



CipherTrace API

Version 1.24.1 - May 11, 2020

This document details the CipherTrace API. This API provides data access to CipherTrace customers and represents itself as an HTTPS based query service with JSON encoded data.

The API is an active project with many new features in development. The API implementation contains the Core API and the AML API. The Core API provides an address/wallet query service with transaction details and the AML API provides risk scores for addresses and transactions. Subsequent releases will provide historical address balance information, IP info for addresses, and IP info for transactions.

CipherTrace reserves the right to perform minor non-breaking updates to the API, such as potentially adding additional fields to existing information structures.

Table of Contents

Table of Contents	2
History	6
Authentication	7
Wallet Queries	8
Wallet Data Structures	9
Owner	9
Wallet	9
Transaction Queries	10
Transaction Data Structures	10
Transaction History	10
TxInput	10
TxOutput	11
Transaction Detail	11
AddressInfo	12
Transactions	12
Address Queries	13
Address Data Structures	13
Address Tx	13
IP Info	13
Address Results	14
Queries	16
Wallet By Address	16
Wallet By Wallet Id	16

Wallet Addresses	17
Transaction History for Address	19
Details for transaction list	20
Address Search	24
Query Count for Account User	25
BCH Queries	27
BCH Wallet By Address	27
BCH Wallet By Wallet Id	27
BCH Wallet Addresses	28
BCH Transaction History for Address	29
Details for BCH transaction list	29
BCH Address Search	31
LTC Queries	33
LTC Wallet By Address	33
LTC Wallet By Wallet Id	33
LTC Wallet Addresses	34
LTC Transaction History for Address	35
Details for LTC transaction list	35
LTC Address Search	37
Eth Queries	39
Eth Wallet By Address	39
Eth Wallet By Wallet Id	39
Eth Wallet Addresses	40
ETH Transaction History for Address	40
Details for Eth transaction list	41

Eth Address Search	42
BNB Queries	44
BNB Wallet By Address	44
BNB Wallet By Wallet Id	44
BNB Wallet Addresses	45
BNB Transaction History for Address	46
Details for BNB transaction list	46
BNB Address Search	48
IP Queries	50
IP Result	50
Address Match	51
IP Address Search	52
AML Risk Scoring API	53
Risk Scores	53
Note:	53
Call Back	54
Bitcoin Risk Scoring API	55
Transaction Risk Score Info	55
AddressRisks Info	55
Address Risk Score Info	58
Ethereum Risk Scoring API	60
ETH Transaction Risk Score Info	60
ETH Address Risk Info	61
ETH AddressRisks Map Info	61
Bitcoin Cash Risk Scoring API	64

Transaction Risk Score Info	64
Bitcoin Cash Address Risks Info	64
Address Risk Score Info	66
Litecoin Risk Scoring API	68
Transaction Risk Score Info	68
Litecoin Address Risks Info	68
Address Risk Score Info	70
Binance Chain Risk Scoring API	72
Transaction Risk Score Info	72
BNB Address Risks Info	72
Address Risk Score Info	74
BTC Watch List for Alerts	76
Changing and Inspecting the Watch List	76
Adding a BTC Address to watch	76
Removing a BTC Address from the watch list	76
Inspecting the entire watch list, use GET:	77
Clear the entire watch list	77
Updating User Preference for Webhook and Email Delivery	77
Receiving Webhook notifications	78
API FAQs (Frequently Asked Questions)	79

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

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 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 the CipherTrace 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 the Console 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 the transaction hashes that included the search address over a given 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)
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

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
txIndex	Long	Sequential index of transaction (useful for sorting transactions within a block)
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

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	Ending date for query
Wallet	Wallet	Wallet 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

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 By Address

This query returns wallet 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.

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": [
    "1EktpvfcPPyqbuRGyL6UkDgJHWDJQAScQ",
    "1Fr8xcEe9LkqN8Kgnr5dqj4cnyU7KJLNpb",
    "1PP1x2d42HL6vFy7XA5haUewuD67FpwxRa",
    "1DRPAA6m6gLez77PureMFiXhxS6rMg5Q3",
    "1HzEKvHPYHUnvCMzAndjLpJnMwvUDL5nd5",
    "1FrrQ67wcpDLisYaGshw54f2veHDzZTTQe",
    "1GXMT15AQXsgr2fHEqkUUitU6vR6SxucQd",
    "14hczTzPoa8cxbLSWmxutX4os6Vzs3QH5M",
    "1L7xBY9uq22V3UhtEdPp3DCbWL45TYE6XW",
    "1F5YcKGiT5i2wvKNwdxDWbbgzYzz2Hf36h",
    "1ELcjkDtgn1zp4zcCnmvy2MwMzvlJWvPlE",
    "1FUKHd3moVYTMFYpHggERjYp7HrzccMPPa",
  ]
}
```

"1Agkv6bWdeE7t1UH72vDdFtLsiGkNdgAPU",
"1GiFtyKRfbSTX6xJoQ6X2ABkizhcMmQF3Z",
"1HcUBeADVWJPJ8DtSVbjPpowWBmtcF8shv",
"1DnSnGfbCiljRQSPS9pf6utGjJ9XbMD6ta",
"1JPQQlTrjXrqRqEofEDoC2Zzfp9KvyG1FH",
"1QLH65j7zcZePNBhs5YyD5diG4kZVTXZre",
"1GYURtbqcnF9H3fVU7PgD3yopQWWA1GGQA",
"1AjxCSfAwpgTCLcGbkxCZTVZ7AxDo2CUFb",
"1Jv2h3YxtDMC7Y1D24qn8psympebzXMeCZ",
"1DvomEXpbmw1Z37RiwY653N1dfS1UZCXC3",
"1H7dwK3VCK6RqoRc7PmcZDiiEFKJboxesXr",
"1GusLDqkL1ShHDgSyRGPsKS7haGogxCYRU",
"1Fv1fK1JsacJ1fVChfoU3fJdYMHxNhCmjL",
"123zTvJw931gKezg4bMwaBS45YBQjJh3pZ",
"1EyfeFpyJFr5ahb56PJSmFRYajGFEhqeY",
"16Pd7Rgz2t45LtpgYqpeLG3VgVrb8KwPK",
"1Cy8AbHkMzWTBSJjHJtnUCXrvdfV9wCjcd",
"1CwxcDazTjK7h1BJwpABMLBqVajxCrP41c",
"1J2KmDQyQCQJebuzds5RFk3CSjyMZW8A28",
"1PyPvKT4XQcLwoCUwi9FVNVjRwrJ86oQya",
"1GRMuB5KsLRjsdnyP7NjXohLFmpxktFWSJ",
"15Jouskm1UHmZ2M2kUtNWNUGDwiQVtmoGA",
"17FANmXhwoDjUy276dskQwt3imejgYxwq4",
"183pjpcdni3SgK5yZCNDtz8TmsiZYyxYQ",
"1MWrS2P9HudUtsDzNAkUQXy9ZTwaLwYaH1",
"1AoG69yW5yrnKqKMcR1mbGvqCvLxwDAqQs",
"1PerzYxYd4ukRqMAHMcA1DuMU3aP5bPDeg",
"19A9tWsdB68KZgcKYcxHYtqn2sA9HR2ZZU",
"12mP1rBBdQNu6M2FmCx5WQpawsbzGH5AL4",
"13fbQ3WeYtTwFYcQuvmYaZmMH4Sn7iFmUo",
"1CFL9jYjS48Nv5nHgEMhXiqz5JKvU2kvTv",
"18uYMTeZxNLoANKv483CQUtVqx7g46fZ18",
"12LyHDCEGkxdVGygfSintzKhXeNikXCMFt",
"1h5Nx6jA4aLdj2Qn8NydX7bCAxi3HQkSU",
"19A4thzhK8Eq6PHbR6eiklCdqH9HVjrYA5",
"1Mip4rxtheHgkREe9mzGZGXzNTBbrShkiu",
"19HP4WhwUc3Hy6pqfNZiJfYPrhBD2xvtNA",
"1DPQiNFfn3L5ZGVdzVCQuSRkUhhXhmDSay",
"12GM2RDDWLCPAAzLDNadnvegBgzBiHMHun",
"1BAi9bB9PKpNiGmhqVvhYo4D2ioj7hgfpA",
"16EDTPCBUAtrRNrjzsb9v3PRrUMHjZMQ3v",
"1QEhETnNBJeQbwi2HW37Xu4Nh3fMSVXn9R",
"17JxnAGqBnq5Zg3qKhVVXymNyNrpBxZrAA",
"19SspSUHZzGBFMavW3hZppxZtdo66cNG4F",
"1Eex1fZZBPwkHj9bZGT4QZTegajqoYQbEY",
"1PqXDoWQerCSfj2ummFUV88sdFCnbzvV57",
"1japUvvpdz4uT49CSMUjqm4n8qsJhrKu",
"12FQZBebt7nQgA7VubbbGHQzKbUTjk9Avny",
"1Eru7ozyAjVmA4URtmwGNUFf5fNxKnEJPL",
"1H8KjbPsPSGCvRLj68vF3VoYzYzMhP9nuK",
"1HuLrXAKN9QiQW5e6a7q1p4bkhAQ5tjHtn",
"1JLdDwCbh2uyPiQMBBn9SjBodKcyluqUo",
"1K4UUqnnq9R2vUufodeCegokgdGfBNjYRj",
"1Jta5JwTGTDBjW86tnEJmJRYj9LamX2jjP",
"1FW9xGDLs7Qrkr7fWCCZfJfM98v2WL6leg",
"18QTXyUjIBRuEah4RXnGzGhSey6DEhzcio",
"1Pkts269uSb3nbT9EYcQpT1jGuQfviEMN6",
"19LZB5QkGQXbWB5zAxSDy3p6WkfsSvdFbB",
"1LBd2Ddm9iYBBYvYGgb6wwJjVsujahbcEY",
"1DvrGU3HGfbRp6Wb8wiAds53bSPUtYSjMc",
"1EVN8Kq6gX6QM4dc7bRgid9jhJLPVaQQeR",
"14g2MB8QVT8nE7uhcRPVo6X8cjpjs3Ezx",
"1Fs1T2RESrAT44zovp473H5F8NpMCxdwct",
"17t2tsxe8wWo8o1YG5CnRAujitRfv2n6Bi",
"16rUr5Sx5eFF7LK5mprgdeESZYHthi52og",

```

    "18cyCdZ38d7xHKHCPjB61xKdAzerdwoF7",
    "1PGRubz4R6CEa41kJjDR4p1sknAWhKBcEe",
    "15GTDsWZHvFxNfnHxFQbRHFfFqEe2Nqos8",
    "1QBGqWgFRrFLvzxx3kojQYUczuEbUne6Xd",
    "1kjChGREPEJtKAim4Ebvrc3mwk1QrEq8h",
    "15UheiezGRMGh2DsJv1JSKXYsugJcb2NnP",
    "1A4gemYhncwf78krmXxPgUK7fNV836GNGR",
    "1L8Ksxr3zYXncLPzxFEHj2F8GZLhnJfPeD",
    "1E4nbMYzgbZG5PwfjuaiTqGHAbD3Ye4aG8",
    "1FzNEXoi85QpwnVhNkwUGx5qK2jYrPBeY8",
    "1FwGLgBQ8YpjgH6VuoTjYyV7bFCpVCTZS2",
    "1GkYNcCCkTxckim7cV7hMCy5kRFwnh3uUc",
    "16S4jvoMttnnigCyBEzRoWTMnxbihWkg3w",
    "18gGwoyKzegNz4QZxE1TJDtKLgs38Xsjn9",
    "1HPNjrjDtm14zrrJHZ2dmYyfjviV2acyPK",
    "1PW9KS8T1ySvfois7KnwPDjQCkDi8SQDbk",
    "14eMZx6wiU3wSfk9sbFbepbiQrUJokDuv7",
    "19Pe7r8WFzyEMBZVMxgehCQzk36VTVcqz6",
    "1BgRb5VQ4aetvqmVCsTUBkEJ3sg9Y6QmZL",
    "1PpBWFijScRfFT3gF5iwZSulvFhKyhQ7BY",
    "1FzkKdTTMZQLMazzhn7oLz8hBUcFJkZh1x",
    "1Q8rVutEc2BTeBexsXTFr1WnD9rPUxEAkS",
    "1B4wuXbhNRsf7H6MuqWWWu2FG3jRwVBwQn"
  ]
}

```

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=17aaJMZqArjH3eufDaEJ3HZg74BJT7Gmgz&startdate=1459363904&enddate=1459373001>

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": "17aaJMzqArjH3eufDaEJ3HZg74BJT7Gmgz",
  "startDate": 1459363904,
  "endDate": 1459373001,
  "transactions": [
    "19e0886e6c6bdade6eb6fbae8aa0e83929cd4c6cf31fc442ff596af5c7f3035a",
    "e4bb4a6c82592be5e981b8551d97456bb508e6662d5524aacb837137b66f0543"
  ]
}
```

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 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": "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": "1FafR9D6zzQdNJB3mswRwPjyR6LbDtPtz",
    "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,
"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,
  "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
  }
},
"1M8MSttZPzUUmpcccNptPKKf5k3s3qq7H": {
  "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
  }
},
"14rGFdBqxfsi932Tpq6K56isQL2MxUHdWeg": {
  "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",

```

```

        "clientVersion": "/breadwallet:0.6.2/"
    }
  ],
  "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=133uy6u2VuYWNwyrNnUhYJj3GkoeTtzpcg&startdate=1513108829&enddate=1513127120>

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": 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": "133uy6u2VuYWNwyrNnUhYJj3GkoeTtzpcg",
}

```

```

"txHistory": [
  {
    "txHash": "3ea7b3067066c22cc58f577ed6aaf7fbac39c3202a05e70899bf5622e5e6afaf",
    "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",
    "pqmud4zkjyqyd7cdvgzcp5dux37npflrhg0u8k6uqg",
    ...
  ]
}
```

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=qrlfsgth5nq6sx0478q5pum12g5d65rcsv5h35yc5n5rcsv5h35yc5n

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": "qqqfv026xdaqdru0zcynd6819qn4kqhvs7rtwxflg",
          "value": 0.3
        },
        {

```

```

    "pos": 1,
    "address": "qq3vpr7hyeaphsf515asmz7qww3fjj3v0q9atekxah",
    "value": 2.66584708
  },
  {
    "pos": 2,
    "address": "qr5m999harx1phgv2g5ntpel7hndqn9p4q2y8ee0cq",
    "value": 0.00788939
  }
],
"total": 2.97373647,
"inputs": [
  {
    "pos": 0,
    "address": "qrmf7ymjy4rkp20qv8cwfpxs5qxczkr91cl3w73xry",
    "value": 2.96584708
  },
  {
    "pos": 1,
    "address": "qz7jhxx75fs4a5zp22mqrkyh288gtepqq5mfxvsfv2",
    "value": 0.00838939
  }
],
"date": 1381345912,
"fee": 0.00050
},
{
  "txHash": "f96b6f05faf74f1c3e33d365cc83203cf31bd67b756321db4ab54c0a0f66aaf8",
  "outputs": [
    {
      "pos": 0,
      "address": "qqnh7j4254qclfy3uzk0r3c5gtgzhwvugqrltekd",
      "value": 0.3
    },
    {
      "pos": 1,
      "address": "qz62e6pdhxx190xdlgcztac71z4ws4p5updfqq8n",
      "value": 0.0042922
    }
  ],
  "total": 0.3042922,
  "inputs": [
    {
      "pos": 0,
      "address": "qqqfv026xdaqdru0zcynd6819qn4kqhv6s7rtwxflg",
      "value": 0.3
    },
    {
      "pos": 1,
      "address": "qpprp3pua775jfnwv3n9pyr07p10cgpnhgcvwte88t",
      "value": 0.0047922
    }
  ],
  "date": 1381345912,
  "fee": 0.00050
}
],
"addresses": {
  "qrmf7ymjy4rkp20qv8cwfpxs5qxczkr91cl3w73xry": {
    "wallet": {
      "walletId": "0131025c",
      "owner": {},
      "totalAddressCount": 2,
      "revision": 0
    }
  }
}

```

```

    },
    "qz62e6pdhxxt190xdlgczktac71z4ws4p5updfqq8n": {
      "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=qrlfsgth5nq6sx0478q5pum12g5d65rcsv5h35yc5n

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": "qrlfsgth5nq6sx0478q5pum12g5d65rcsv5h35yc5n",
  "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=LQcctH7yCV1qh97ktAHWHAbDHtc5hgCdAF

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": [
    "LLMQrWWkNBy2Q1rtpuvKNNZXxzphPXFvV",
    "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",
    "f354585871aaca128f7a27b179fd0bed4807dafbc640b2b5719035222bf2d0d",
    ...
  ]
}
```

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=A58F941AEE0AAA32B8123452D2717CA532DB63DB54A786BE365CAB0F29922023,28A301ABFE1F1CD72DF36020FCC34D09AFE024A2CF67A987837498F656EC0A01

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": "LNtA2kZnX7cwnzFXfnaMTLGcCyjyeaPmcA",
    "value": 3.41281029
  }
],
"date": 1518653907,
"fee": 0.05072998
},
{
  "txHash": "28A301ABFE1F1CD72DF36020FCC34D09AFE024A2CF67A987837498F656ECA01",
  "outputs": [
    {
      "pos": 0,
      "address": "LcpldUUeYpNctkqGh8GKPLDms6hqKmxnwy",
      "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": "001b29e5",
  "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=001b29e5

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

```
{
  "walletId": "001b29e5",
  "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=001b29e5&count=100&offset=100

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

```
{
  "addressOffset": 0,
  "walletId": "001b29e5",
  "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",
    "0xbc6f3e826c0983a5277d269acdca76061444ceb210fa45046c374f7709cf48c",
    "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.

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": [
    {
      "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
    }
  },
  "0x209c4784ab1e8183cf58ca33cb740efbf3fc18ef": {
    "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=133uy6u2VuYWNwyrNnUhYj3GkoeTtzpcg&startdate=1513108829&enddate=1513127120&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,
  "next_offset": -1,
  "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": "000f637d",
    "owner": {},
    "totalAddressCount": 1,
    "revision": 0
  }
}
```

BNB Queries

BNB 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=bnb12wpk84anf1tnwj9l7l9xazur4u70yxmdyj8g1k

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

```
{
  "walletId": "bnb12wpk84anf1tnwj9l7l9xazur4u70yxmdyj8g1k",
  "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=bnb1f69utnu7stm6kd84j0d7y2520hjq3ak8khhczj

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

```
{
  "walletId": "bnb1f69utnu7stm6kd84j0d7y2520hjq3ak8khhczj",
  "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=bnb12wpk84anf1tnwj9l7l9xazur4u70yxmdyj8g1k&count=100

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

```
{
  "addressOffset": 0,
  "walletId": "bnb12wpk84anf1tnwj9l7l9xazur4u70yxmdyj8g1k",
  "revision": 0,
  "walletIdChanged": false,
  "owner": {
    "name": "AtomicWallet",
    "subpoenable": false,
    "url": "https://atomicwallet.io/",
    "country": "UN",
    "type": "wallet"
  },
  "totalAddressCount": 1,
  "addresses": [
    "bnb12wpk84anf1tnwj9l7l9xazur4u70yxmdyj8g1k"
  ]
}
```

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",
    "D5ED106A1ED9BA237166BB0886A1504B7F738BBFA6DF6429F70D8A6790D138",
    "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": "bnb12cvjxjrqw6lz092pvzsealsr17g90pkx25n7mc",

```

```

        "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": "bnb12wpk84anf1tnwj91719xazur4u70yxmdyj8glk",
          "value": 1.5
        }
      ],
      "outputs": [
        {
          "address": "bnb119whj8d4vjw6jwkj6h260eu5xr6lkt067zhumu",
          "value": 1.5
        }
      ]
    }
  ],
  "feeAsset": "BNB",
  "date": 1572634618,
  "fee": 0.000375
}
],
"addresses": {
  "bnb12cvjxjrqw6lz092pvzsealsrl7g90pkx25n7mc": {
    "wallet": {
      "walletId": "bnb12cvjxjrqw6lz092pvzsealsrl7g90pkx25n7mc",
      "owner": {},
      "totalAddressCount": 1,
      "revision": 0
    }
  },
  "bnb1000exsx2fy58zve825nerr6v605m6v626yd2yp": {
    "wallet": {
      "walletId": "bnb1000exsx2fy58zve825nerr6v605m6v626yd2yp",
      "owner": {},
      "totalAddressCount": 1,
      "revision": 0
    }
  },
  "bnb12wpk84anf1tnwj91719xazur4u70yxmdyj8glk": {
    "wallet": {
      "walletId": "bnb12wpk84anf1tnwj91719xazur4u70yxmdyj8glk",
      "owner": {
        "name": "AtomicWallet",
        "subpoenable": false,
        "url": "https://atomicwallet.io/",
        "country": "UN",

```

```

        "type": "wallet"
      },
      "totalAddressCount": 1,
      "revision": 0
    }
  },
  "bnb119whj8d4vjwt6jwkj6h260eu5xr6lkt067zhumu": {
    "wallet": {
      "walletId": "bnb119whj8d4vjwt6jwkj6h260eu5xr6lkt067zhumu",
      "owner": {
        "name": "Exrates",
        "subpoenable": false,
        "url": "https://exrates.me/dashboard",
        "country": "CH",
        "type": "exchange"
      },
      "totalAddressCount": 1,
      "revision": 0
    }
  }
}

```

BNB 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/bnb_address/search?startdate=1546329600&enddate=1572897821&features=tx&address=bnb119whj8d4vjwt6jwkj6h260eu5xr6lkt067zhumu&offset=0&limit=10

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": "bnb119whj8d4vjwt6jwkj6h260eu5xr6lkt067zhumu",
  "startDate": 1546329600,
  "endDate": 1572897821,
  "inCase": false,
  "wallet": {
    "walletId": "bnb119whj8d4vjwt6jwkj6h260eu5xr6lkt067zhumu",
    "owner": {
      "name": "Exrates",
      "subpoenable": false,
      "url": "https://exrates.me/dashboard",
      "country": "CH",
      "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
}
]
}

```

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=1549359083&enddate=1549764527>

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)

Note:

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, the address has no transactions, or this is a new address for which CipherTrace is still in the process of calculating its risk classification (in this situation, the updated risk classification should appear within a few hours).
1	No transactions with any level 9 or 10 addresses within one hop.

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

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": {
    "14cN2pTimACRJ4dqitFLuhrmKQL6xxAoY": {
      "outputValue": 0.022,
      "callbackSeconds": 86400,
      "risk": 10,
      "sanctionsRisk": 1,
      "gamblingOkRisk": 10,
      "address": "14cN2pTimACRJ4dqitFLuhrmKQL6xxAoY",
      "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=4c97b52c13b6a42ed949d57d0b4e88bbe13e591c14f123de615799b34b8abc5>

```

{
  "callbackSeconds": 86400,
  "risk": 4,
  "sanctionsRisk": 1,
  "gamblingOkRisk": 4,
  "txhash": "4c97b52c13b6a42ed949d57d0b4e88bbe13e591c14f123de615799b34b8abc5",
  "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
  },
  "1GeTxbEJUguDYNb7EtXkwrtVHlwCndjA6f": {
    "outputValue": 0.00234029,
    "callBackSeconds": 86400,
    "risk": 1,
    "sanctionsRisk": 1,
    "gamblingOkRisk": 1,
    "address": "1GeTxbEJUguDYNb7EtXkwrtVHlwCndjA6f",
    "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.

The current version of our API only supports native Ethereum transactions; support for token transfers will be coming soon.

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

ETH AddressRisks 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

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	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. 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": {
    "qpqdc0cxn5jgl78x9uznx14yx5h6xevz5heqmfant": {
      "outputValue": 0.0,
      "callbackSeconds": 86400,
      "risk": 1.0,
      "sanctionsRisk": 1.0,
      "gamblingOkRisk": 1.0,
      "address": "qpqdc0cxn5jgl78x9uznx14yx5h6xevz5heqmfant",
      "inputValue": 4.0
    },
    "qqvqptrmntnap48hk2m25n3wng9g5lryxs36ftpl9a": {
```

```

    "outputValue": 0.0,
    "callbackSeconds": 86400,
    "risk": 1.0,
    "sanctionsRisk": 1.0,
    "gamblingOkRisk": 1.0,
    "address": "qqvqptrmtnap48hk2m25n3wng9g5lryxs36ftp19a",
    "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	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/bch/risk?address=qrlfsgth5nq6sx0478q5puml2g5d65rcsv5h35yc5n>

```

{
  "callbackSeconds": 86400,
  "risk": 1.0,
  "sanctionsRisk": 1.0,
  "gamblingOkRisk": 1.0,
  "address": "qrlfsgth5nq6sx0478q5puml2g5d65rcsv5h35yc5n",
  "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	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. Example below.

<https://rest.ciphertrace.com/aml/v1/ltc/risk?txhash=eca234a041edaef3bfd353fdf99d5b2fb54cbccab9837a7aade8038cfdd404fe>

```
{
  "callbackSeconds": 86400,
  "risk": 10.0,
  "sanctionsRisk": 8.0,
  "gamblingOkRisk": 8.0,
  "txhash": "eca234a041edaef3bfd353fdf99d5b2fb54cbccab9837a7aade8038cfdd404fe",
  "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	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/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	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. 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	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/bnb/risk?address=bnb1l9whj8d4vjwt6jwkj6h260eu5xr6lkt067zhumu>

```
{
  "callbackSeconds": 0,
  "risk": 1.0,
  "sanctionsRisk": 1.0,
  "gamblingOkRisk": 1.0,
  "address": "bnb1l9whj8d4vjwt6jwkj6h260eu5xr6lkt067zhumu",
  "updatedToBlock": 46143578
}
```


Inspecting the entire watch list, use GET:

To see the entire watch list, use a GET call to the base subscriptions URL

```
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)

- 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.

- 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.

- What are all the types of wallets that we have?
 - Exchange = A cryptocurrency exchange such as Coinbase, Kraken, etc.
 - 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 fail to cooperate with law enforcement and regulators.
 - Wallet = A cryptocurrency wallet that stores one’s keys to send/receive a specified cryptocurrency.
 - Miner = An individual miner or mining pool entity that mines the Bitcoin blockchain.
 - Enterprise = A business or company.
 - ATM = Bitcoin ATMs.
 - Services = Various types of services that allow movement of cryptocurrency.
 - Faucet = A faucet is an entity that dispenses rewards in the form of Bitcoin or satoshi (the lowest unit of Bitcoin)
 - Abandoned = Cryptocurrency assets that have been deserted.
 - Pools = Bitcoin Mining Pools.
 - Gambling = An online gambling site that uses cryptocurrency.
 - Hyip = A fake investment fund/pyramid scheme. Also known as High Yield Investment Program scam.
 - Mixer = A third party service that allows people to break the connection of who they are sending Bitcoin to. Also known as tumbling.
 - Malware = A type of software that damages or is harmful to a computer.

- o Ransomware = A type of malicious software that blocks service to one's computer and requests ransom in order to give access back to the user.
- o Dark Market = An illegal market that operates via Tor, I2P, etc. that primarily is used to sell drugs, weapons, counterfeit items, etc.
- o Criminal = Known criminals via thefts and attribution.

- Is an owner of a wallet 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.

- 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.

- How are entity names returned and what are the various types?

The following list of entity types is what CipherTrace currently supports:

- o ATM
- o Criminal
- o DarkMarket
- o Enterprise
- o Exchange
- o Faucet
- o Gambling
- o High Risk Exchange
- o Hyip
- o Malware
- o Miner
- o Mixer
- o Pool
- o Ransomware
- o Services
- o Wallet

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=1BqKYVB56bCigs8zvpAYT9fvob8psRfvbd>

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=1Hi1hRqeDW8psEt3K4zXEN8AhgnMVX4xD>

Wallet:

API Response: "wallet"

Example:

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