# A Monero data model and API specification

with implementations in Java, TypeScript, and C++ using monero v0.18.3.4 'Flourine Fermi'

Last updated August 28, 2024



Java implementation: <a href="https://github.com/monero-ecosystem/monero-java">https://github.com/monero-ecosystem/monero-java</a>

TypeScript implementation: <a href="https://github.com/monero-ecosystem/monero-ts">https://github.com/monero-ecosystem/monero-ts</a>

C++ implementation: <a href="https://github.com/monero-ecosystem/monero-cpp">https://github.com/monero-ecosystem/monero-cpp</a>

Document source: https://github.com/monero-ecosystem/monero-java/blob/master/docs/monero-spec.drawio

Document created and revisable using: https://www.draw.io/

# Monero Daemon Interface 1/2 setProxyUri(string proxyUri): void isConnected(): bool getVersion(): MoneroVersion isTrusted(): bool getHeight(): ulong getBlockHash(ulong height): string getBlockTemplate(string walletAddress, uint reserveSize=null): MoneroBlockTemplate getLastBlockHeader(): MoneroBlockHeader getBlockHeaderByHash(string blockHash): MoneroBlockHeader getBlockHeaderByHeight(ulong height): MoneroBlockHeader getBlockHeadersByRange(ulong startHeight=0, ulong endHeight=chainHeight): MoneroBlockHeader[] getBlockByHash(string blockHash): MoneroBlock getBlocksByHash(string[] blockHashes, ulong startHeight, bool prune=false): MoneroBlock[] getBlockByHeight(ulong height): MoneroBlock getBlocksByHeight(ulong[] heights): MoneroBlock[] getBlocksByRange(ulong startHeight=0, ulong endHeight=chainHeight): MoneroBlock[] getBlocksByRangeChunked(ulong startHeight=0, ulong endHeight=chainHeight, ulong maxChunkSize=3000000): MoneroBlock[] getBlockHashes(string[] blockHashes, ulong startHeight): string[] getTx(string txHash, bool prune=false): MoneroTx getTxs(string[] txHashes, bool prune=false): MoneroTx[] getTxHex(string txHash, bool prune=false): string getTxHexes(string[] txHashes, bool prune=false): string[] getMinerTxSum(ulong height, ulong numBlocks=chainHeight): MoneroMinerTxSum getFeeEstimate(ulong graceBlocks=?): MoneroFeeEstimate $submitTxHex(string\ txHex,\ bool\ doNotRelay=false):\ MoneroSubmitTxResult$ relayTxByHash(string txHash): void relayTxsByHash(string[] txHashes): void getTxPool(): MoneroTx[] getTxPoolHashes(): string[] getTxPoolBacklog(): MoneroTxBacklogEntry[] getTxPoolStats(): MoneroTxPoolStats flushTxPool(string[] txHashes=null): void getKeyImageSpentStatus(string keyImage): MoneroKeyImageSpentStatus getKeyImageSpentStatuses(string[] keyImages): MoneroKeyImageSpentStatus[] getOutputs(MoneroOutput[] outputs): MoneroOutput[] getInfo(): MoneroDaemonInfo getSyncInfo(): MoneroDaemonSyncInfo getHardForkInfo(): MoneroHardForkInfo

```
Monero Daemon Interface 2/2
getAltChains(): MoneroAltChain[]
getAltBlockHashes(): string[]
getDownloadLimit(): uint
setDowloadLimit(uint limit): uint
resetDownloadLimit(): uint
getUploadLimit(): uint
setUploadLimit(uint): uint
resetUploadLimit(): uint
getPeers(): MoneroPeer[]
getKnownPeers(): MoneroPeer[]
setOutgoingPeerLimit(uint limit): void
setIncomingPeerLimit(uint limit): void
getPeerBans(): MoneroBan[]
setPeerBan(MoneroBan ban): void
setPeerBans(MoneroBan[] bans): void
qetOutputDistribution(ulong[] amounts, bool isCumulative, ulong startHeight=0, ulong endHeight=chainHeight):
         MoneroOutputDistributionEntry[]
getOutputHistogram(ulong[] amounts, ulong minCount, ulong maxCount, bool isUnlocked, ulong recentCutoff):
         MoneroOutputHistogramEntry[]
startMining(string address, ulong numThreads=null, bool isBackground=false, bool ignoreBattery=false): void
stopMining(): void
getMiningStatus(): MoneroMiningStatus
submitBlock(string blockBlob): void
submitBlocks(string[] blockBlobs): void
checkForUpdate(): MoneroDaemonUpdateCheckResult
downloadUpdate(string path): MoneroDaemonUpdateDownloadResult
addListener(MoneroDaemonListener listener): void
removeListener(MoneroDaemonListener listener): void
```

waitForNextBlockHeader(): MoneroBlockHeader

pruneBlockchain(bool check): MoneroPruneResult

stop(): void

# Monero Daemon Types 1/3

#### MoneroBlockHeader

hash: string height: ulong

timestamp: ulong

size: ulong weight: ulong

long\_term\_weight: ulong

depth: ulong difficulty: ulong

cumulative\_difficulty: ulong

major\_version: uint minor\_version: uint

nonce: ulong

miner\_tx\_hash: string

num\_txs: uint

orphan\_status: bool

prev\_hash: string

pow\_hash: string

reward: ulong



#### MoneroBlock

hex: string

miner\_tx: MoneroTx

txs: MoneroTx[]

tx\_hashes: string[]

#### MoneroOutput

tx: MoneroTx

key\_image: MoneroKeyImage

amount: ulong index: ulong

ring\_output\_indices: ulong[]
stealth\_public\_key: string

#### MoneroDaemonInfo

version: string

num\_alt\_blocks: ulong block\_size\_limit: ulong

block\_size\_median: ulong block\_weight\_limit: ulong

block\_weight\_median: ulong

bootstrap\_daemon\_address: string

difficulty: ulong

cumulative\_difficulty: ulong

free\_space: ulong

num\_offline\_peers: uint

num\_online\_peers: uint

height: ulong

height\_without\_bootstrap: ulong

network\_type: MoneroNetworkType

is\_offline: bool

num\_incoming\_connections: uint

num\_outgoing\_connections: uint

num\_rpc\_connections: uint

start\_timestamp: ulong

adjusted\_timestamp: ulong

target: ulong

target\_height: ulong

top\_block\_hash: string

num\_txs: uint

num\_txs\_pool: uint

was\_bootstrap\_ever\_used: bool

database\_size: uint update\_available: bool

credits: ulong

is\_busy\_syncing: bool

is\_synchronized: bool

is\_restricted: bool

#### MoneroTx

block: MoneroBlock

height: ulong hash: string version: uint

is\_coinbase: bool
payment\_id: string

fee: ulong

ring\_size: uint

do\_not\_relay: bool is\_relayed: bool is\_confirmed: bool

in\_tx\_pool: bool

num\_confirmations: ulong

unlock\_time: ulong

last\_relayed\_timestamp: ulong
received\_timestamp: ulong

is\_double\_spend: bool

key: string

full\_hex: string

pruned\_hex: string
prunable\_hex: string

prunable\_hash: string

size: ulong

weight: ulong

inputs: MoneroOutput[]
outputs: MoneroOutput[]

output\_indices: ulong[]

metadata: string

extra: byte[]

rct\_signatures: string[]

rct\_sig\_prunable: ?

is\_kept\_by\_block: bool

is\_failed: bool

last\_failed\_height: ulong

last\_failed\_hash: string

max\_used\_block\_height: ulong

# Monero Daemon Types 2/3

MoneroDaemonSyncInfo

height: ulong

connections: MoneroDaemonConnection[]

spans: MoneroDaemonConnectionSpan[]

target\_height: ulong

next\_needed\_pruning\_seed: uint

overview: ?

MoneroBan

host: string ip: string

is\_banned: bool

seconds: ulong

MoneroBlockTemplate

block\_template\_blob: string

block\_hashing\_blob: string

difficulty: ulong

expected\_reward: ulong

height: ulong

prev\_hash: string

reserved offset: ulong

seed\_height: ulong

seed\_hash: string

next\_seed\_hash: string

 ${\tt MoneroDaemonConnectionSpan}$ 

connection\_id: string

num blocks: ulong

remote\_address: string

rate: ulong

speed: ulong

size: ulong

start\_block\_height: ulong

MoneroDaemonListener

onBlockHeader(MoneroBlockHeader header): void

<enumeration>
MoneroNetworkType

mainnet: 0 testnet: 1

stagenet: 2

MoneroKeyImage

hex: string

signature: string

<enumeration>
MoneroKeyImageSpentStatus

not\_spent: 0

confirmed: 1

tx\_pool: 2

MoneroSubmitTxResult

is\_good: bool

is\_relayed: bool

is\_double\_spend\_seen: bool

is\_fee\_too\_low: bool

is\_mixin\_too\_low: bool

has\_invalid\_input: bool

has\_invalid\_output: bool

has\_too\_few\_outputs: bool

is\_rct: bool

is overspend: bool

is\_too\_big: bool

sanity\_check\_failed: bool

reason: string

credits: ulong

top\_block\_hash: string

is\_tx\_result\_too\_big: bool

nonzero\_unlock\_time: bool

MoneroPeer

max used block hash: string

signatures: string[]

id: string

address: string

host: string

port: uint

is\_online: boolean

last\_seen\_timestamp: ulong

pruning\_seed: uint

rpc\_port: uint

rpc\_credits\_per\_hash: ulong

type: ConnectionType

num\_support\_flags: uint

state: string

send\_idle\_time: ulong

receive\_idle\_time: ulong

num\_sends: uint

num\_receives: uint

is\_local\_host: bool

is\_local\_ip: bool

live\_time: ulong

is incoming: bool

height: ulong

current\_upload: ulong

current\_download: ulong

avg\_upload: ulong

avg\_download: ulong

# **Monero Daemon Types 3/3**

#### MoneroHardForkInfo

earliest\_height: ulong

is\_enabled: bool

state: uint

threshold: uint

version: string

num\_votes: uint

window: uint

voting: uint

credits: ulong

top\_block\_hash: string

#### MoneroVersion

number: uint

is\_release: bool

# <enumeration> ConnectionType

invalid: 0

ipv4: 1

ipv6: 2

tor: 3

i2p: 4

#### MoneroFeeEstimate

fee: ulong

fees: ulong[]

quantizationMask: ulong

#### MoneroDaemonUpdateCheckResult

is\_update\_available: bool

version: string
hash: string
auto\_uri: string

user\_uri: string

Extends

#### MoneroDaemonUpdateDownloadResult

download\_path: string

#### MoneroMinerTxSum

emission\_sum: ulong

fee\_sum: ulong

# MoneroMiningStatus

is\_active: bool

is\_background: bool

address: string speed: ulong

.

num\_threads: uint

#### MoneroPruneResult

is\_pruned: bool

pruning\_seed: uint

#### MoneroOutputHistogramEntry

amount: ulong

num\_instances: ulong

num\_unlocked\_instances: ulong
num\_recent\_instances: ulong

#### MoneroTxPoolStats

num\_txs: uint

num\_not\_relayed: uint

num\_failing: uint

num\_double\_spends: uint

num\_10m: uint

fee\_total: ulong

bytes\_max: ulong

bytes\_med: ulong

bytes\_min: ulong

bytes\_total: ulong

histo: ?

histo\_98pc: unlong

oldest\_timestamp: ulong

#### MoneroAltChain

block\_hashes: string[]

difficulty: ulong

height: ulong

length: ulong

main\_chain\_parent\_block\_hash: string

#### Monero Wallet Interface 1/3

```
addListener(MoneroWalletListener listener): void
removeListener(MoneroWalletListener): void
getListeners(): MoneroWalletListener[]
isViewOnly(): bool
setDaemonConnection(MoneroDaemonConnection connection): void
getDaemonConnection(): MoneroDaemonConnection
setProxyUri(string proxyUri): void
isConnectedToDaemon(): bool
getVersion(): MoneroVersion
getNetworkType(): MoneroNetworkType
getPath(): string
getSeed(): string
getSeedLanguage(): string
getSeedLanguages(): string[]
getPrivateSpendKey(): string
getPrivateViewKey(): string
getPublicSpendKey(): string
getPublicViewKey(): string
getPrimaryAddress(): string
getAddress(uint accountIdx, uint subaddressIdx): string
getAddressIndex(string address): MoneroSubaddress
getDaemonConnection(): MoneroRpcConnection
getDaemonHeight(): ulong
getDaemonMaxPeerHeight(): ulong
getApproximateChainHeight(): ulong
getHeight(): ulong
getHeightByDate(uint year, uint month, uint day): ulong
sync(ulong startHeight=null, MoneroSyncListener listener=null): MoneroSyncResult
startSyncing(): void
stopSyncing(): void
scanTxs(string[] txHashes): void
rescanSpent(): void
rescanBlockchain(): void
getBalance(uint accountIdx=null, uint subaddressIdx=null): ulong
getUnlockedBalance(uint accountIdx=null, uint subaddressIdx=null): ulong
getAccounts(bool includeSubaddresses=false, string tag=null): MoneroAccount[]
getAccount(uint accountIdx, bool includeSubaddresses=false): MoneroAccount
createAccount(string label=null): void
getSubaddresses(uint accountIdx, uint[] subaddressIndices): void
getSubaddress(uint accountIdx, uint subaddressIdx): MoneroSubaddress
```

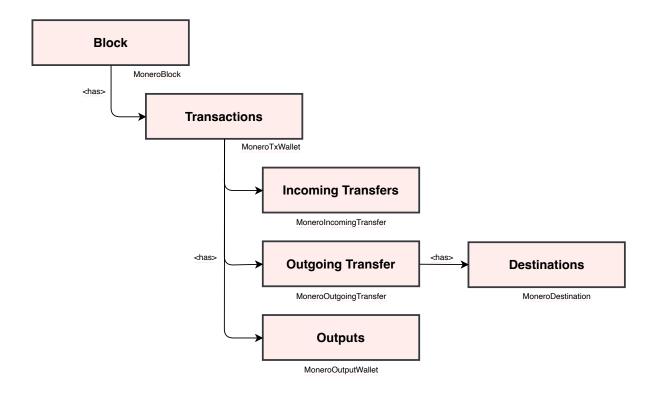
#### Monero Wallet Interface 2/3

```
createSubaddress(uint accountIdx, string label=null): MoneroSubaddress
setAccountLabel(uint accountIdx, string label): void
setSubaddressLabel(uint accountIdx, string subaddressIdx, string label): void
getTx(string txId): MoneroTxWallet
getTxs(MoneroTxQuery query=null): MoneroTxWallet[]
getTransfers(uint accountIdx=null, uint subaddressIdx=null): MoneroTransfer[]
getOutputs(MoneroOutputQuery query=null): MoneroOutputWallet[]
getOutgoingTransfers(MoneroTransferQuery query=null): MoneroOutgoingTransfer[]
getIncomingTransfers(MoneroTransferQuery query=null): MoneroIncomingTransfer[]
getTransfers(MoneroTransferQuery query=null): void
exportOutputs(bool all=false): string
importOutputs(string outputsHex): uint
exportKeyImages(bool all=false): MoneroKeyImage[]
importKeyImages(MoneroKeyImage[] keyImages): MoneroKeyImageImportResult
freezeOutput(String keyImage): void
thawOutput(String keyImage): void
isOutputFrozen(String keyImage): bool
getNewKeyImagesFromLastImport(): MoneroKeyImage[]
createTx(MoneroTxConfig config): MoneroTxWallet
createTxs(MoneroTxConfig config): MoneroTxWallet[]
sweepOutput(MoneroTxConfig config): MoneroTxWallet
sweepUnlocked(MoneroTxConfig config): MoneroTxWallet[]
sweepDust(bool relay=false): MoneroTxWallet[]
relayTx(string txMetadata): string
relayTx(MoneroTxWallet tx): string
relayTxs(string[] txMetadatas): string[]
relayTxs(MoneroTxWallet[] txs): string[]
describeTxSet(MoneroTxSet txSet): MoneroTxSet
signTxs(string unsignedTxHex): MoneroTxSet
submitTxs(string signedTxHex): string[]
signMessage(string message, MoneroMessageSignatureType type, int accountIdx, int subaddressIdx): string
verifyMessage(string message, string address, string signature): MoneroMessageSignatureResult
getTxKey(string txId): string
checkTxKey(string txId, string txKey, string address): MoneroCheckTx
getTxProof(String txId, string address, string message=null): string
checkTxProof(string txId, string address, string message, string signature): MoneroCheckTx
getSpendProof(string txId, string message=null): string
checkSpendProof(string txId, string message, string signature): bool
```

#### Monero Wallet Interface 3/3

```
getReserveProofWallet(string message): string
getReserveProofAccount(uint accountIdx, ulong amount, string message): string
checkReserveProof(string address, string message, string signature): MoneroCheckReserve
setTxNotes(string[] txHashes, string[] notes): void
setTxNote(string txHash, string note): void
getTxNotes(string[] txHashes): string[]
getTxNote(string txHash): string
getAddressBookEntries(uint[] entryIndices=null): MoneroAddressBookEntry[]
addAddressBookEntry(string address, string description): uint
editAddressBookEntry(uint entryIdx, bool setAddress, string address, bool setDescription, string description): void
deleteAddressBookEntry(uint entryIdx): void
tagAccounts(string tag, uint[] accountIndices): void
untagAccounts(uint[] accountIndices): void
getAccountTags(): MoneroAccountTag[]
setAccountTagLabel(string tag, string label): void
getPaymentUri(MoneroTxConfig request): string
parsePaymentUri(string uri): MoneroSendRequest
getAttribute(string key): string
setAttribute(string key, string val): void
startMining(uint numThreads=null, bool backgroundMining=false, bool ignoreBattery=true): void
stopMining(): void
isMultisigImportNeeded(): bool
isMultisig(): bool
getMultisigInfo(): MoneroMultisigInfo
prepareMultisig(): string
makeMultisig(string[] multisigHexes, uint threshold, string password): string
exchangeMultisigKeys(string[] multisigHexes, string password): MoneroMultisigInitResult
exportMultisigHex(): string
importMultisigHex(string[] multisigHexes): uint
signMultisigTxHex(string multsiigTxHex): MoneroMultisigSignResult
submitMultisig(string signedMultisigHex): string[]
moveTo(string path): void
changePassword(string oldPassword, string newPassword): void
save(): void
close(bool save=false): void
isClosed(): bool
getIntegratedAddress(string standardAddress=null, string paymentId=null): MoneroIntegratedAddress (deprecated)
decodeIntegratedAddress(string integratedAddress): MoneroIntegratedAddress (deprecated)
```

# Monero Wallet Types 1/4 - Transactions, Transfers, and Outputs



Transactions are part of a block and have incoming transfers and/or an outgoing transfer.

The outgoing transfer may have destination amounts and addresses which are saved locally with the wallet and are not recoverable from the blockchain.

Transactions may also have outputs received by the wallet when requested.

## Monero Wallet Types 2/4 - Send Request and Queries for Transactions, Transfers, and Outputs

MoneroTxConfig

address: string amount: ulong

destinations: MoneroDestination[]

subtract\_fee\_from: int[]
payment\_id: string

priority: MoneroTxPriority

fee: ulong

account\_index: uint

subaddress\_index: uint

subaddress\_indices: uint[]

can\_split: bool relay: bool note: string

recipient\_name: string below\_amount: ulong

sweep\_each\_subaddress: bool

key\_image: string

MoneroTxQuery extends MoneroTxWallet

is\_outgoing: bool is\_incoming: bool hashes: string[]

has\_payment\_id: bool
payment\_ids: string[]

height: ulong

min\_height: ulong
max\_height: ulong
include\_outputs: bool

transfer\_request: MoneroTransferQuery

output\_request: MoneroOutputQuery

Configures a query to get wallet transactions.

Configures creating transactions to send funds.

MoneroOutputQuery extends MoneroOutputWallet

subaddress\_indices: uint[]
tx\_query: MoneroTxQuery

min\_amount: ulong max amount: ulong

Configures a query to get wallet outputs.

MoneroTransferQuery extends MoneroTransfer

is\_incoming: bool
address: string
addresses: string[]
subaddress\_index: uint

subaddress\_indices: uint[]

destinations: MoneroDestination[]

has\_destinations: bool

tx\_query: MoneroTxQuery

Configures a query to get wallet transfers.

# Monero Wallet Types 3/4

#### MoneroAccount

index: uint

primary\_address: string

balance: ulong

unlocked\_balance: ulong

subaddresses: MoneroSubaddress[]

tag: string

#### MoneroSubaddress

account index: uint

index: uint

address: string

label: string

balance: ulong

unlocked\_balance: ulong

is\_used: bool

num\_unspent\_outputs: ulong

num\_blocks\_to\_unlock: ulong

#### MoneroDestination

address: string amount: ulong

# MoneroOutputWallet extends MoneroOutput

account\_index: uint

subaddress\_index: uint

is\_spent: bool
is\_frozen: bool

#### MoneroTransfer

tx: MoneroTxWallet
is\_incoming: bool
amount: ulong

account\_index: uint

# Extends

# MoneroIncomingTransfer

subaddress index: uint

address: string

num\_suggested\_confirmations: ulong

# MoneroOutgoingTransfer

subaddress indices: uint[]

addresses: string[]

destinations: MoneroDestination[]

#### MoneroTxSet

txs: MoneroTxWallet[]

multisig\_tx\_hex: string

unsigned\_tx\_hex: string

signed\_tx\_hex: string

#### MoneroTxWallet extends MoneroTx

tx\_set: MoneroTxSet

incoming\_amount: ulong

outgoing\_amount: ulong

incoming\_transfers: MoneroTransfer[]

outgoing\_transfer: MoneroTransfer

note: string

is\_locked: bool

input\_sum: ulong

output\_sum: ulong

change\_address: string

change\_amount: ulong

num dummy outputs: uint

extra\_hex: string

#### MoneroSyncResult

num\_blocks\_fetched: ulong

received\_money: bool

#### MoneroWalletListener

onSyncProgress(ulong height, ulong startHeight, ulong endHeight, double percentDone, string message): void

onNewBlock(ulong height): void

onOutputReceived(MoneroOutputWallet output): void

Extends

onOutputSpent(MoneroOutputWallet output): void

# Monero Wallet Types 4/4

#### MoneroAccountTag

tag: string label: string

account\_indices: uint[]

#### MoneroMultisigInfo

is\_multisig: bool is\_ready: bool threshold: uint

num\_participants: uint

#### MoneroKeyImageImportResult

height: ulong

spent\_amount: ulong

unspent\_amount: ulong

## ${\tt MoneroAddressBookEntry}$

index: uint

address: string

description: string payment\_id: string

# Monero Mult is ig In it Result

address: string

multisig\_hex: string

## MoneroIntegratedAddress (deprecated)

standard\_address: string

payment\_id: string

integrated\_address: string

#### <<enumeration>> MoneroSendPriority

default: 0

unimportant: 1

normal: 2 elevated: 3

#### MoneroMultisigSignResult

signed\_multisig\_tx\_hex: string

tx\_hashes: string[]

spend\_key: 0

view\_key: 1

## MoneroCheck

is\_good: bool

Extends Extends

#### MoneroCheckReserve

total\_amount: ulong

unconfirmed\_spent\_amount: ulong

# MoneroCheckTx

in\_tx\_pool: bool

num\_confirmations: ulong

received\_amount: ulong

# MoneroMessageSignatureResult

<<enumeration>>  ${\tt MoneroMessageSignatureType}$ 

is\_good: bool

is\_old: bool

signature\_type: MoneroMessageSignatureType

version: int



46FR1GKVqFNQnDiFkH7AuzbUBrGQwz2VdaXTDD4jcjRE8YkkoTYTmZ2Vohsz9gLSqkj5EM6ai9Q7sBoX4FPPYJdGKQQXPVz



#### woodser

donation\_address: const string

irc: "woodser"

reddit: "XmrApiDev"

time\_committed\_to\_xmr: ulong

competing\_interests: list<?>

Motivation tends to increase with support to donation address.