Electrum Protocol

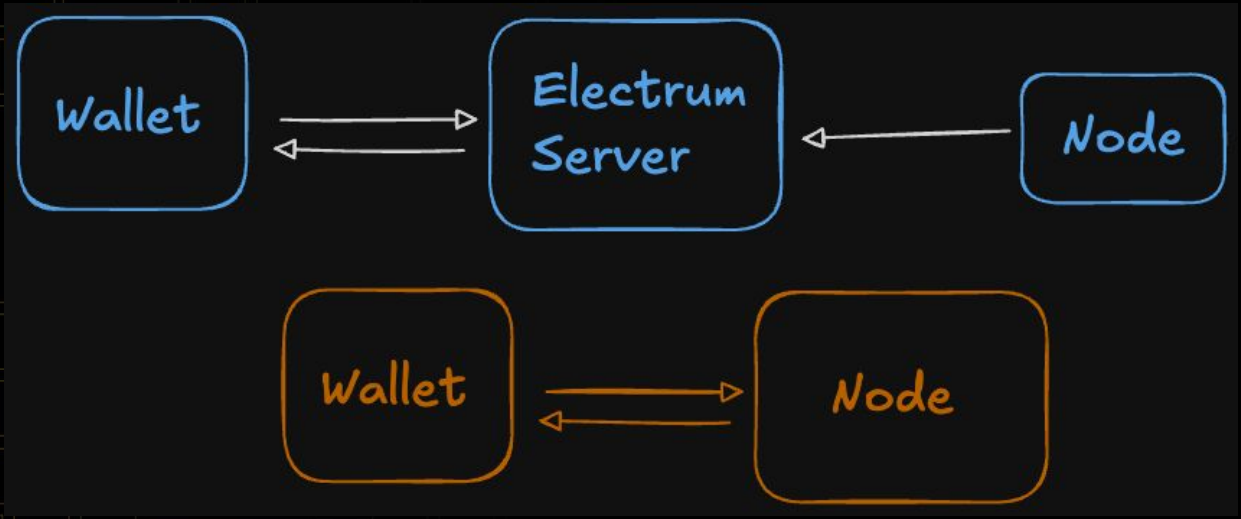
What is Electrum Protocol?

- The Electrum Protocol is a client-server JSON-RPC protocol. The primary use case is a light self-custodial Bitcoin wallet keeping track of its onchain history.

Key-ideas

- What? → Client-Server Protocol
- Why? → Interact with a node
- How? → Json RPC

How to keep track of wallet addresses?



JSON-RPC 2.0

- Javascript Object Notation
- Remote Procedure Call
- RFC 4627

Syntax:

```
--> data sent to Server
<-- data sent to Client
```

rpc call with positional parameters:

```
--> {"jsonrpc": "2.0", "method": "subtract", "params": [42, 23], "id": 1}
<-- {"jsonrpc": "2.0", "result": 19, "id": 1}

--> {"jsonrpc": "2.0", "method": "subtract", "params": [23, 42], "id": 2}
<-- {"jsonrpc": "2.0", "result": -19, "id": 2}
```

rpc call with named parameters:

```
--> {"jsonrpc": "2.0", "method": "subtract", "params": {"subtrahend": 23, "minuend": 42}, "id": 3}
<-- {"jsonrpc": "2.0", "result": 19, "id": 3}

--> {"jsonrpc": "2.0", "method": "subtract", "params": {"minuend": 42, "subtrahend": 23}, "id": 4}
<-- {"jsonrpc": "2.0", "result": 19, "id": 4}
```

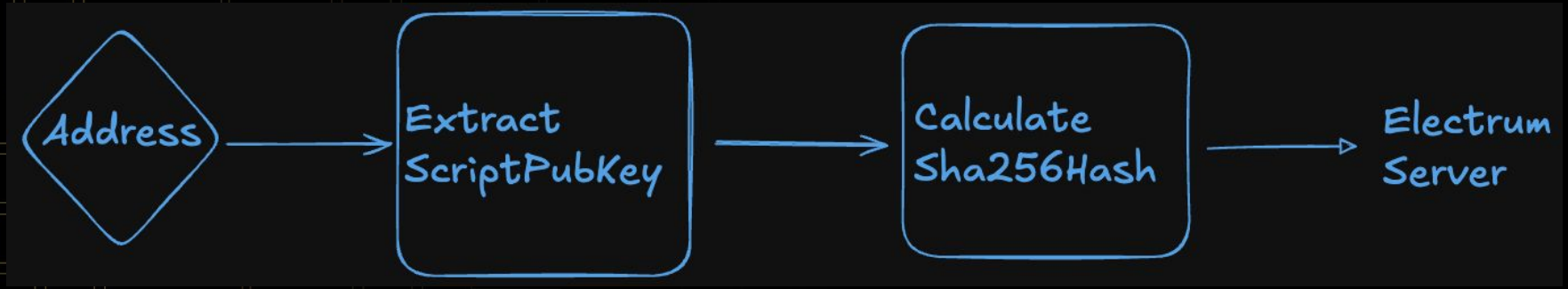
a Notification:

```
--> {"jsonrpc": "2.0", "method": "update", "params": [1,2,3,4,5]}
--> {"jsonrpc": "2.0", "method": "foobar"}
```

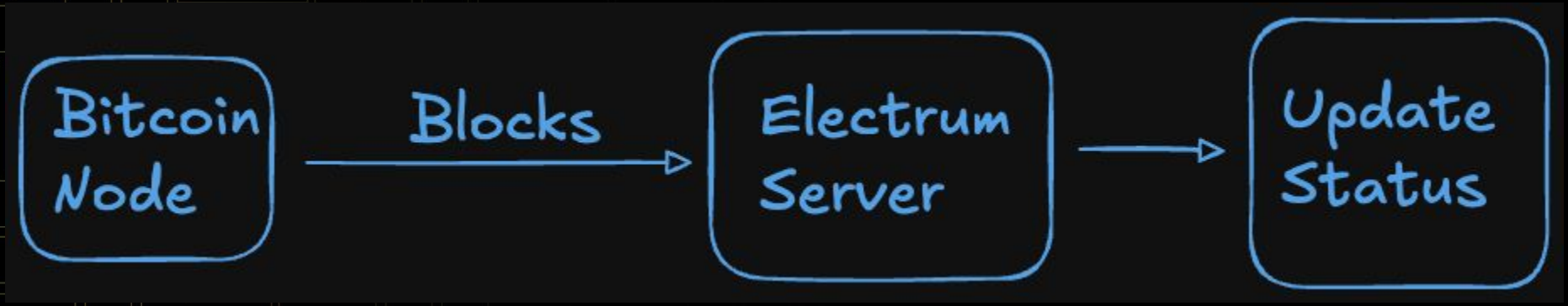
rpc call of non-existent method:

```
--> {"jsonrpc": "2.0", "method": "foobar", "id": "1"}
<-- {"jsonrpc": "2.0", "error": {"code": -32601, "message": "Method not found"}, "id": "1"}
```

Script Hashes



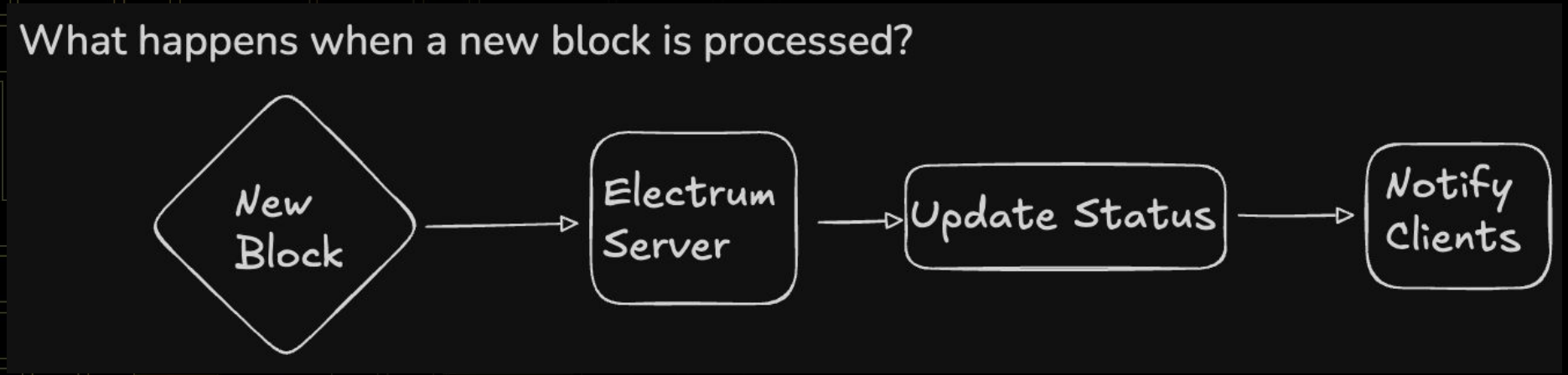
Status



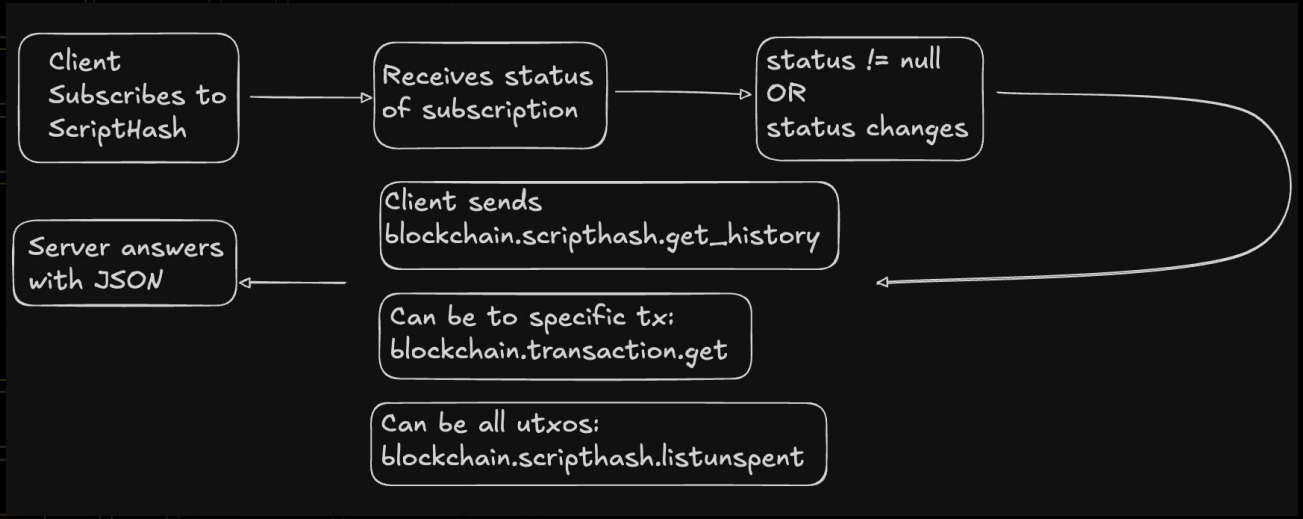
Status


STATUS OF A SCRIPT HASH:
sha256
hex_string
tx1_hash:height100 || tx2_hash:height112...

Status


What happens when a new block is processed?
New Block
Electrum Server
Update Status
Notify Clients

Example


Client Subscribes to ScriptHash
Receives status of subscription
status != null OR status changes
Client sends blockchain.scripthash.get_history
Server answers with JSON
Can be to specific tx: blockchain.transaction.get
Can be all utxos: blockchain.scripthash.listunspent

Next Presentation:

How does it work on Floresta?

Obrigado.

Learn more:

vinteum