Taming Monero: The Hidden Model



A Specification for

Monero Wallet and Daemon Interfaces

based on Monero Core v0.15.0.1 Carbon Chameleon

Revision 31 - December 15, 2019

Java reference implementation: https://github.com/monero-ecosystem/monero-java

JavaScript reference implementation: https://github.com/monero-ecosystem/monero-javascript

C++ reference implementation: https://github.com/woodser/monero-cpp-library

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

Document source created and modifiable using: https://www.draw.io/

Monero Daemon Interface 1/2

```
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=?): ulong
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
qetKeyImageSpentStatuses(string[] keyImages): MoneroKeyImageSpentStatus[]
getOutputs(MoneroOutput[] outputs): MoneroOutput[]
getInfo(): MoneroDaemonInfo
getSyncInfo(): MoneroDaemonSyncInfo
getHardForkInfo(): MoneroHardForkInfo
```

```
Monero Daemon Intereface 2/2
getAltChains(): MoneroAltChain[]
getAltBlockHashes(): string[]
getDownloadLimit(): uint
setDowloadLimit(uint limit): uint
resetDownloadLimit(): uint
getUploadLimit(): uint
setUploadLimit(uint): uint
resetUploadLimit(): uint
getKnownPeers(): MoneroDaemonPeer[]
getConnections(): MoneroDaemonConnection[]
setOutgoingPeerLimit(uint limit): void
setIncomingPeerLimit(uint limit): void
getPeerBans(): MoneroBan[]
setPeerBan(MoneroBan ban): void
setPeerBans(MoneroBan[] bans): void
getOutputDistribution(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
getNextBlockHeader(): MoneroBlockHeader
addListener(MoneroDaemonListener listener): void
removeListener(MoneroDaemonListener listener): void
```

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: uint

miner_tx_hash: string

num_txs: uint

orphan_status: bool

prev_hash: string

reward: ulong

pow_hash: string



MoneroBlock

hex: string

miner_tx: MoneroTx

txs: MoneroTx[]

tx_hashes: string[]

MoneroOutput

tx: MoneroTx

key_image: MoneroKeyImage

amount: ulong

index: uint

ring_output_indices: uint[]

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

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

<enumeration> MoneroNetworkType

mainnet: 0

testnet: 1

stagenet: 2

MoneroTx

block: MoneroBlock

height: ulong

hash: string

version: uint

 $is_coinbase \colon bool$

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: uint[]

metadata: string

extra: uint[]

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: ?

MoneroDaemonConnection

peer: MoneroDaemonPeer

id: string

avg_download: ulong

avg_upload: ulong

current_download: ulong

current_upload: ulong

height: ulong

is_incoming: bool

live_time: ulong

is_local_ip: bool

is_local_host: bool

num_receives: uint

num sends: uint

receive_idle_time: ulong

send_idle_time: ulong

state: string

num_support_flags: uint

type: ConnectionType

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

MoneroKeyImage

hex: string

signature: string

<enumeration>
MoneroKeyImageSpentStatus

not_spent: 0

confirmed: 1

tx_pool: 2

 ${\tt MoneroSubmitTxResult}$

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

MoneroDaemonPeer

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

MoneroBan

host: string

ip: string

is_banned: bool

seconds: ulong

 ${\tt MoneroBlockTemplate}$

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

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

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

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

```
isWatchOnly(): bool
setDaemonConnection(MoneroDaemonConnection connection): void
getDaemonConnection(): MoneroDaemonConnection
isConnected(): bool
getVersion(): MoneroVersion
getNetworkType(): MoneroNetworkType
getPath(): string
getMnemonic(): string
getMnemonicLanguage(): string
getMnemonicLanguages(): string[]
getPrivateSpendKey(): string
getPrivateViewKey(): string
getPublicSpendKey(): string
getPublicViewKey(): string
getPrimaryAddress(): string
getAddress(uint accountIdx, uint subaddressIdx): string
getAddressIndex(string address): MoneroSubaddress
getDaemonConnection(): MoneroRpcConnection
getHeight(): ulong
getDaemonHeight(): ulong
getDaemonMaxPeerHeight(): ulong
getApproximateChainHeight(): ulong
sync(ulong startHeight=null, MoneroSyncListener listener=null): MoneroSyncResult
startSyncing(): void
stopSyncing(): 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
createSubaddress(uint accountIdx, string label=null): MoneroSubaddress
getTx(string txId): MoneroTxWallet
getTxs(MoneroTxQuery query=null): MoneroTxWallet[]
getTransfers(uint accountIdx=null, uint subaddressIdx=null): MoneroTransfer[]
```

Monero Wallet Interface 2/3

```
getOutputs(MoneroOutputQuery query=null): MoneroOutputWallet[]
qetOutgoingTransfers(MoneroTransferQuery query=null): MoneroOutgoingTransfer[]
getIncomingTransfers(MoneroTransferQuery guery=null):                         MoneroIncomingTransfer[]
getTransfers(MoneroTransferQuery query=null): void
getKeyImages(): MoneroKeyImage[]
importOutputsHex(string outputsHex): uint
getOutputsHex(): string
importKeyImages(MoneroKeyImage[] keyImages): MoneroKeyImageImportResult
getNewKeyImagesFromLastImport(): MoneroKeyImage[]
createTx(MoneroSendRequest request): MoneroTxSet
createTx(uint accountIdx, string address, ulong amount): MoneroTxSet
createTxs(MoneroSendRequest request): MoneroTxSet
relayTx(string txMetadata): string
relayTx(MoneroTxWallet tx): string
relayTxs(string[] txMetadatas): string[]
relayTxs(MoneroTxWallet[] txs): string[]
send(MoneroSendRequest request): MoneroTxSet
send(uint accountIdx, string address, ulong amount): MoneroTxSet
sendSplit(MoneroSendRequest request): MoneroTxSet
sendSplit(uint accountIdx, string address, ulong amount): MoneroTxSet
sweepOutput(MoneroSendRequest request): MoneroTxSet
sweepOutput(string address, string keyImage): MoneroTxSet
sweepSubaddress(uint accountIdx, uint subaddressIdx, string address): MoneroTxSet
sweepAccount(uint accountIdx, string address): MoneroTxSet
sweepWallet(string address): MoneroTxSet[]
sweepUnlocked(MoneroSendRequest request): MoneroTxSet[]
sweepDust(bool doNotRelay=false): MoneroTxSet
parseTxSet(MoneroTxSet txSet): MoneroTxSet
signTxs(string unsignedTxHex): string
submitTxs(string signedTxHex): string[]
sign(string message): string
verify(string message, string address, string signature): bool
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, string paymentId=null): uint
editAddressBookEntry(uint entryIdx, bool setAddress, string address, bool setDescription, string description, bool setPaymentId,
          string paymentId): void
deleteAddressBookEntry(uint entryIdx): void
tagAccounts(string tag, uint[] accountIndices): void
untagAccounts(uint[] accountIndices): void
getAccountTags(): MoneroAccountTag[]
setAccountTagLabel(string tag, string label): void
createPaymentUri(MoneroSendRequest 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): MoneroMultisigInitResult
exchangeMultisigKeys(string[] multisigHexes, string password): MoneroMultisigInitResult
getMultisigHex(): string
importMultisigHex(string[] multisigHexes): uint
signMultisigTxHex(string multsiigTxHex): MoneroMultisigSignResult
submitMultisig(string signedMultisigHex): string[]
moveTo(string path, string password): void
save(): void
close(bool save=false): void
qetIntegratedAddress(string paymentId=null): MoneroIntegratedAddress (deprecated)
decodeIntegratedAddress(string integratedAddress): MoneroIntegratedAddress (deprecated)
```

Monero Wallet Types 1/3 - Send Request and Queries for Transactions, Transfers, and Outputs

MoneroSendRequest

destinations: MoneroDestination[]

payment_id: string

priority: MoneroSendPriority

fee: ulong

account_index: uint

subaddress_indices: uint[]

unlock_time: ulong

can_split: bool

do not relay: bool

note: string

recipient_name: string below_amount: ulong

sweep_each_subaddress: bool

key_image: string

Configures outgoing transfers, sweeps, and creation of payment URIs.

MoneroOutputQuery extends MoneroOutputWallet

subaddress_indices: uint[]
tx_request: MoneroTxRequest

Configures a query to get wallet outputs, allowing filtering on all output attributes and extensions.

MoneroTxQuery extends MoneroTxWallet

is_outgoing: bool
is_incoming: bool
tx_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, allowing filtering on all transaction attributes and extensions.

MoneroTransferQuery extends MoneroTransfer

is_incoming: bool
address: string

addresses: string[]

subaddress_index: uint

 $subaddress_indices:\ uint[]$

destinations: MoneroDestination[]

has_destinations: bool

tx_request: MoneroTxQuery

Configures a query to get wallet transfers, allowing filtering on all transfer attributes and extensions.

Monero Wallet Types 2/3

MoneroAccount

index: uint

primary_address: string

balance: ulong

unlocked_balance: ulong

subaddresses: MoneroSubaddress[]

tag: string

MoneroSubaddress

address: string

label: string

balance: ulong

unlocked_balance: ulong

is used: bool

MoneroDestination

address: string

amount: ulong

txs: MoneroTxWallet[]

multisig_tx_hex: string

unsigned_tx_hex: string

signed_tx_hex: string

MoneroOutputWallet extends MoneroOutput

account_index: uint

subaddress_index: uint

is_spent: bool

is_frozen: bool

tx: MoneroTxWallet

is_incoming: bool

amount: ulong

MoneroTxWallet extends MoneroTx

MoneroTxSet

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

account index: uint

index: uint

num_unspent_outputs: ulong

num_blocks_to_unlock: ulong

account index: uint

MoneroTransfer

num_suggested_confirmations: ulong

Extends

MoneroIncomingTransfer

Extends

subaddress_index: uint

address: string

MoneroOutgoingTransfer

subaddress_indices: uint[]

addresses: string[]

destinations: MoneroDestination[]

MoneroSyncResult

num_blocks_fetched: ulong

received_money: bool

MoneroSyncListener

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



MoneroWalletListener extends MoneroSyncListener

onNewBlock(ulong height): void

onOutputReceived(MoneroOutputWallet output): void

onOutputSpent(MoneroOutputWallet output): void

Monero Wallet Types 3/3

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

MoneroAddressBookEntry

index: uint

address: string

description: string

payment_id: string

 ${\bf Monero Multisig Init Result}$

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

Monero Multisig SignResult

signed_multisig_tx_hex: string

tx_hashes: string[]

MoneroCheck

is_good: bool

Extends

MoneroCheckReserve

total_amount: ulong

unconfirmed_spent_amount: ulong

MoneroCheckTx

in_tx_pool: bool

Extends

num_confirmations: ulong

received_amount: ulong



46 FR1 GKVqFNQnDiFkH7 AuzbUBrGQwz2VdaXTDD4jcjRE8YkkoTYTmZ2Vohsz9gLSqkj5 EM6ai9Q7sBoX4FPPYJdGKQQXPVzBoX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBoX4FPPYJdGKQQXPQXBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGKQQXPVZBOX4FPPYJdGCAYAFPPYJdCAYAFPPYJdCAYAFPPYJdCAYAFPPYJdCAYAFPPYJdCAYAFPPYJdCAYAFPPYJdCAYAFPPYJdCAYAFPPYJdCAYAFPPYTGAYAFPTAYAFPYTGAYAFPTAYAFTAYAFPTAYAFPTAYAFPTAYAFPTAYAFPTAYAFPTAYAF



woodser

donation_address: const string

irc: "woodser"

reddit: "XmrApiDev"

time_committed_to_xmr: ulong

competing_interests: list<?>

Motivation tends to increase with support shown to donation address.