anyblock.tools Documentation

Anyblock Analytics GmbH

Jan 16, 2020

Documentation Contents:

Anyblock.tools is a hosted Ethereum API providing sophisticated support to search, filter and aggregate events from multiple Ethereum based blockchains. It is based on Elasticsearch and PostgreSQL.

Constructing a query and understanding what the anyblock.tools server returns is the most important skill you need in order to get started with anyblock.tools.

If you are new to **ElasticSearch** and / or the **anyblock.tools API**, you first should:

- Inform yourself about the *authorization* methods
- Read our *elastic developer tutorial*
- Familiarise yourself with the Elasticsearch Query DSL.
- Understand the elastic-schema and how events are *mapped*
- Leverage our *example queries* and build your own queries.

You might also want to take a look at our **SQL** interface:

- Check the *sql-access* to our database
- Maybe start with looking at the *entity-relation model*
- To get a quickstart on how to use the interface you should see the *sql tutorial*

You may also find here help for our **ALERTING** dashboard:

- Visit *alerting* to understand how our alerting works
- Contact us to get access to the alerting feature

Please also visit our main Website and get in touch. We're always interested in what you're BUIDLing.

CHAPTER 1

API

1.1 Authorization

To access anyblock.tools, no matter if you just want to use the free service or have a paid service agreement, you'll need to get an API Key.

You can register for a **free** account and get an API key right now at https://account.anyblock.tools/ in just a few seconds. Go ahead, I'll wait.

1.1.1 Sending your API key

Authorization Bearer Header

The fastest and most secure way to send your API key is via the *Authorization* header

```
curl -X GET https://api.anyblock.tools/status/ -H 'Authorization: Bearer $mytoken'
```

Basic Auth

For compatibility reasons it's also possible to send the API key as your password via Basic Auth

```
curl -X GET https://api.anyblock.tools/status/ -u '$myemail:$mytoken'
```

Please keep in mind that you're supposed to send your **API key**, not your password here.

Query Parameter

This is by far the least secure option, because your API key may end up in all sorts of logfiles and will even be visible to network sniffers. Only use the query parameter with short lived API keys for demonstration purposes.

```
curl -X GET 'https://api.anyblock.tools/status/?access_token=$mytoken'
```

1.1.2 API key security

At the time of this writing there are two mechanisms in place to secure API access to your account.

Lifetime

When creating a new API key you can select a future date at which the key will no longer work. For most applications it's obviously not reasonable to switch the API key every few days, so you can create a long lived key and keep it a secret, while you may use a key with only a few days of validity for demos and other public use cases.

Domain

In case you want to use your API key in an environment where it's necessary to expose it to your intended audience (say, a website), you can additionally secure the API key with an allowed domain name. The key will then only work, if the referrer of the request matches the configured domain.

1.1.3 Why bother?

In the end this is a free service and anyone can get an API key anyways, so why all the hassle?

Well, for one we're going to use the API keys to restrict access to certain semi-private data, but mostly it's to control abuse to some extent.

We're monitoring the amount of requests and used data per account and in case your usage is **way** above *normal usage* we'll warn you and eventually disable your account.

In this case it would be a shame if some stranger on the internet just hijacked your API key.

1.2 Index endpoints

When interacting with the anyblock.tools API, the base URL structure is always as follows:

/$technology/$blockchain/$network/$interface/...

The first triple of *technology*, *blockchain* and *network* describes the network you want to interact with. For most users this would be **/ethereum/ethereum/mainnet/**, which is also the default and can be omitted. Other possible values would be for example */ethereum/classic/morden/*.

The fourth part is the search interface you want to use. Currently only the ElasticSearch interface **/es/** is supported, but we're already working on SQL and GraphQL support.

So, for most users the base URL will be

```
https://api.anyblock.tools/ethereum/ethereum/mainnet/es/
```

CHAPTER 2

ElasticSearch

Following the search interface, you can select the resource you want to query. Possible values are

- *block*
- *tx*
- *log*
- *event*
- *call*

which already reflects the type parameter of the ElasticSearch query syntax.

For obvious reasons we're limiting the full scope of the ElasticSearch Query DSL, but the following APIs will work as expected:

- *search*
- *_search*
- *count*
- *_count*

It's also possible to explicitly provide the desired index in the URL which follows the format **$technology-$blockchain-$network-$resource**. This is completely optional but required for ElasticSearch client compatibility and is normally derrived from the selected network and resource, but must match the network and resource if present.

A simple query for the latest block would look like this:

```
https://api.anyblock.tools/es/block/search
```

2.1 ElasticSearch Clients

In order to use a default ElasticSearch client, you can provide the following parameters:

- **server**: *https://api.anyblock.tools/ethereum/ethereum/mainnet/es/*
- **index**: *ethereum-ethereum-mainnet-block*
- **type**: *block*
- **username**: *your email address*
- **password**: *your API key*

The following example shows how to fetch the latest 5 DAI transfers from ElasticSearch in Node.js

```
const Client = require('elasticsearch').Client

const esClient = new Client({
  hosts: 'https://api.anyblock.tools/ethereum/ethereum/mainnet/es/',
  httpAuth: 'your-email-address:your-api-key',
})

esClient.search({
  index: 'ethereum-ethereum-mainnet-event',
  type: 'event',
  body: {
    query: {
      bool: {
        filter: [
          {
            term: {
              'address.raw': '0x89d24A6b4CcB1B6fAA2625fE562bDD9a23260359'
            }
          },
          {
            term: {
              'event.raw': 'Transfer'
            }
          }
        ]
      }
    },
    sort: {
      timestamp: 'desc'
    },
    size: 5
  }
})
.then(result => console.log(require('util').inspect(result, { depth: null })))
.catch(err => console.error(err))
```

2.2 ElasticSearch Data Structure

The following chapters will document the available entities and explain it's property structure.

2.2.1 Block

Object schema

The block object inherits it's properties from the web3 API:

- *number*: *Number* - the block number.
- *hash*: *String* - hash of the block.
- *parentHash*: *String* - hash of the parent block.
- *nonce*: *String* - hash of the generated proof-of-work.
- *sha3Uncles*: *String* - SHA3 of the uncles data in the block.
- *logsBloom*: *String* - the bloom filter for the logs of the block.
- *transactionsRoot*: *String*- the root of the transaction trie of the block
- *stateRoot*: *String* - the root of the final state trie of the block.
- *miner*: *String* - the address of the beneficiary to whom the mining rewards were given.
- *difficulty*: *BigNumber* - integer of the difficulty for this block.
- *totalDifficulty*: *BigNumber* - integer of the total difficulty of the chain until this block.
- *extraData*: *String* - the "extra data" field of this block.
- *size*: *Number* - integer the size of this block in bytes.
- *gasLimit*: *Number* - the maximum gas allowed in this block.
- *gasUsed*: *Number* - the total used gas by all transactions in this block.
- *timestamp*: *Number* - the unix timestamp for when the block was collated.
- *transactions*: *Array* - Array of transaction hashes
- *uncles*: *Array* - Array of uncle hashes.

Mapping

For some fields, there are multiple encodings available, which are nested as properties on the field. More information on those data types can be found *here*.

The following is the output of the Elasticsearch mapping for the *Block* type:

```
{
  "difficulty": {
    "properties": {
      "padded": {
        "type": "keyword",
        "ignore_above": 256
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "extraData": {
    "type": "keyword",
    "ignore_above": 256
```

(continues on next page)

(continued from previous page)

```
  },
  "gasLimit": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "gasUsed": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "hash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "step": {
    "type": "keyword",
    "ignore_above": 256
  },
  "signature": {
    "type": "keyword",
    "ignore_above": 256
  },
  "logsBloom": {
    "type": "keyword",
    "ignore_above": 256
  },
  "miner": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "nonce": {
    "type": "keyword",
    "ignore_above": 256
  },
  "mixHash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "number": {
```

(continues on next page)

(continued from previous page)

```
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "parentHash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "receiptsRoot": {
    "type": "keyword",
    "ignore_above": 256
  },
  "sha3Uncles": {
    "type": "keyword",
    "ignore_above": 256
  },
  "size": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "stateRoot": {
    "type": "keyword",
    "ignore_above": 256
  },
  "timestamp": {
    "type": "date",
    "format": "epoch_second"
  },
  "totalDifficulty": {
    "properties": {
      "padded": {
        "type": "keyword",
        "ignore_above": 256
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "transactionsRoot": {
    "type": "keyword",
    "ignore_above": 256
  },
```

(continues on next page)

(continued from previous page)

```
  "uncles": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "sealFields": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  }
}
```

2.2.2 Transaction

Object schema

The *tx* object inherits it's properties from the transaction object, as specified in the web3 API:

- *from*: *String* - The address for the sending account. Uses the web3.eth.defaultAccount property, if not specified.
- *to*: *String* - (optional) The destination address of the message, left undefined for a contract-creation transaction.
- *value*: *Number|String|BigNumber* - (optional) The value transferred for the transaction in Wei, also the endowment if it's a contract-creation transaction.
- *gas*: *Number|String|BigNumber* - (optional) The amount of gas to use for the transaction (unused gas is refunded).
- *gasPrice*: *Number|String|BigNumber* - (optional) The price of gas for this transaction in wei, defaults to the mean network gas price.
- *data*: *String* - (optional) Either a byte string containing the associated data of the message, or in the case of a contract-creation transaction, the initialisation code.
- *nonce*: *Number* - (optional) Integer of a nonce. This allows to overwrite your own pending transactions that use the same nonce.

Mapping

For some fields, there are multiple encodings available, which are nested as properties on the field. More information on those data types can be found *here*.

The following is the output of the Elasticsearch mapping for the *Transaction* type:

```
{
  "blockHash": {
    "type": "keyword",
    "ignore_above": 256
```

(continues on next page)

(continued from previous page)

```
  },
  "blockNumber": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "contractAddress": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "cumulativeGasUsed": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "from": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "gas": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "gasPrice": {
    "properties": {
      "num": {
        "type": "long"
      },
```

(continues on next page)

(continued from previous page)

```
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "gasUsed": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "hash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "publicKey": {
    "type": "keyword",
    "ignore_above": 256
  },
  "creates": {
    "type": "keyword",
    "ignore_above": 256
  },
  "input": {
    "type": "keyword",
    "ignore_above": 256
  },
  "logsBloom": {
    "type": "keyword",
    "ignore_above": 256
  },
  "nonce": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "r": {
    "type": "keyword",
    "ignore_above": 256
  },
  "root": {
    "type": "keyword",
    "ignore_above": 256
  },
  "s": {
```

(continues on next page)

(continued from previous page)

```
    "type": "keyword",
    "ignore_above": 256
  },
  "status": {
    "type": "boolean"
  },
  "timestamp": {
    "type": "date",
    "format": "epoch_second"
  },
  "to": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "transactionIndex": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "v": {
    "type": "keyword",
    "ignore_above": 256
  },
  "value": {
    "properties": {
      "num": {
        "type": "long"
      },
      "eth": {
        "type": "double"
      },
      "padded": {
        "type": "keyword",
        "ignore_above": 256
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  }
}
```

2.2.3 Log

Object schema

The *log* object inherits it's properties from the web3 API:

- *logIndex*: *Number* - integer of the log index position in the block.
- *transactionIndex*: *Number* - integer of the transactions index position log was created from.
- *transactionHash*: *String*- hash of the transactions this log was created from.
- *blockHash*: *String* - hash of the block where this log was in. *null* when its pending.
- *blockNumber*: *Number* - the block number where this log was in. *null* when its pending.
- *address*: *String* - address from which this log originated.
- *data*: *String* - contains one or more non-indexed arguments of the log.
- *topics*: *Array of hex strings* - Array of indexed log arguments.

Mapping

For some fields, there are multiple encodings available, which are nested as properties on the field. More information on those data types can be found *here*.

Note: For example the *address* is stored using the format *raw (text stored as keyword)* described on the datatypes page. In that particular case, the checksum-case formatted address can be used as a term filter query using *address.raw* and for a case-insensitive query, use *address*.

The following is the output of the Elasticsearch mapping for the *Log* type:

```
{
  "address": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "blockHash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "id": {
    "type": "keyword",
    "ignore_above": 256
  },
  "blockNumber": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
```

(continues on next page)

(continued from previous page)

```
  "data": {
    "type": "keyword",
    "ignore_above": 256
  },
  "logIndex": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "type": {
    "type": "keyword",
    "ignore_above": 256
  },
  "timestamp": {
    "type": "date",
    "format": "epoch_second"
  },
  "topics": {
    "type": "keyword",
    "ignore_above": 256
  },
  "transactionHash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "transactionIndex": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  }
}
```

2.2.4 Event

Object schema

- *address*: *String*- address from which this event originated.
- *args*: *Array* - Array of argument objects coming from that event.
- *blockHash*: *String* - hash of the block where this event was in.
- *blockNumber*: *Number* - the block number where this event was in.
- *logIndex*: *Number* - integer of the event index position in the block.

- *event*: *String* - The event name.
- *transactionIndex*: *Number* - integer of the transactions index position event was created from.
- *transactionHash*: *String*- hash of the transactions this event was created from.
- *probability*: *Float* - the truthness of this event. 1.0 is the best.

Event arguments

The event's arguments with it's corresponding values are located in an object representation in an array of arguments. This allows different events to have different types and numbers of arguments.

The argument object's structure:

- *name* - the argument's name in human readable form
- *pos* - the index of the argument's position in the event
- *value.hex*,'value.scaled', *value.num* - the value of the events argument in it's corresponding representation
- *value.type* - the type of the argument's value, can be any type as specified for Solidity

Mapping

For some fields, there are multiple encodings available, which are nested as properties on the field. More information on those data types can be found *here*.

Note: For example the *address* is stored using the format *raw (text stored as keyword)* described on the datatypes page. In that particular case, the checksum-case formatted address can be used as a term filter query using *address.raw* and for a case-insensitive query, use *address*.

The following is the output of the Elasticsearch mapping for the *Event* type:

```
{
  "address": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "args": {
    "type": "nested",
    "properties": {
      "name": {
        "type": "keyword",
        "ignore_above": 256
      },
      "pos": {
        "type": "long"
      },
      "value": {
        "properties": {
          "hex": {
            "type": "keyword",
            "ignore_above": 256
```

(continues on next page)

(continued from previous page)

```
          },
          "num": {
            "type": "long"
          },
          "scaled": {
            "type": "double"
          },
          "type": {
            "type": "keyword",
            "ignore_above": 256
          }
        }
      }
    }
  },
  "probability": {
    "type": "double"
  },
  "blockHash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "blockNumber": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "logIndex": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "event": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "timestamp": {
    "type": "date",
    "format": "epoch_second"
  },
```

(continues on next page)

(continued from previous page)

```
  "transactionHash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "transactionIndex": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  }
}
```

2.2.5 Call

Object schema

- *from*: *String* - The address for the sending account. Uses the web3.eth.defaultAccount property, if not specified.
- *to*: *String* - (optional) The destination address of the message, left undefined for a contract-creation transaction.
- *blockNumber*: *Number* - the block number.
- *hash*: *String* - hash of the transaction.
- *blockHash*: *String* - hash of the block.
- *method*: *String* - name of the method that was called during the transaction.
- *probability*: *Float* - the truthness of this call. 1.0 is the best.

Call arguments

The transaction call's arguments with it's corresponding input values are located in an object representation in an array of arguments. This allows different calls to have different types and numbers of arguments.

The argument object's structure:

- *name* - the argument's name in human readable form
- *pos* - the index of the argument's position in the call
- *value.hex*,'value.scaled', *value.num* - the value of the calls argument in it's corresponding representation
- *value.type* - the type of the argument's value, can be any type as specified for Solidity

Mapping

For some fields, there are multiple encodings available, which are nested as properties on the field. More information on those data types can be found *here*.

The following is the output of the Elasticsearch mapping for the *Call* type:

```
{
  "args": {
    "type": "nested",
    "properties": {
      "name": {
        "type": "keyword",
        "ignore_above": 256
      },
      "pos": {
        "type": "long"
      },
      "value": {
        "properties": {
          "hex": {
            "type": "keyword",
            "ignore_above": 256
          },
          "num": {
            "type": "long"
          },
          "scaled": {
            "type": "double"
          },
          "type": {
            "type": "keyword",
            "ignore_above": 256
          }
        }
      }
    }
  },
  "blockHash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "blockNumber": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "from": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "to": {
    "type": "text",
```


(continues on next page)

(continued from previous page)

```
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "transactionIndex": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "probability": {
    "type": "double"
  },
  "timestamp": {
    "type": "date",
    "format": "epoch_second"
  },
  "hash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "method": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "status": {
    "type": "boolean"
  }
}
```

2.2.6 Contract

Object schema

- *address*: *String*- address of the deployed contract.
- *abi*: *String* - the application binary interface of the deployed contract, formatted in JSON.
- *probability*: *Float* - the truthness of this contract information. 1.0 is the best.

Mapping

For some fields, there are multiple encodings available, which are nested as properties on the field. More information on those data types can be found *here*.

The following is the output of the Elasticsearch mapping for the *Contract* type:

```
{
  "address": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "abi": {
    "type": "binary"
  },
  "name": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "runs": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "bytecodeLsh": {
    "type": "keyword",
    "ignore_above": 256
  },
  "bytecodeHash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "bytecode": {
    "type": "binary"
  },
  "source": {
    "type": "binary"
  },
  "compiler": {
    "type": "keyword"
  },
  "library": {
```

(continues on next page)

(continued from previous page)

```
    "type": "keyword"
  },
  "createdAt": {
    "type": "date",
    "format": "epoch_second"
  },
  "updatedAt": {
    "type": "date",
    "format": "epoch_second"
  },
  "optimizations": {
    "type": "boolean"
  },
  "probability": {
    "type": "double"
  },
  "links": {
    "type": "nested",
    "properties": {
      "description": {
        "type": "text",
        "fields": {
          "raw": {
            "type": "keyword",
            "ignore_above": 256
          }
        }
      },
      "link": {
        "type": "keyword"
      }
    }
  },
  "constructorArgs": {
    "type": "nested",
    "properties": {
      "name": {
        "type": "keyword",
        "ignore_above": 256
      },
      "pos": {
        "type": "long"
      },
      "value": {
        "properties": {
          "hex": {
            "type": "keyword",
            "ignore_above": 256
          },
          "num": {
            "type": "long"
          },
          "scaled": {
            "type": "double"
          },
          "type": {
            "type": "keyword",
```

(continues on next page)

(continued from previous page)

```
            "ignore_above": 256
          }
        }
      }
    }
  }
}
```

2.2.7 Token

Object schema

- *address*: *String*- address of the deployed contract.
- *name*: *String* - a human readable name for the contract.
- *symbol*: *String* - the currency symbol of the contract.
- *totalSupply*: *Number* - the total supply of shared value for the currency.
- *links*: *Array* - an array of weblinks with description and link.
- *probability*: *Float* - the truthness of this token information. 1.0 is the best.

Mapping

For some fields, there are multiple encodings available, which are nested as properties on the field. More information on those data types can be found *here*.

The following is the output of the Elasticsearch mapping for the *Token* type:

```
{
  "address": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "symbol": {
    "type": "keyword",
    "ignore_above": 256
  },
  "name": {
    "type": "text",
    "fields": {
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "type": {
```

(continues on next page)

(continued from previous page)

```
    "type": "keyword",
    "ignore_above": 256
  },
  "decimals": {
    "type": "long"
  },
  "totalSupply": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "createdAt": {
    "type": "date",
    "format": "epoch_second"
  },
  "updatedAt": {
    "type": "date",
    "format": "epoch_second"
  },
  "links": {
    "type": "nested",
    "properties": {
      "description": {
        "type": "text",
        "fields": {
          "raw": {
            "type": "keyword",
            "ignore_above": 256
          }
        }
      },
      "link": {
        "type": "keyword"
      }
    }
  },
  "probability": {
    "type": "double"
  }
}
```

2.2.8 Trace

Object schema

The *trace* object inherits it's properties from the parity replay transaction object, as specified in the parity API:

Mapping

For some fields, there are multiple encodings available, which are nested as properties on the field. More information on those data types can be found *here*.

The following is the output of the Elasticsearch mapping for the *Trace* type:

```
{
  "blockHash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "blockNumber": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "transactionIndex": {
    "properties": {
      "num": {
        "type": "long"
      },
      "raw": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "transactionHash": {
    "type": "keyword",
    "ignore_above": 256
  },
  "timestamp": {
    "type": "date",
    "format": "epoch_second"
  },
  "output": {
    "type": "keyword",
    "ignore_above": 256
  },
  "trace": {
    "type": "nested",
    "properties": {
      "type": {
        "type": "keyword",
        "ignore_above": 256
      },
      "error": {
        "type": "keyword",
        "ignore_above": 256
      },
      "traceAddress": {
```

(continues on next page)

(continued from previous page)

```
        "type": "long"
      },
      "action": {
        "type": "nested",
        "properties": {
          "callType": {
            "type": "keyword",
            "ignore_above": 256
          },
          "init": {
            "type": "keyword",
            "ignore_above": 256
          },
          "balance": {
            "type": "keyword",
            "ignore_above": 256
          },
          "from": {
            "type": "text",
            "fields": {
              "raw": {
                "type": "keyword",
                "ignore_above": 256
              }
            }
          },
          "address": {
            "type": "text",
            "fields": {
              "raw": {
                "type": "keyword",
                "ignore_above": 256
              }
            }
          },
          "refundAddress": {
            "type": "text",
            "fields": {
              "raw": {
                "type": "keyword",
                "ignore_above": 256
              }
            }
          },
          "to": {
            "type": "text",
            "fields": {
              "raw": {
                "type": "keyword",
                "ignore_above": 256
              }
            }
          },
          "gas": {
            "properties": {
              "num": {
                "type": "long"
```

(continues on next page)

(continued from previous page)

```
            },
            "raw": {
              "type": "keyword",
              "ignore_above": 256
            }
          }
        },
        "input": {
          "type": "keyword",
          "ignore_above": 256
        },
        "value": {
          "properties": {
            "num": {
              "type": "long"
            },
            "raw": {
              "type": "keyword",
              "ignore_above": 256
            }
          }
        }
      }
    },
    "result": {
      "type": "nested",
      "properties": {
        "gasUsed": {
          "properties": {
            "num": {
              "type": "long"
            },
            "raw": {
              "type": "keyword",
              "ignore_above": 256
            }
          }
        },
        "address": {
          "type": "text",
          "fields": {
            "raw": {
              "type": "keyword",
              "ignore_above": 256
            }
          }
        },
        "code": {
          "type": "keyword",
          "ignore_above": 256
        },
        "output": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    }
```

(continues on next page)

(continued from previous page)

```
        }
    }
}
```

2.3 Data types

2.3.1 Elasticsearch types

All the types from the blockchain as well as their encodings have to be represented with a Elasticsearch type for indexing and searching. Most blockchain types that are no number types are represented as a string in Elasticsearch (*keyword* or *text* type).

To learn more about the types in Elasticsearch, visit their documentation.

2.3.2 Anyblock.tools encoded types

This are the types that represent a value on the blockchain. For some values, there are alternative encodings available.

raw

The raw value as read by the ethereum node used for indexing. This corresponds to the normal type as defined in the *web3 API*. Implemented as a *keyword* type in Elasticsearch.

scaled

A double floating point number that directly represents the ether value. Due to rounding this is not as accurate as using the *raw* or *padded* value directly. Implemented as a *double* type in Elasticsearch.

padded

A hexadecimal data type, where the hex string is padded to the biggest possible value. This allows e.g. for string sorting of big integer fields Implemented as a *keyword* type in Elasticsearch.

num

An integer representation of a value. *num* values are only accessible for integers that fit within the *long* type of Elasticsearch (64bit). BigInteger blockchain types (e.g. *uint256*) are only accessible from the *hex* representation Implemented as a *long* type in Elasticsearch.

hex

A hex string, representing the hex encoding of a value. This also includes hex encodings of BigInteger blockchain types (e.g. *uint256*), since they are not accessible from a *num* type. Implemented as a *keyword* type in Elasticsearch.

raw (text stored as keyword)

An explicit property that makes the *keyword* Elasticsearch type of a string accessible, when the default value is of type *text*. This is useful for allowing literal searches instead of pattern matching text searches. Implemented as a *keyword* type in Elasticsearch.

2.4 Example queries

The following queries are meant to be a building block for your own anyblock.tools queries.

You also will need a registered anyblock.tools API-Account in order to run the REST calls. Keep in mind to replace the `$mytoken` variable in the `cURL` commands with your personal API token.

2.4.1 Block

Get block by blockhash

The results will contain only the block with the given block *number*. This requires no body.

```
GET /ethereum/ethereum/mainnet/es/block/
↪0xf44f60a66257d1c6c8afd2a64aaeb306d9c471d5d38b6dc277811455192ecee1/
```

Select by block number

The results will contain only number selected with the given term.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/block/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "filter": {
        "term": {
          "number.num": 6600000
        }
      }
    }
  },
  "_source": ["number.num"]
}
```

Execute the request with cURL:

```
curl -X POST \
https://api.anyblock.tools/ethereum/ethereum/mainnet/es/block/search/ \
-H 'Authorization: Bearer $mytoken' \
-H 'Content-Type: application/json' \
-d '{
  "query": {
    "bool": {
      "filter": {
        "term": {
          "number.num": 6600000
        }
      }
    }
  },
  "_source": ["number.num"]
}'
```

Filter last 5 known blocks (sorted)

The results will only contain the 5 most recent blocks (highest block number) on the index. Sorted in descending order (highest block number first).

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/block/search/
```

JSON body:

```
{
  "sort": {
    "number.num": "desc"
  },
```

(continues on next page)

(continued from previous page)

```
  "size": 5
}
```

Execute the request with cURL:

```
curl -X POST \
https://api.anyblock.tools/ethereum/ethereum/mainnet/es/block/search/ \
-H 'Authorization: Bearer $mytoken' \
-H 'Content-Type: application/json' \
-d '{
  "sort": {
    "number.num": "desc"
  },
  "size": 5
}'
```

2.4.2 Transaction

Filter by the transaction's block's hash

The results will contain all transactions that are included in the specified block, identified with it's *blockHash*.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/tx/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "term": {
            "blockHash":
↪"0x4e3a3754410177e6937ef1f84bba68ea139e8d1a2258c5f85db9f1cd715a1bdd"
          }
        }
      ]
    }
  },
  "size": 200
}
```

Execute the request with cURL:

```
curl -X POST \
https://api.anyblock.tools/ethereum/ethereum/mainnet/es/tx/search/ \
-H 'Authorization: Bearer $mytoken' \
-H 'Content-Type: application/json' \
-d '{
  "query": {
    "bool": {
      "filter": [
        {
```

(continues on next page)

(continued from previous page)

```
          "term": {
            "blockHash":
↪"0x4e3a3754410177e6937ef1f84bba68ea139e8d1a2258c5f85db9f1cd715a1bdd"
          }
        }
      ]
    }
  },
  "size": 200
}'
```

Filter by a range of block numbers

The results will contain all transactions, that are included in a block, that is within the specified boundaries of the block number range. The block number has to be greater than or equal to 6400000 (*gte*) and less than or equal to 6500000 (*lte*). The results will show a maximum of 200 blocks, in no particular order.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/tx/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "range": {
            "blockNumber.num": {
              "gte": 6400000,
              "lte": 6500000
            }
          }
        }
      ]
    }
  },
  "size": 200
}
```

Execute the request with `cURL`:

```
curl -X POST \
https://api.anyblock.tools/ethereum/ethereum/mainnet/es/tx/search/ \
-H 'Authorization: Bearer $mytoken' \
-H 'Content-Type: application/json' \
-d '{
  "query": {
    "bool": {
      "filter": [
        {
          "range": {
            "blockNumber.num": {
              "gte": 6400000,
```

(continues on next page)

(continued from previous page)

```
              "lte": 6500000
            }
          }
        }
      ]
    }
  },
  "size": 200
}'
```

Filter by receiving or originating address

The results will contain all transactions, whose sender (*from*) or receiver (*to*) is has the specified address.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/tx/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "should": [
        {
          "term": {
            "from": "0xa1e4380a3b1f749673e270229993ee55f35663b4"
          }
        },
        {
          "term": {
            "to": "0xa1e4380a3b1f749673e270229993ee55f35663b4"
          }
        }
      ]
    }
  }
}
```

Execute the request with `cURL`:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/tx/search/ \
  -H 'Authorization: Bearer $mytoken' \
  -H 'Content-Type: application/json' \
  -d '{
    "query": {
      "bool": {
        "should": [
          {
            "term": {
              "from": "0xa1e4380a3b1f749673e270229993ee55f35663b4"
            }
          },
          {
```

(continues on next page)

(continued from previous page)

```
            "term": {
              "to": "0xa1e4380a3b1f749673e270229993ee55f35663b4"
            }
          }
        ]
      }
    }
  }'
```

Select by transaction hash

The results will contain only the transaction with the given transaction *hash*.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/tx/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "term": {
            "_id": "0x5c504ed432cb51138bcf09aa5e8a410dd4a1e204ef84bfed1be16dfba1b22060
↪"
          }
        }
      ]
    }
  }
}
```

Execute the request with cURL:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/tx/search/ \
  -H 'Authorization: Bearer $mytoken' \
  -H 'Content-Type: application/json' \
  -d '  {
    "query": {
      "bool": {
        "filter": [
          {
            "term": {
              "_id":
↪"0x5c504ed432cb51138bcf09aa5e8a410dd4a1e204ef84bfed1be16dfba1b22060"
            }
          }
        ]
      }
    }
  }'
```

2.4.3 Log

Filter by causing transaction's sender

The results will contain all logs, where the sender of the transaction that caused the log to be emitted has the specified address.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/log/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "term": {
            "transactionHash":
↪"0xca9b47a8bfd1c8c0e184992e0a2714558603182fc4a7f2ac16cf16f6be4f0a2a"
          }
        }
      ]
    }
  }
}
```

Execute the request with `cURL`:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/log/search/ \
  -H 'Authorization: Bearer $mytoken' \
  -H 'Content-Type: application/json' \
  -d '{
      "query": {
        "bool": {
          "filter": [
            {
              "term": {
                "transactionHash":
↪"0xca9b47a8bfd1c8c0e184992e0a2714558603182fc4a7f2ac16cf16f6be4f0a2a"
              }
            }
          ]
        }
      }
    }'
```

Filter by emitting contract

The results will contain all logs that were emitted from the specified contract.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/log/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "term": {
            "address": "0x12459c951127e0c374ff9105dda097662a027093"
          }
        }
      ]
    }
  },
  "size": 100
}
```

Execute the request with cURL:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/log/search/ \
  -H 'Authorization: Bearer $mytoken' \
  -H 'Content-Type: application/json' \
  -d '{
    "query": {
      "bool": {
        "filter": [
          {
            "term": {
              "address": "0x12459c951127e0c374ff9105dda097662a027093"
            }
          }
        ]
      }
    },
    "size": 100
  }'
```

2.4.4 Event

Filter by event name

The results will contain all events with the specified event name.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/event/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "term": {
```

(continues on next page)

(continued from previous page)

```
            "event": "transfer"
          }
        }
      ]
    }
  }
}
```

Execute the request with cURL:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/event/search/ \
  -H 'Authorization: Bearer $mytoken' \
  -H 'Content-Type: application/json' \
  -d '{
    "query": {
      "bool": {
        "filter": [
          {
            "term": {
              "event": "transfer"
            }
          }
        ]
      }
    }
  }'
```

Filter by emitting contract

The results will contain all events that where emitted by the specified contract.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/event/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "term": {
            "address.raw": "0xcfb98637bcae43C13323EAa1731cED2B716962fD"
          }
        }
      ]
    }
  }
}
```

Execute the request with cURL:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/event/search/ \
  -H 'Authorization: Bearer $mytoken' \
  -H 'Content-Type: application/json' \
  -d '{
    "query": {
      "bool": {
        "filter": [
          {
            "term": {
              "address.raw": "0xcfb98637bcae43C13323EAa1731cED2B716962fD"
            }
          }
        ]
      }
    }
  }'
```

Filter by ERC20 contract's address and *from* address

The results will contain all events that where emitted by the specified contract, and where the *from* argument of the event matches the specifid address. Although this query is tailored for ERC20 contracts, there is no parameter that specifically filters for the ERC20 interface.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/event/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "term": {
            "address.raw": "0xcfb98637bcae43C13323EAa1731cED2B716962fD"
          }
        },
        {
          "nested": {
            "path": "args",
            "query": {
              "bool": {
                "filter": [
                  {
                    "term": {
                      "args.name": "_from"
                    }
                  },
                  {
                    "term": {
                      "args.value.hex": "0x59a5208B32e627891C389EbafC644145224006E8"
                    }
                  }
                ]
```

(continues on next page)

(continued from previous page)

```
                }
              }
            }
          }
        ]
      }
    }
}
```

Execute the request with `cURL`:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/event/search/ \
  -H 'Authorization: Bearer $mytoken' \
  -H 'Content-Type: application/json' \
  -d '{
    "query": {
      "bool": {
        "filter": [
          {
            "term": {
              "address.raw": "0xcfb98637bcae43C13323EAa1731cED2B716962fD"
            }
          },
          {
            "nested": {
              "path": "args",
              "query": {
                "bool": {
                  "filter": [
                    {
                      "term": {
                        "args.name": "_from"
                      }
                    },
                    {
                      "term": {
                        "args.value.hex": "0x59a5208B32e627891C389EbafC644145224006E8"
                      }
                    }
                  ]
                }
              }
            }
          }
        ]
      }
    }
  }'
```

2.4.5 Specialised queries

Find entity by hash

The results will contain either a block with the specified block hash or all transactions, whose sender (*from*) or receiver (*to*) has the specified address. Queries like this are useful if the type of the entity that a hash represents is not known in advance.

HTTP-Method/Endpoint:

```
POST /ethereum/ethereum/mainnet/es/block,tx/search/
```

JSON body:

```
{
  "query": {
    "bool": {
      "should": [
        {
          "ids": {
            "values": [
              "0x4e3a3754410177e6937ef1f84bba68ea139e8d1a2258c5f85db9f1cd715a1bdd"
            ]
          }
        },
        {
          "term": {
            "from":
↪"0x4e3a3754410177e6937ef1f84bba68ea139e8d1a2258c5f85db9f1cd715a1bdd"
          }
        },
        {
          "term": {
            "to": "0x4e3a3754410177e6937ef1f84bba68ea139e8d1a2258c5f85db9f1cd715a1bdd"
          }
        }
      ]
    }
  }
}
```

Execute the request with `cURL`:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/block,tx/search/ \
  -H 'Authorization: Bearer d2560f14-1935-44e7-ad3e-a1718dc03bd2' \
  -H 'Content-Type: application/json' \
  -d '{
    "query": {
      "bool": {
        "should": [
          {
            "ids": {
              "values": [
                "0x4e3a3754410177e6937ef1f84bba68ea139e8d1a2258c5f85db9f1cd715a1bdd"
              ]
            }
          },
          {
            "term": {
```

(continues on next page)

(continued from previous page)

```
              "from":
↪"0x4e3a3754410177e6937ef1f84bba68ea139e8d1a2258c5f85db9f1cd715a1bdd"
            }
          },
          {
            "term": {
              "to":
↪"0x4e3a3754410177e6937ef1f84bba68ea139e8d1a2258c5f85db9f1cd715a1bdd"
            }
          }
        ]
      }
    }
  }'
```

2.5 Tutorials

To get started with anyblock.tools queries, you should have a look at our tutorials. They are a good starting point for getting used to the Elasticsearch syntax and the schemes and structuring of the query-results.

2.5.1 Simple contract event query

Welcome!

Within this tutorial you will learn how to retrieve and analyze data from the Ethereum Blockchain with the help of the anyblock.tools API.

We will show you how to retrieve data from anyblock.tools using the ElasticSearch Query DSL.

You will learn

- How to access anyblock.tools
- How to use different methods to query the anyblock.tools API
- How to write a basic query returning some events
- How a return object is structured and which data it returns
- How to filter events for a specific contract or a specific event type
- How to sort the events by blocknumber

What you must know already

This tutorial is written for programmers, who have some experience with JSON, Rest-APIs and the basic structure of HTTP-requests.

What you need

If you want to play around with the HTTP-requests, you should install an HTTP client. The good ol' terminal users might use `cURL`. For advanced usage and a graphical UI we recommend using Postman. We provide copy-pasteable commands for `cURL` throughout the tutorial, so if you want to follow along, it is advisable to install the software first.

You also will need a registered anyblock.tools API-Account in order to run the REST calls. The token of your account will be used in the following tutorial as `$token`. Please replace the variables with your user and password.

Create an anyblock.tools query step-by-step

Retrieve all events indexed by anyblock.tools

On the anyblock.tools endpoint `/ethereum/ethereum/mainnet/es/event/search`, you are able to query all events from the Ethereum mainnet.

A simple GET request to `/ethereum/ethereum/mainnet/es/event/search` shows us 10 events in no particular order.

Execute the request with `cURL`:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/event/search/ \
  -H 'Authorization: Bearer $mytoken' \
  -H 'Content-Type: application/json'
```

The returned JSON starts with meta-information about the processing of the query (not shown here).

The query results are shown under the `"hits"` keyword in the retrieved JSON data-structure:

```
"hits":{
  "total":69502921,
  "max_score":1,
  "hits":[
    ...
  ]
}
```

You get the `"total"` number of hits. It represents the total number of events in the anyblock.tools index.

> The `"max_score"` isn't very interesting to us in general, because we mostly filter for boolean conditions, that can only be `0` (not returned by the query at all) or `1`.

The actual events are listed under the `hits.hits` keyword. If we look at one of the events, we can observe the general structure of an event.

```
{
  "_index":"ethereum_2",
  "_type":"event",
  "_id":"0x92c1b864051b9e6758ab217bc70e0d8641d5f830e16b0a7d15ba78ef2356ba9c_e_52",
  "_score":1,
  "_routing":"0x251d33d4ab03fb675bb2d09304a4aca28b943373c0bd8dbc85402d9e23f4f061",
  "_parent":"0x92c1b864051b9e6758ab217bc70e0d8641d5f830e16b0a7d15ba78ef2356ba9c",
  "_source":{
    "args":[
      {
        "name":"hash",
        "value.hex":"b
↪'eb8dd23ef00be18cb4a263b4271e2f9c28bb47a239f179001691f6e887a6ed47'",
```

(continues on next page)

(continued from previous page)


```
        "value.num":null,
        "value.scaled":null,
        "value.type":"bytes32",
        "pos":0
      },
      {
        "name":"registrationDate",
        "value.hex":"0x59948642",
        "value.num":1502905922,
        "value.type":"uint256",
        "pos":1,
        "value.scaled":null
      }
    ],
    "event":"AuctionStarted",
    "logIndex":{
      "num":52,
      "raw":"0x34"
    },
    "transactionIndex":{
      "num":92,
      "raw":"0x5c"
    },
    "transactionHash":
↪"0x92c1b864051b9e6758ab217bc70e0d8641d5f830e16b0a7d15ba78ef2356ba9c",
    "address":"0x6090a6e47849629b7245dfa1ca21d94cd15878ef",
    "blockHash":"0x251d33d4ab03fb675bb2d09304a4aca28b943373c0bd8dbc85402d9e23f4f061",
    "blockNumber":{
      "num":4145267,
      "raw":"0x3f4073"
    },
    "error":null,
    "str":"AuctionStarted(b\"\\xeb\\x8d\\xd2>\\xf0\\x0b\\xe1\\x8c\\xb4\\xa2c\\xb4
↪'\\x1e/\\x9c(\\xbbG\\xa29\\xf1y\\x00\\x16\\x91\\xf6\\xe8\\x87\\xa6\\xedG\",␣
↪1502905922)",
    "timestamp":"2017-08-11T17:52:02"
  }
}
```


Again, we see meta information that is related to Elasticsearch internals (not shown here).

We want to focus on the event fields, under the `"_source"` keyword:

- `"event"` - event name
- `"blockNumber"` - the block, where it was omitted
- `"timestamp"` - approximate timestamp, when it was included in the blockchain

Each argument of an event is an element in a list `"args"`.

Filter events from a specific contract

You are probably interested in filtering for events that belong to a specific smart contract.

To demonstrate that, we will examine one of the DAI's `DSToken` contracts.

The contract for the DAI Stablecoin on the mainnet resides under the address `0x89d24A6b4CcB1B6fAA2625fE562bDD9a23260359`

The `"address"` field is where the originating contract address is given. You will have to restrict the results with Elasticsearchs filtering methods.

We don't want to use the very limited GET query. We will send a POST request to anyblock.tools, where we provide additional parameters in the body of the HTTP-request:

```
{
  "query":{
    "bool":{
      "filter":{
        "term":{
          "address":"0x89d24a6b4ccb1b6faa2625fe562bdd9a23260359"
        }
      }
    }
  }
}
```

Execute the request with `cURL`:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/event/search/ \
  -H 'Authorization: Bearer d2560f14-1935-44e7-ad3e-a1718dc03bd2' \
  -H 'Content-Type: application/json'
  -d '{
    "query": {
      "bool": {
        "filter":
          {
            "term": {
              "address": "0x89d24a6b4ccb1b6faa2625fe562bdd9a23260359"
            }
          }
      }
    }
  }'
```

The query has to be specified in the `"query"` parameter. We use a filter context `"bool": {"filter": ...}` because we are only interested in filtering elements.

In the `"term"` parameter of the filter context, we require the results to exactly match the specified value in the `"address"` argument of the event, namely the address of the DAI contract.

Filter for a specific type of event

Now every event under the `hits.hits` keyword originates from the contract of interest. but there are still different types of events present in the queries result.

The `"event"` field contains the name of the event, and if you look through the results from the last query, you will most likely see 2 different types of events, `Approval` and `Transfer`.

> *Note*: the feature of filtering by arguments and cleartext names of events is unique to anyblock.tools and it's most outstanding feature. When using the usual `web3` interface, an event and it's values are encoded in a 64 byte hexstring. To decode the event to a human readable and easy to filter representation, the hexstring has to be decoded with the help of the ABI of the events contract.

In anyblock.tools, the events are already decoded and indexed for you!

The DAI contract is following the ERC20 token standard.

From the DAI-Stablecoins ERC20 contracts code, we can see what events are defined:

```
contract ERC20Events {
    event Approval(address indexed src, address indexed guy, uint wad);
    event Transfer(address indexed src, address indexed dst, uint wad);
}
```

If we are interested in one type of event (`"Transfer"`), we have to introduce another `"term"` filter, that gets appended to the `"filter"` list:

```
{
  "query":{
    "bool":{
      "filter":[
        {
          "term":{
            "event.raw":"Transfer"
          }
        },
        {
          "term":{
            "address":"0x89d24a6b4ccb1b6faa2625fe562bdd9a23260359"
          }
        }
      ]
    }
  }
}
```

The `"event"` field defaults to a `text` type for full-text searching. We want to match the event name exactly (case sensitive), so we filter for the `event.raw` field, which is of type `keyword`. To learn more about the differences between `text` and `keyword` types in Elasticsearch, look here.

Execute the request with `cURL`:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/event/search/ \
  -H 'Authorization: Bearer d2560f14-1935-44e7-ad3e-a1718dc03bd2' \
  -H 'Content-Type: application/json'
  -d '{
    "query": {
      "bool": {
        "filter": [
          {
            "term": {
              "event.raw": "Transfer"
            }
          },
          {
            "term": {
              "address": "0x89d24a6b4ccb1b6faa2625fe562bdd9a23260359"
            }
          }
        ]
      }
```

(continues on next page)

(continued from previous page)

```
    }
  }'
```

Retrieving sorted results

You may notice that the `"timestamp"` of the events is outdated and that they are not sorted by their `"blockNumber"`.

In order to change that, the query has to be modified again:

```
{
  "query":{
    "bool":{
      "filter":[
        {
          "term":{
            "event.raw":"Transfer"
          }
        },
        {
          "term":{
            "address":"0x89d24a6b4ccb1b6faa2625fe562bdd9a23260359"
          }
        }
      ]
    }
  },
  "sort":{
    "blockNumber.num":{
      "order":"desc"
    }
  },
  "size":5
}
```

The `"sort"` parameter outside of the `"query"` nesting tells anyblock.tools which field should be used for sorting.

We specify the `.num` attribute of the `blockNumber`, because we want the integer representation and not a hex encoding.

With `"order":"desc"`, the events will be sorted in descending order of the block, where they were included in the blockchain.

Execute the request with `cURL`:

```
curl -X POST \
  https://api.anyblock.tools/ethereum/ethereum/mainnet/es/event/search/ \
  -H 'Authorization: Bearer d2560f14-1935-44e7-ad3e-a1718dc03bd2' \
  -H 'Content-Type: application/json'
  -d '{
    "query":{
        "bool":{
          "filter":[
              {
                "term":{
                    "event.raw":"Transfer"
```

(continues on next page)

(continued from previous page)

```
                }
            },
            {
              "term":{
                  "address":"0x89d24a6b4ccb1b6faa2625fe562bdd9a23260359"
              }
            }
        ]
      }
  },
  "sort":{
      "blockNumber.num":{
        "order":"desc"
      }
  },
  "size":5
}'
```

Restricting result size

In the last query we specified the `"size"` parameter with a value of `5`. This will limit the number of retrieved events to 5. For testing queries, it is advisable to set this to a small number.

With `"size":-1`, all filtered results are retrieved from the server. You will need to use this in conjunction with a carefully selected range filter, for example a range of block-numbers.

Where to go from here

The best starting point is the Elasticsearch documentation. There you'll learn how to construct more complex filter queries or how to combine filters with a boolean logic.

If you are not interested in single events, but rather on cumulated properties and statistics, you should have a look at the various possibilities of aggregations.

CHAPTER 3

SQL

3.1 Authorization

To access the SQL interface you need to retrieve your access credentials.

You can register for a **free** account and get the SQL access credentials right now at https://account.anyblock.tools/ in just a few seconds. Go ahead, I'll wait.

3.1.1 Decide on a SQL-Client

Get yourself a proper SQL-Client to access our database. We currently favour PGAdmin4, but it's up to you:

- PGAdmin4
- Valentina Studio

3.1.2 Connect to the database

Setup your connection as mentioned in the account backend. If you need help or any errors occur, please don't hesitate to ask for help from us.

3.1.3 Note

Please keep in mind that the SQL interface is still in a beta status, hence the service might not be constantly available and the database schema could change from one day through another. Now you might proceed using the SQL database or go on to the *tutorial*.

3.1.4 Contact

We might also be able to help you to pin down and visualize the data relevant for your specific use case. Just email us at mailto:contact@anyblockanalytics.com - we are excited to see our data used in many new ways!

3.2 Entity Relation Model

3.2.1 Overview

Please also refer to the leading schema defined in *ElasticSearch*

3.2.2 SQL tables and data sources

Blocks (*block*), Transactions (*tx*) and Logs (*log*) are coming directly from the Ethereum blockchain. Traces (*trace*) are client specific - here we currently only save the data from our Parity nodes. The Calls (*call*) and Events (*event*) tables contain some of our enriched data, e.g. the decoded name of the contract method (in method and event columns respectively) etc.

To enrich the data, we use the Contract (*contract*) and Token (*token*) tables to match the contract addresses and extract relevant information from the ABI. As you can see, we are only able to make the data human-readable if we have the contract ABI.

If you are interested in monitoring your own (non-public) contract - contact us and we can integrate your ABI so that you can interpret the data for your business case more easily.

The arguments of either the *Contract*, the *Call* or the *Event* are encoded as a JSON array in their enclosing tables. In case of referencing a contract that would mean the constructor arguments at the time of creation.

3.2.3 ID fields (primary keys)

The ID of the table *Trace* is the Keccak256 of: `block-hash + _ + tx-hash + _ + transaction_index`

The ID of the table *Log* is the Keccak256 of: `block-hash + _ + tx-hash + _ + log_index`

The ID of *Event* is inherited from the *Log* table, the *Call* ID is based on the *TX*.

All other ID fields should be self-explanatory. Ultimately you will rarely query data by the ID but instead using hashes, numbers and addresses.

3.2.4 Probability fields

The *Contract* and *Token* tables contain fields for numeric probability. Currently these are set to 1 for all data that we can retrieve from the blockchain or verify via Etherscan. In case we're able to find a matching contract in our database by comparing the byte code of a contract or find a similar contract on a different blockchain, this is reflected in the probability. The probabilities are then copied into the *Event* and *Call* tables to give an indication of how sure we are this is the right translation.

3.2.5 Sub-Entities and their JSON representation

The sub entities - like arguments, links and traces - are encoded in their enclosing tables using the official JSON SQL-Type. Here are some resources to get familiar with that data type:

- JSON Datatype
- JSON Functions

All subentities are stored using the PostgreSQL-Type **JSONB**.

3.2.6 Full Data model for the Ethereum SQL index

Fig. 1: Full Data model for the Ethereum SQL index

3.3 Tutorials

To get started with anyblock.tools SQL interface, you should have a look at our tutorials. Please also make sure you have had a look at the *database schema*.

3.3.1 Basic SQL Usage Examples

Welcome!

Within this tutorial you will learn how to retrieve and analyze data from the Ethereum Blockchain with the help of the anyblock.tools SQL interface.

We will show you how to retrieve data from anyblock.tools using common SQL language.

What you must know already

This tutorial is written for programmers, who have some experience with SQL. You should also have visited the *authorization* page and setup our connection to the database. Remember that the subentities are stored using the Postgresql-Type **JSONB**. For more information on that, please take a look at the *ER model*.

Basic anyblock.tools SQL queries

Choose one of the databases available. All of them are encoded as the triple of:

```
<technology>_<chain>_<network>
```

The main chain is named *ethereum_ethereum_mainnet*.

After choosing a blockchain, you might continue with the example queries.

Find the latest block

```
SELECT * FROM block ORDER BY number DESC LIMIT 1
```

This will show the whole block. But you can use a shorter form:

```
SELECT max(number) FROM block
```

Find events for a given block

```
SELECT * FROM event
WHERE event.block_number = 7075271
```

Find calls for a transaction hash

```
SELECT * FROM call
WHERE call.hash = '0xadd837afa5b68987eb9f0167ad65cbb8131f57da84db56a19acf4a5a98bd35da'
```

Find transactions for a given contract

For our example we use the address of the TenXPay token contract:

```
SELECT * FROM tx
WHERE tx.to = '0xB97048628DB6B661D4C2aA833e95Dbe1A905B280'
LIMIT 100
```

Find specific events for a given contract

For our example we use the address of the TenXPay token contract again, however we would like to know the values of transfers greater than *1ETH*:

```
SELECT arg->'scaled', arg ->'num'
FROM "event",jsonb_array_elements(args) arg
WHERE event = 'Transfer' AND address = '0xB97048628DB6B661D4C2aA833e95Dbe1A905B280'
AND (arg->'num')::numeric > 1000000000000000000
LIMIT 100
```

Find the latest 10 DAI Transfer events and extract sender, receiver and value from JSON

```
SELECT
      *,
      args->0->>'hex' as "from",
      args->1->>'hex' as "to",
      CAST(args->2->'scaled' AS NUMERIC) AS "value"
FROM event
WHERE address = '0x89d24A6b4CcB1B6fAA2625fE562bDD9a23260359'
AND event = 'Transfer'
ORDER BY timestamp DESC
LIMIT 10
```

Where to go from here

You may continue with taking a look at the *Elasticsearch tutorial*. Please let us know if you have any further questions or need some help with your application.

CHAPTER 4

Alerting

4.1 Alerting General Information

4.1.1 Overview

The alerting feature of anyblock.tools is capable of monitoring and alerting mostly all of the information that a blockchain emits.

If you haven't checked yet, or just came here for the first time, you might contact us to get access to the alerting feature.

Make sure you can access the alerting feature by opening the Dashboard. You should see an (empty) list of alerting rules.

4.1.2 Frontend Usage

Just hit + *New* on the Dashboard page to add a new alerting rule. Give it a name, select the network and configure when your data is considered *final*. See the [Example section](#examples) for the actual configuration.

4.1.3 API Usage

You can access the API with cURL or your preferred REST library. See the documentation for authorization details.

4.1.4 Properties

After you visit the dashboard you might see an empty list, you should create one first.

Name

The name has just visible purpose.

Counter

An alert has a counter which shows how often an alert has been triggered since its creation. The counter is visible in the list overview.

Network

An alert is always linked to a specific network which can be chosen from the dropdown.

Confirmation Count

The block distance needed to trigger this alert. Using `0` means that it will triggered directly without waiting for a new block to confirm. Be aware that a **reorg** on the blockchain might happen and thus the alert will trigger false-positive results - you should wait at least `5` blocks to be on the safe side.

JSON Configuration

The definition of an alert is currently checked against a JSON schema in the background (and also before you save it). You can find help and the actual alerting schema *here*.

4.2 Alerting Examples

4.2.1 Kovan DAI Transfer

```
{
    "alerts": [
        {
            "type": "Webhook (POST)",
            "payload": [
                {
                    "fieldName": "transactionHash",
                    "fieldType": "Field"
                },
                {
                    "fieldName": "args",
                    "fieldType": "Sub Field",
                    "subPayloads": [
                        {
                            "fieldName": "dst",
                            "fieldType": "Field"
                        },
                        {
                            "fieldName": "src",
                            "fieldType": "Field"
                        },
                        {
                            "fieldName": "wad",
                            "fieldType": "Field"
                        }
                    ]
                }
```

(continues on next page)

(continued from previous page)

```
            ],
            "parameters": {
                "url": "https://mywebhook.example/{transactionHash}/{args#src}"
            }
        }
    ],
    "targetMap": [
        {
            "name": "address",
            "value": "0xC4375B7De8af5a38a93548eb8453a498222C4fF2",
            "operator": "Equals"
        },
        {
            "name": "event",
            "value": "Transfer",
            "operator": "Equals (ignore case)"
        },
        {
            "name": "args",
            "operator": "Inspect",
            "operatorParameters": [
                {
                    "name": "dst",
                    "value": "0x52243C97DD8556fe1092084c199aeFAD4c34fD89",
                    "operator": "Equals (ignore case)"
                }
            ]
        }
    ],
    "targetType": "Event"
}
```

4.2.2 Kovan ETH Traces

```
{
    "alerts": [
        {
            "type": "Webhook (POST)",
            "payload": [
                {
                    "fieldName": "transactionHash",
                    "fieldType": "Field"
                },
                {
                    "fieldName": "trace",
                    "fieldType": "Sub Field",
                    "subPayloads": [
                        {
                            "fieldName": "action",
                            "fieldType": "Sub Field",
                            "subPayloads": [
                                {
                                    "fieldName": "to",
                                    "fieldType": "Field"
                                }
```

(continues on next page)

(continued from previous page)

```
                            ]
                        }
                    ]
                }
            ],
            "parameters": {
                "url": "https://mywebhook.example/{transactionHash}/{args#src}"
            }
        }
    ],
    "targetMap": [
        {
            "name": "trace",
            "operator": "Inspect",
            "operatorParameters": [
                {
                    "name": "action",
                    "operator": "Inspect",
                    "operatorParameters": [
                        {
                            "name": "to",
                            "value": "0x52243C97DD8556fe1092084c199aeFAD4c34fD89",
                            "operator": "Equals (ignore case)"
                        }
                    ]
                }
            ]
        }
    ],
    "targetType": "Trace"
}
```

4.2.3 Full Alerting

Usage of all possible alert-triggers were all events (decoded logs) are matched that have:

- `address` = 0xe3818504c1B32bF1557b16C238B2E01Fd3149C17
- `event` = Transfer
- `to` = 0x8d12A197cB00D4747a1fe03395095ce2A5CC6819
- `value` > 999999

```
{
    "targetType": "Event",
    "targetMap": [
        {
            "name": "address",
            "value": "0xe3818504c1B32bF1557b16C238B2E01Fd3149C17",
            "operator": "Equals"
        },
        {
            "name": "event",
            "value": "Transfer",
            "operator": "Equals (ignore case)"
```

(continues on next page)

(continued from previous page)

```
        },
        {
            "name": "args",
            "operator": "Inspect",
            "operatorParameters": [
                {
                    "name": "to",
                    "value": "0x8d12A197cB00D4747a1fe03395095ce2A5CC6819",
                    "operator": "Equals (ignore case)"
                },
                {
                    "name": "value",
                    "value": "999999",
                    "operator": "Greater",
                    "useScaledValue": true
                }
            ]
        }
    ],
    "alerts": [
        {
            "type": "Slack",
            "payload": [
                {
                    "fieldName": "transactionHash",
                    "fieldType": "Field"
                },
                {
                    "fieldName": "args",
                    "fieldType": "Sub Field",
                    "subPayloads": [
                        {
                            "fieldType": "Field",
                            "fieldName": "to"
                        }
                    ]
                }
            ],
            "parameters": {
                "url": "https://hooks.slack.com/services/myslackhookurl",
                "text": ":warning: There has been a new alert match",
                "channel": "#alerting",
                "username": "#blockchain-alerting-bot"
            }
        },
        {
            "type": "Email",
            "payload": [
                {
                    "fieldName": "transactionHash",
                    "fieldType": "Field"
                },
                {
                    "fieldName": "args",
                    "fieldType": "Sub Field",
                    "subPayloads": [
                        {
```

(continues on next page)

(continued from previous page)

```
                        "fieldType": "Field",
                        "fieldName": "to"
                    }
                ]
            }
        ],
        "parameters": {
            "recipients": [
                "user1@foobar.example",
                "user2@foobar.example"
            ]
        }
    },
    {
        "type": "Webhook (GET)",
        "parameters": {
            "url": "https://mywebhook1.example/{transactionHash}/{args#to}"
        },
        "payload": [
            {
                "fieldType": "Field",
                "fieldName": "transactionHash"
            },
            {
                "fieldType": "Sub Field",
                "fieldName": "args",
                "subPayloads": [
                    {
                        "fieldType": "Field",
                        "fieldName": "to"
                    }
                ]
            }
        ]
    },
    {
        "type": "Webhook (POST)",
        "parameters": {
            "url": "https://mywebhook2.example"
        },
        "payload": [
            {
                "fieldType": "Field",
                "fieldName": "transactionHash"
            },
            {
                "fieldType": "Sub Field",
                "fieldName": "args",
                "subPayloads": [
                    {
                        "fieldType": "Field",
                        "fieldName": "to"
                    }
                ]
            }
        ]
    }
```

(continues on next page)

(continued from previous page)

```
    ]
}
```

4.3 Alerting JSON Schema

The schema has three main parts:

- `targetType`
- `targetMap`
- `alerts`

The `targetType` is the type of entity that our alerting infrastructure will look for and then match against your configured `targetMap`. The `alerts` define types of actions that should get triggered once an entity has been matched.

4.3.1 Target-Type

The target-type can be any that is defined in the enumeration of this element. In that case it is currently list as:

- `Event`
- `Log`
- `Transaction`
- `Call`
- `Trace`

(Omitted other types as they are not user-relevant)

4.3.2 Target-Map

The `targetMap` defines an array of target-definitions that the entity should have in order to be a successful match and trigger an alert. Each of the target-definition can have:

- `name`
- `value`
- `operator`
- `operatorParameters`
- `useScaledValue`

Name

The name of the attribute that should be inspected

Example: `address` for a log to inspect the contract address of a log that came through)

In order to decide which fields are available you should look at our *Elastic Data-Structure*.

Value

The value the attribute should have represented as a String, or String-Array in case you want to match one of multiple values

Example: `0xe3818504c1B32bF1557b16C238B2E01Fd3149C17` for a contract address

Operator

The operator that should be used to match the `value` against:

- `Greater`: **>** `value`
- `Greater or Equal`: **>=** `value`
- `Less`: **<** `value`
- `Less or Equal`: **<=** `value`
- `Equals`: **==** `value` (For String *AND* Numeric)
- `Equals (ignore case)`: Case insensitive variant of `Equals`
- `Equals any`: Matches any against `value` using `Equals` - in that case `value` must be a String-Array
- `Equals any (ignore case)`: Case insensitive variant of `Equals any`
- `Inspect`: Steps into that property

Operator: Inspect

Some of the Target-Types have a deep structure. For example `call` and `event` both have the property `args` which contain the arguments of an Eth-Transaction (call) and the parameters of an emitted Eth-Log.

In order to inspect the arguments/parameters, we need the `Inspect` operator.

The stepping works 2 levels deep (Eth-Traces have a structure 2 levels deep).

Usage of Scaled values

In case of `call` and `event` and their arguments/parameters you are able to match them against the scaled variant of them. This special flag is only available on the 2nd level of `Inspect` because the scaled values only appear there.

Note: We can only decode values if the event/call comes from a popular token where we have the number of decimals used.

4.3.3 Alerts

The `alerts` property defines an array with alert-definitions that should get triggered once a match was found. Each of the alert-definition can have:

- `type`
- `parameters`
- `payload`

Type

The type defines the type of the alert which can be: - `Webhook (GET)`: Calls an endpoint using *HTTP/GET* - `Webhook (POST)`: Calls an endpoint using *HTTP/POST* with the body encoded in JSON - `Email`: Will send an email - `Slack`: Triggers a slack webhook URL

Parameters

This object type property of the schema depends on the type you have chosen.

- `Email`: * `recipients` (String-Array) with email-addresses that should get the alerting-mail
- `Slack`: * `url` (String) The full URL of the webhook (can be generated by a Slack-Adminstrator) * `text` (String) Introductional text (slack emoticons can be used, like *:warning:* * `channel` (String) The channel where to post the alert * `username` (String) The username that the message should be posted as
- `Webhook (GET)`: * `url` (String) The url that should get called
- `Webhook (POST)`: * `url` (String) The url that should get called

Note: Strings like `{transactionHash}` inside of the webhook URLs will get replaced with the actual value given from the payload.

Payload

A array of objects that should get send with the alert, along the matching properties defined in the `targetMap`. Each of them can have the following (the syntax is almost the same to the `operator`:

- `fieldType`: Can be `Field` or `Sub Field`
- `fieldName`: The name of the property that should get extracted from the matching entity and send along with the alert
- `subPayloads`: If `Sub Field` is chosen, you can append another level of inspection

4.3.4 Schema JSON

The current alerting schema formatted as a JSON schema:

```
{
    "$schema": "http://json-schema.org/draft-07/schema#",
    "$id": "http://anyblock.tools/alertingConfig.json",
    "type": "object",
    "required": [
        "blockchain",
        "name",
        "network",
        "technology",
        "config",
        "maxConfirmationCount"
    ],
    "additionalProperties": true,
    "properties": {
        "version": {
            "type": "integer"
        },
```

(continues on next page)

(continued from previous page)

```
        "maxConfirmationCount": {
            "type": "integer"
        },
        "description": {
            "type": [
                "string",
                "null"
            ]
        },
        "blockchain": {
            "type": "string"
        },
        "name": {
            "type": "string"
        },
        "network": {
            "type": "string"
        },
        "technology": {
            "type": "string"
        },
        "config": {
            "type": "object",
            "required": [
                "targetType",
                "targetMap",
                "alerts"
            ],
            "additionalProperties": false,
            "properties": {
                "targetType": {
                    "type": "string",
                    "enum": [
                        "Event",
                        "Log",
                        "Transaction",
                        "Call",
                        "Contract",
                        "Token",
                        "Trace",
                        "Method"
                    ]
                },
                "targetMap": {
                    "type": "array",
                    "minItems": 1,
                    "maxItems": 10,
                    "uniqueItems": true,
                    "items": {
                        "type": "object",
                        "required": [
                            "name",
                            "operator"
                        ],
                        "additionalProperties": false,
                        "properties": {
                            "name": {
```

(continues on next page)

(continued from previous page)

```
                "type": "string"
            },
            "value": {},
            "additionalProperties": false,
            "operator": {
                "type": "string",
                "enum": [
                    "Greater",
                    "Greater or Equal",
                    "Less",
                    "Less or Equal",
                    "Equals",
                    "Equals (ignore case)",
                    "Equals any",
                    "Equals any (ignore case)",
                    "Inspect"
                ]
            },
            "operatorParameters": {
                "type": "array",
                "items": {
                    "type": "object",
                    "required": [
                        "name",
                        "operator"
                    ],
                    "properties": {
                        "name": {
                            "type": "string"
                        },
                        "useScaledValue": {
                            "type": "boolean"
                        },
                        "value": {},
                        "operator": {
                            "type": "string",
                            "enum": [
                                "Greater",
                                "Greater or Equal",
                                "Less",
                                "Less or Equal",
                                "Equals",
                                "Equals (ignore case)",
                                "Equals any",
                                "Equals any (ignore case)",
                                "Inspect"
                            ]
                        },
                        "operatorParameters": {
                            "type": "array",
                            "items": {
                                "type": "object",
                                "required": [
                                    "name",
                                    "value",
                                    "operator"
                                ],
```

(continues on next page)

(continued from previous page)

```
                                        "properties": {
                                            "name": {
                                                "type": "string"
                                            },
                                            "value": {},
                                            "operator": {
                                                "type": "string",
                                                "enum": [
                                                    "Greater",
                                                    "Greater or Equal",
                                                    "Less",
                                                    "Less or Equal",
                                                    "Equals",
                                                    "Equals (ignore case)",
                                                    "Equals any",
                                                    "Equals any (ignore case)"
                                                ]
                                            }
                                        },
                                        "allOf": [
                                            {
                                                "if": {
                                                    "properties": {
                                                        "operator": {
                                                            "enum": [
                                                                "Equals any",
                                                                "Equals any␣
↪(ignore case)"
                                                            ]
                                                        }
                                                    }
                                                },
                                                "then": {
                                                    "properties": {
                                                        "value": {
                                                            "type": "array",
                                                            "items": {
                                                                "type":
↪"string"
                                                            }
                                                        }
                                                    }
                                                },
                                                "else": {
                                                    "properties": {
                                                        "value": {
                                                            "type": "string"
                                                        }
                                                    }
                                                }
                                            }
                                        ]
                                    }
                                }
                            },
                            "allOf": [
                                {
```

(continues on next page)

(continued from previous page)

```
                                    "if": {
                                        "properties": {
                                            "operator": {
                                                "enum": [
                                                    "Inspect"
                                                ]
                                            }
                                        }
                                    },
                                    "then": {
                                        "required": [
                                            "operator",
                                            "operatorParameters"
                                        ]
                                    },
                                    "else": {
                                        "properties": {
                                            "operatorParameters": {
                                                "type": "null"
                                            }
                                        }
                                    }
                                },
                                {
                                    "if": {
                                        "properties": {
                                            "operator": {
                                                "enum": [
                                                    "Equals any",
                                                    "Equals any (ignore case)"
                                                ]
                                            }
                                        }
                                    },
                                    "then": {
                                        "properties": {
                                            "value": {
                                                "type": "array",
                                                "items": {
                                                    "type": "string"
                                                }
                                            }
                                        }
                                    },
                                    "else": {
                                        "properties": {
                                            "value": {
                                                "type": "string"
                                            }
                                        }
                                    }
                                }
                            ]
                        }
                    }
                },
                "allOf": [
```

(continues on next page)

(continued from previous page)

```
                        {
                            "if": {
                                "properties": {
                                    "operator": {
                                        "enum": [
                                            "Inspect"
                                        ]
                                    }
                                }
                            },
                            "then": {
                                "required": [
                                    "operator",
                                    "operatorParameters"
                                ]
                            },
                            "else": {
                                "properties": {
                                    "operatorParameters": {
                                        "type": "null"
                                    }
                                }
                            }
                        },
                        {
                            "if": {
                                "properties": {
                                    "operator": {
                                        "enum": [
                                            "Equals any",
                                            "Equals any (ignore case)"
                                        ]
                                    }
                                }
                            },
                            "then": {
                                "properties": {
                                    "value": {
                                        "type": "array",
                                        "items": {
                                            "type": "string"
                                        }
                                    }
                                }
                            },
                            "else": {
                                "properties": {
                                    "value": {
                                        "type": "string"
                                    }
                                }
                            }
                        }
                    ]
                }
            },
            "alerts": {
```

(continues on next page)

(continued from previous page)

```
                "type": "array",
                "minItems": 1,
                "maxItems": 10,
                "uniqueItems": true,
                "items": {
                    "type": "object",
                    "required": [
                        "type",
                        "parameters"
                    ],
                    "properties": {
                        "type": {
                            "type": "string",
                            "enum": [
                                "Webhook (GET)",
                                "Webhook (POST)",
                                "Email",
                                "Slack"
                            ]
                        },
                        "parameters": {
                            "type": "object"
                        },
                        "payload": {
                            "type": "array",
                            "maxItems": 10,
                            "uniqueItems": true,
                            "items": {
                                "type": "object",
                                "additionalProperties": false,
                                "properties": {
                                    "fieldType": {
                                        "type": "string",
                                        "enum": [
                                            "Field",
                                            "Sub Field"
                                        ]
                                    },
                                    "fieldName": {
                                        "type": "string"
                                    },
                                    "subPayloads": {
                                        "type": "array",
                                        "items": {
                                            "type": "object",
                                            "additionalProperties": false,
                                            "properties": {
                                                "fieldType": {
                                                    "type": "string",
                                                    "enum": [
                                                        "Field",
                                                        "Sub Field"
                                                    ]
                                                },
                                                "fieldName": {
                                                    "type": "string"
                                                },
```

(continues on next page)

(continued from previous page)

```
                                        "subPayloads": {
                                            "type": "array",
                                            "required": [
                                                "fieldName",
                                                "fieldType"
                                            ],
                                            "items": {
                                                "type": "object",
                                                "additionalProperties":␣
↪false,
                                                "properties": {
                                                    "fieldType": {
                                                        "type": "string",
                                                        "enum": [
                                                            "Field"
                                                        ]
                                                    },
                                                    "fieldName": {
                                                        "type": "string"
                                                    }
                                                }
                                            }
                                        }
                                    },
                                    "if": {
                                        "properties": {
                                            "fieldType": {
                                                "enum": [
                                                    "Sub Field"
                                                ]
                                            }
                                        }
                                    },
                                    "then": {
                                        "required": [
                                            "fieldName",
                                            "subPayloads"
                                        ]
                                    },
                                    "else": {
                                        "properties": {
                                            "subPayloads": {
                                                "type": "null"
                                            }
                                        }
                                    }
                                }
                            }
                        },
                        "if": {
                            "properties": {
                                "fieldType": {
                                    "enum": [
                                        "Sub Field"
                                    ]
                                }
                            }
                        }
```

(continues on next page)

(continued from previous page)

```
                                    },
                                    "then": {
                                        "required": [
                                            "fieldName",
                                            "subPayloads"
                                        ]
                                    },
                                    "else": {
                                        "properties": {
                                            "subPayloads": {
                                                "type": "null"
                                            }
                                        }
                                    }
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
```

4.4 Alerting API-Routes

When adding or modifying alerting rules via the API, you have to provide the metadata you can just select in the frontend. The actual configuration goes into the config section.

```
{
    "name": "Example Alerting Rule 0001",
    "maxConfirmationCount": 10,
    "technology": "ethereum",
    "blockchain": "ethereum",
    "network": "kovan",
    "config": {
        "see": "examples"
    }
}
```

The available routes are:

4.4.1 Get all Alerting Rules

```
curl -X GET \
https://api.anyblock.tools/alerting/rules/ \
-H 'Authorization: Bearer <your-token>'
```

4.4.2 Get a single Alerting Rule

```
curl -X GET \
https://api.anyblock.tools/alerting/rules/<id>/ \
-H 'Authorization: Bearer <your-token>'
```

4.4.3 Add an Alerting Rule

```
curl -X POST \
https://api.anyblock.tools/alerting/rules/ \
-H 'Authorization: Bearer <your-token>' \
-H 'Content-Type: application/json' \
-d '{
        "name": "Example Alerting Rule 0001",
        "maxConfirmationCount": 10,
        "technology": "ethereum",
        "blockchain": "ethereum",
        "network": "kovan",
        "config": {
            "see": "examples"
        }
    }'
```

4.4.4 Update an Alerting Rule

```
curl -X PUT \
https://api.anyblock.tools/alerting/rules/<id>/ \
-H 'Authorization: Bearer <your-token>' \
-H 'Content-Type: application/json' \
-d '{
        "name": "Example Alerting Rule 0002",
        "maxConfirmationCount": 5,
        "config": {
            "see": "examples"
        }
    }'
```

4.4.5 Delete an Alerting Rule

```
curl -X DELETE \
https://api.anyblock.tools/alerting/rules/<id>/ \
-H 'Authorization: Bearer <your-token>'
```