambling: An online gambling site that uses cryptocurrency as inputs and/or payouts. “Gambling” is accepting, recording, or registering bets, or carrying on a policy game (A lottery in which bets are made on an unpredictable number, such as a daily stock quotation) or any other lottery, or playing any game of

chance, for money or other thing of value.

High Risk Exchange: There are several factors that determine when an entity is categorized as a “High Risk Exchange”. These factors include, but are not limited to, the following: They are known bad actors, Intentionally try to circumvent AML and KYC measures, and/or are known to regularly fail to cooperate with law enforcement and regulators

HYIP: A high-yield investment program (HYIP) is a type of Ponzi scheme, an investment scam that promises unsustainably high return on investment by paying previous investors with the money invested by new investors. Most of these scams work from anonymous offshore bases which make them hard to track down.

Malware: An entity associated with crypto-malware, which installs a malicious payload into a victim’s computer that diverts CPU processing time to cryptocurrency mining, which doesn’t really do any harm to the computer or data, but can dramatically slow down performance. Unlike ransomware, it can go about doing its work completely undetected.

Miner: An individual miner or Cloud Mining company. A Cloud Mining Company operates a remote datacenter with shared processing power. This type of cloud mining enables users to mine bitcoins or alternative cryptocurrencies without managing the hardware. Mining rigs are housed and maintained in a facility owned by the mining company and the customer simply needs to register and purchase mining contracts or shares. Be careful not to confuse a miner with a mining pool which is more of an ad-hoc organization to which miners can belong.

Mixer: A cryptocurrency tumbler or cryptocurrency mixing service is a service offered to mix potentially identifiable or ‘tainted’ cryptocurrency funds with others, with the intention of confusing the trail back to the fund’s original source.

Pool: Mining pools are groups of cooperating miners who agree to share block rewards in proportion to their contributed mining hash power.

Ransomware: An entity associated with a type of malicious program that is designed to encrypt a system and its files, asking for cryptopayments to return, or decrypt, them.

Services: General services, including non-profits, forums and news sites, and addresses belonging to token contracts.

Wallet: A device, physical medium, program or service whose sole purpose is to store public and/or private keys and can be used to track ownership, receive or spend cryptocurrencies.

Is an owner of a wallet (cluster) always an actual individual?

No, an owner of a wallet can either be empty if there is no attribution for that wallet, or it can contain information such as the type of entity (criminal, exchange, etc.), the name (Coinbase, Locky, etc.), country, whether it’s subpoenaable or not, and the url.

Do you have some example queries for entity type returns?

A list of example queries that can be run to see examples of how this information is returned via the API is below:

ATM:

API Response: "atm"

Example: <https://rest.ciphertrace.com/api/v1/wallet?address=3E87wg9jWkTd1nYeSYHFr4A2FEff6RSL8Y>

Criminal:

API Response: "criminal"

Example:

<https://rest.ciphertrace.com/api/v1/wallet?address=bc1q9svj9wp68zftgejjgk6f96ukuyx8c5urkqsv69>

DarkMarket:

API Response: "darkmarket"

Example:

<https://rest.ciphertrace.com/api/v1/wallet?address=1PJWKiKXpm4LRpUwu4htHHMnMHCbGhykMS>

Enterprise:

API Response: "enterprise"

Example:

https://rest.ciphertrace.com/api/v1/eth_wallet?address=0xde0b295669a9fd93d5f28d9ec85e40f4cb697bae

Exchange:

API Response: "exchange"

Example:

https://rest.ciphertrace.com/api/v1/bch_wallet?address=qrq50rvl8u7teucv4tj55hkjyq58u5ewfv3j6m3hds

Faucet:

API Response: "faucet"

Example: <https://rest.ciphertrace.com/api/v1/wallet?address=3Ptt3mYRNSt8UQS6sLnZeFVRqJPwfp4ub3>

Gambling:

API Response: "gambling"

Example:

<https://rest.ciphertrace.com/api/v1/wallet?address=37X91qrSaGXC9Jn51Z4xWmhdSg3ZMgXVWh>

High Risk Exchange:

API Response: "high risk exchange"

Example: <https://rest.ciphertrace.com/api/v1/wallet?address=1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL>

Hyip:

API Response: "hyip"

Example: <https://rest.ciphertrace.com/api/v1/wallet?address=1BqKYVB56bCigs8zvpAYT9fvob8psRfvbd90>

Malware:

API Response: "malware"

Example: <https://rest.ciphertrace.com/api/v1/wallet?address=3DJhaQaKA6oyRaGyDZYdkZcise4b9DrCi2>

Miner:

API Response: "miner"

Example:

<https://rest.ciphertrace.com/api/v1/wallet?address=1Nh7uHdvY6fNwtQtM1G5EZAFLC33B59rB>

Mixer:

API Response: "mixer"

Example: <https://rest.ciphertrace.com/api/v1/wallet?address=1BestMixVhna91MkP7pKRtjej3bFq6Ze46>

Pool:

API Response: "pool"

Example: <https://rest.ciphertrace.com/api/v1/wallet?address=1AF3U6NX1YeArou7FyE4qzMhQVypaiyKkc>

Ransomware:

API Response: "ransomware"

Example:

<https://rest.ciphertrace.com/api/v1/wallet?address=15nLNJc9rfRhqgQMU6F9y85t3hSMG6AYwa>

Services:

API Response: "services"

Example:

<https://rest.ciphertrace.com/api/v1/wallet?address=1Hi1hRqeDW8psEt3K4zXEN8AhgnMVX4xDB>

Wallet:

API Response: "wallet"

Example: <https://rest.ciphertrace.com/api/v1/wallet?address=3QQnN5JwPiENYsjtUJ1hbzeQ2FSfwLpmTc>