Dismiss

Join GitHub today

GitHub is home to over 40 million developers working together to host and review code, manage projects, and build software together.

Sign up

quentinlesceller Fix doc typo (#2303) 8e4c367 on 6 Jan

1 contributor

184 lines (144 sloc) 9.36 KB Raw Blame History

Wallet Foreign API Documentation

Table of Contents

Wallet Foreign Endpoint

POST Build Coinbase

Creates a coinbase output for the given height and block fees

- **URL**

  /v1/wallet/foreign/build_coinbase

- **Method:**

  `POST`

- **URL Params**

  None

- **Data Params**

```
{
    "fees": x,
    "height":y,
}
```

  Required: `fees=[number]` `height=[number]`

- **Success Response:**

  - **Code:** 200

  - **Content:**

Field	Type	Description

Field	Type	Description
output	string	Output
kernel	string	Kernel
key_id	string	Key identifier

- **Error Response:**
  - **Code:** 400
- **Sample Call:**

```
var coinbase_data = {
  fees: 0,
  height: 123456
}
$.ajax({
  url: "/v1/wallet/foreign/build_coinbase",
  dataType: "json",
  type : "POST",
  success : function(r) {
    console.log(r);
  },
  data: JSON.stringify(coinbase_data)
});
```

POST Receive Tx

Receives a transaction, modifying the slate accordingly (which can then be sent back to sender for posting)

- **URL**

/v1/wallet/foreign/receive_tx

- **Method:**

  `POST`

- **URL Params**

  None

- **Data Params**

  Required: A transaction slate in JSON.

Field	Type	Description
num_participants	number	The number of participants intended to take part in this transaction
id	number	Unique transaction ID, selected by sender
tx	object	The core transaction data (inputs, outputs, kernels and kernel offset)
- offset	[]number	The kernel "offset" k2, excess is k1G after splitting the key k = k1 + k2
- body	object	The transaction body - inputs/outputs/kernels
- - inputs	[]object	List of inputs spent by the transaction
- - - features	object	The features of the output being spent
- - - - bits	number	Representation of the features in bits
- - - commit	[]number	The commit referencing the output being spent
- - outputs	[]object	List of outputs the transaction produces

Field	Type	Description
- - - features	object	Options for an output's structure or use
- - - - bits	number	Representation of the features in bits
- - - commit	[]number	The homomorphic commitment representing the output amount
- - - proof	[]number	A proof that the commitment is in the right range
- - kernels	[]object	List of kernels that make up this transaction (usually a single kernel)
- - - features	object	Options for a kernel's structure or use
- - - - bits	number	Representation of the features in bits
- - - fee	number	Fee originally included in the transaction this proof is for
- - - lock_height	number	The max lock_height of all inputs to this transaction
- - - excess	[]number	Remainder of the sum of all transaction commitments
- - - excess_sig	[]number	The signature proving the excess is a valid public key (signs the tx fee)
amount	number	Base amount (excluding fee)
fee	number	Fee amount
height	number	Block height for the transaction
lock_height	number	Lock height
participant_data	object	Participant data
- id	number	Id of participant in the transaction. (For now, 0=sender, 1=rec)

Field	Type	Description
- public_blind_excess	[]number	Public key corresponding to private blinding factor
- public_nonce	[]number	Public key corresponding to private nonce
- part_sig	[]number	Public partial signature

Note on participant data: each participant in the transaction will insert their public data here. For now, 0 is sender and 1 is receiver, though this will change for multi-party transactions.

- **Success Response:**
  - **Code:** 200
  - **Content:** A new transaction slate in JSON.

Field	Type	Description
num_participants	number	The number of participants intended to take part in this transaction
id	number	Unique transaction ID, selected by sender
tx	object	The core transaction data (inputs, outputs, kernels and kernel offset)
- offset	[]number	The kernel "offset" k2, excess is k1G after splitting the key k = k1 + k2
- body	object	The transaction body - inputs/outputs/kernels
- - inputs	[]object	List of inputs spent by the transaction

Field	Type	Description
- - - features	object	The features of the output being spent
- - - - bits	number	Representation of the features in bits
- - - commit	[]number	The commit referencing the output being spent
- - outputs	[]object	List of outputs the transaction produces
- - - features	object	Options for an output's structure or use
- - - - bits	number	Representation of the features in bits
- - - commit	[]number	The homomorphic commitment representing the output amount
- - - proof	[]number	A proof that the commitment is in the right range
- - kernels	[]object	List of kernels that make up this transaction (usually a single kernel)
- - - features	object	Options for a kernel's structure or use
- - - - bits	number	Representation of the features in bits
- - - fee	number	Fee originally included in the transaction this proof is for
- - - lock_height	number	The max lock_height of all inputs to this transaction
- - - excess	[]number	Remainder of the sum of all transaction commitments
- - - excess_sig	[]number	The signature proving the excess is a valid public key (signs the tx fee)
amount	number	Base amount (excluding fee)
fee	number	Fee amount

Field	Type	Description
height	number	Block height for the transaction
lock_height	number	Lock height
participant_data	object	Participant data
- id	number	Id of participant in the transaction. (For now, 0=sender, 1=rec)
- public_blind_excess	[]number	Public key corresponding to private blinding factor
- public_nonce	[]number	Public key corresponding to private nonce
- part_sig	[]number	Public partial signature

- **Error Response:**
  - **Code:** 400
- **Sample Call:**

```
$.ajax({
  url: "/v1/wallet/foreign/receive_tx",
  dataType: "json",
  type : "POST",
  success : function(r) {
    console.log(r);
  },
  data: {
    file: tx.json
  },
});
```