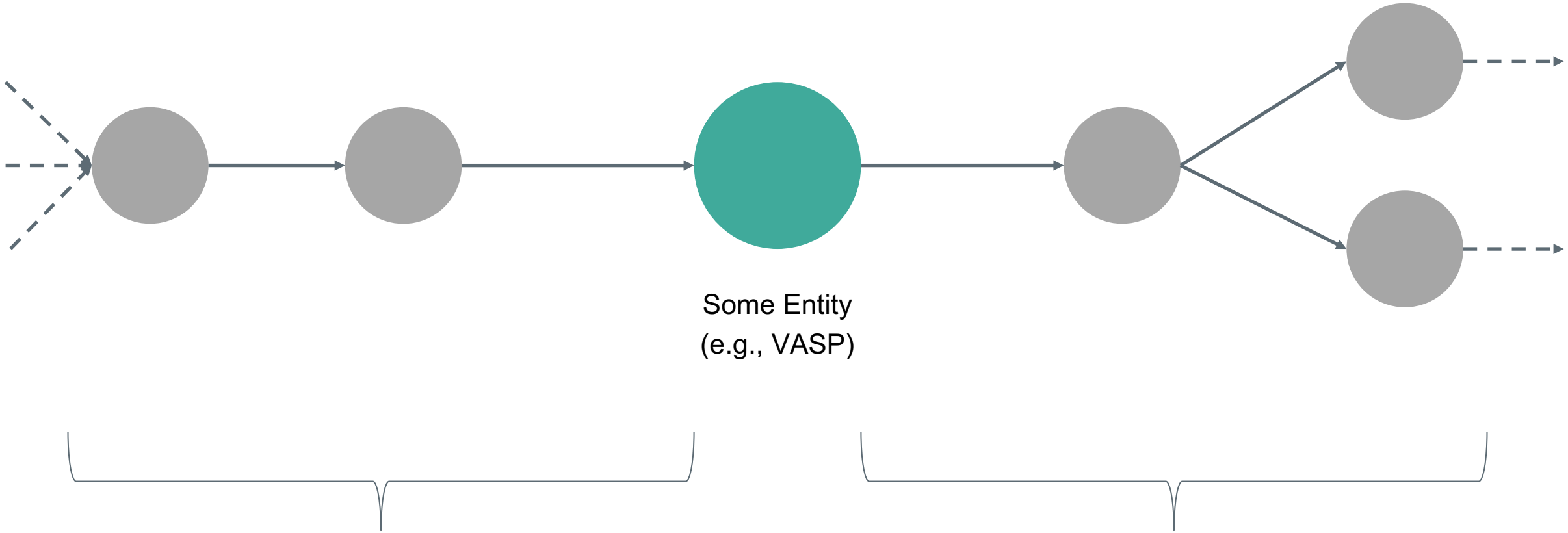
AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

GRAPHSENSE

i-Lead Research Day

Bernhard Haslhofer, March 25th 2021

CRYPTOASSET ANALYTICS

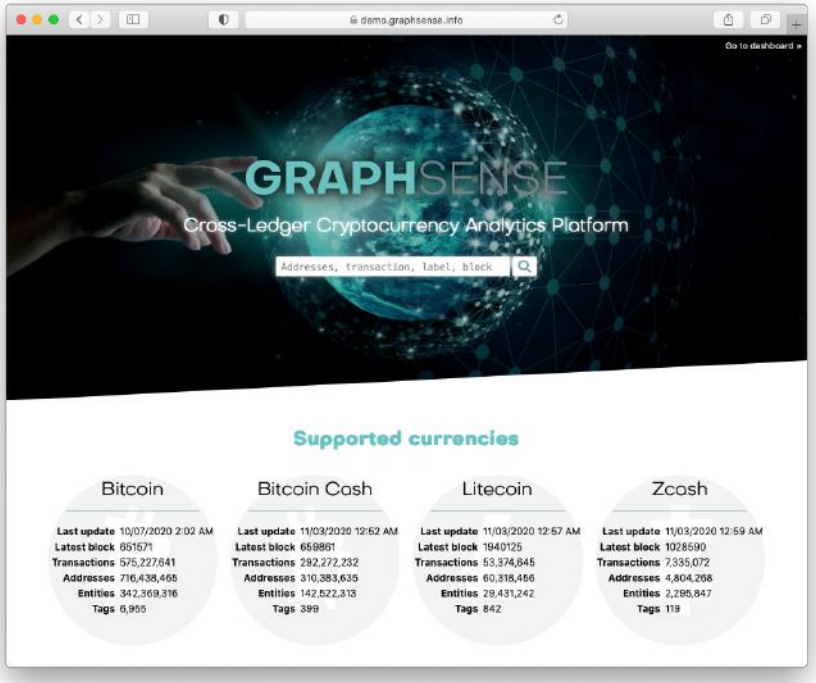


WHAT IS GRAPHSENSE ABOUT?

Full Data Sovereignty

Algorithmic Transparency

Scalability



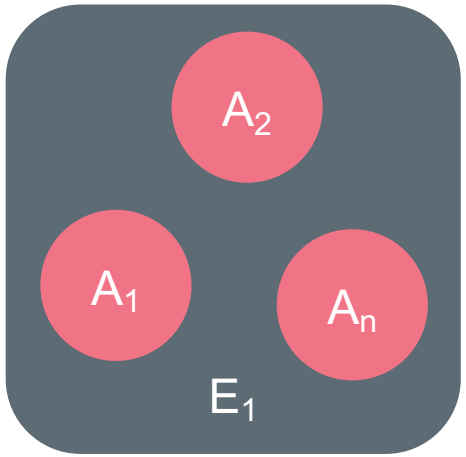
Dashboard for Basic Investigations

Advanced Analysis Capabilities

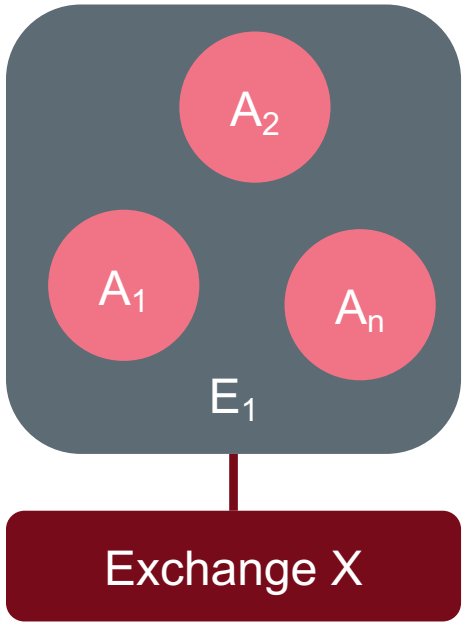
Open Source & Free

made in

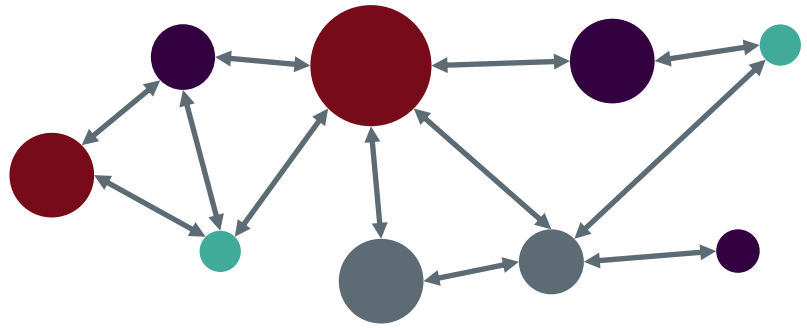
CRYPTOASSET ANALYTICS | BASIC TECHNIQUES



Address Clustering



Attribution Tags



Entity Graph

On-chain Deanonymization Methods

CRYPTOASSET ANALYTICS | EXAMPLES

A Deep Dive into Bitcoin Mining Pools

An Empirical Analysis of Mining Shares

Matteo Romiti[1], Aljosha Judmayer[2], Ale
Haslhofer[1]

[1] Austrian Institute of Technology {r
[2] SBA Research ajudmayer@s
[3] Imperial College London a.zamy

Abstract. Miners play a key role in cry
they invest substantial computational re
tions and minting new currency units. It i
controlling more than half of the network
ulate the state of the system at will. Whil
pools appears evenly split, the actual distri
these pools and their economic relationsh
undisclosed. To this end, we conduct the fi
reward distribution within three of the fo

JOURNAL OF CYBERSECURITY

Research paper

Ransomware payments in the Bitcoin ecosystem

Masarah Paquet-Clouston[1,*], Bernhard Haslhofer[2] and Benoît Dupon

[1]GoSecure, 630 René-Lévesque Blvd W #2630, Montreal, QC H3B 1S6, Canada, [2]AIT Austrian Insti
Technology, Giefinggasse 4, 1210 Vienna, Austria and [3]Université de Montréal, 2900 Edouard Montpet
Montreal, QC H3T 1J4, Canada

*Corresponding address: Research and Development Department, GoSecure, 630 Boul. René-Lévesque Wes
Montréal, QC, H3B 1S6. E-mail: mcpc@gosecure.ca

Received 9 August 2018; revised 18 December 2018; accepted 0 Month 0000

Abstract

Ransomware can prevent a user from accessing a device and its files until a ransom is paid to the attacker, most frequently in Bitcoin. With over 500 known ransomware families, it has become one of the dominant cybercrime threats for law enforcement, security professionals, and the public. However, a more comprehensive, evidence-based picture on the global direct financial impact of ransomware attacks is still missing. In this article, we present a data-driven method for identifying

Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem

Masarah Paquet-Clouston
GoSecure
mcpc@gosecure.net

Matteo Romiti
Austrian Institute of Technology
Matteo.Romiti@ait.ac.at

Bernhard Haslhofer
Austrian Institute of Technology
Bernhard.Haslhofer@ait.ac.at

Thomas Charvat
Excello
tc@excello.cz

ABSTRACT

In the past year, a new spamming scheme has emerged: sexual extortion messages requiring payments in the cryptocurrency Bitcoin, also known as *sextortion*. This scheme represents a first integration of the use of cryptocurrencies by members of the spamming industry. Using a dataset of 4,340,736 sextortion spams, this research aims at understanding such new amalgamation by uncovering spammers' operations. To do so, a simple, yet effective method for projecting Bitcoin addresses mentioned in sextortion spams onto transaction graph abstractions is computed over the entire Bitcoin blockchain. This allows us to track and investigate monetary flows between involved actors and gain insights into the financial structure of sex-

Since 2018, sextortion spams have been distributed in a dozen languages, most likely with the use of the Necurs botnet [13, 32]. Shultz [32] already conducted a primary analysis of the sextortion spammers potential revenues by inspecting 58,611 Bitcoin addresses found in two sextortion-related spam campaigns lasting 60 days. He concluded that a total of 83 addresses received approximately $146,280. However, the author only summed incoming payments without applying more advanced methods for tracing monetary flows in the Bitcoin transaction graph, which have already been applied for studying other forms of cryptocurrency-related cybercrime, such as ransomware [12, 28]. Shultz's [32] findings provide a first overview of a much bigger puzzle, which has yet to be uncov-

Supported currencies

Bitcoin

Last update	11/06/2020 12:53 AM
Latest block	655598
Transactions	584,169,824
Addresses	730,634,215
Entities	349,018,614
Tags	6,956

Bitcoin Cash

Last update	11/06/2020 12:31 AM
Latest block	660278
Transactions	292,332,220
Addresses	310,454,147
Entities	144,170,654
Tags	399

Litecoin

Last update	11/06/2020 12:58 AM
Latest block	1941940
Transactions	53,642,337
Addresses	60,440,537
Entities	29,523,710
Tags	842

Zcash

Last update	11/06/2020 12:59 AM
Latest block	1032041
Transactions	7,350,533
Addresses	4,815,494
Entities	2,304,119
Tags	119

Open Source Software by the Austrian Institute of Technology, supported by the EU H2020 TITANIUM project and by the FFG VIRTCRIME project

Visit us on Github

Version 0.4.4

GRAPHSENSE | ADVANCED ANALYTICS TASK

jupyter GraphSense_API_Python_Example Last Checkpoint: an hour ago (autosaved) Logout

File Edit View Insert Cell Kernel Help Trusted Python 3

Run Code

In [1]:
```
import graphsense
```
executed in 122ms, finished 17:08:10 2020-11-09

In [2]:
```
configuration = graphsense.Configuration(host = "http://localhost:9000", api_key = {'api_key': 'alicekey'})
api_client = graphsense.ApiClient(configuration)
addresses_api = graphsense.AddressesApi(api_client)
address_string = '18NSAybFEhLa6AG3gxEN1hiaRJoSvvbnDb'
currency = 'btc'
```
executed in 10ms, finished 17:08:10 2020-11-09

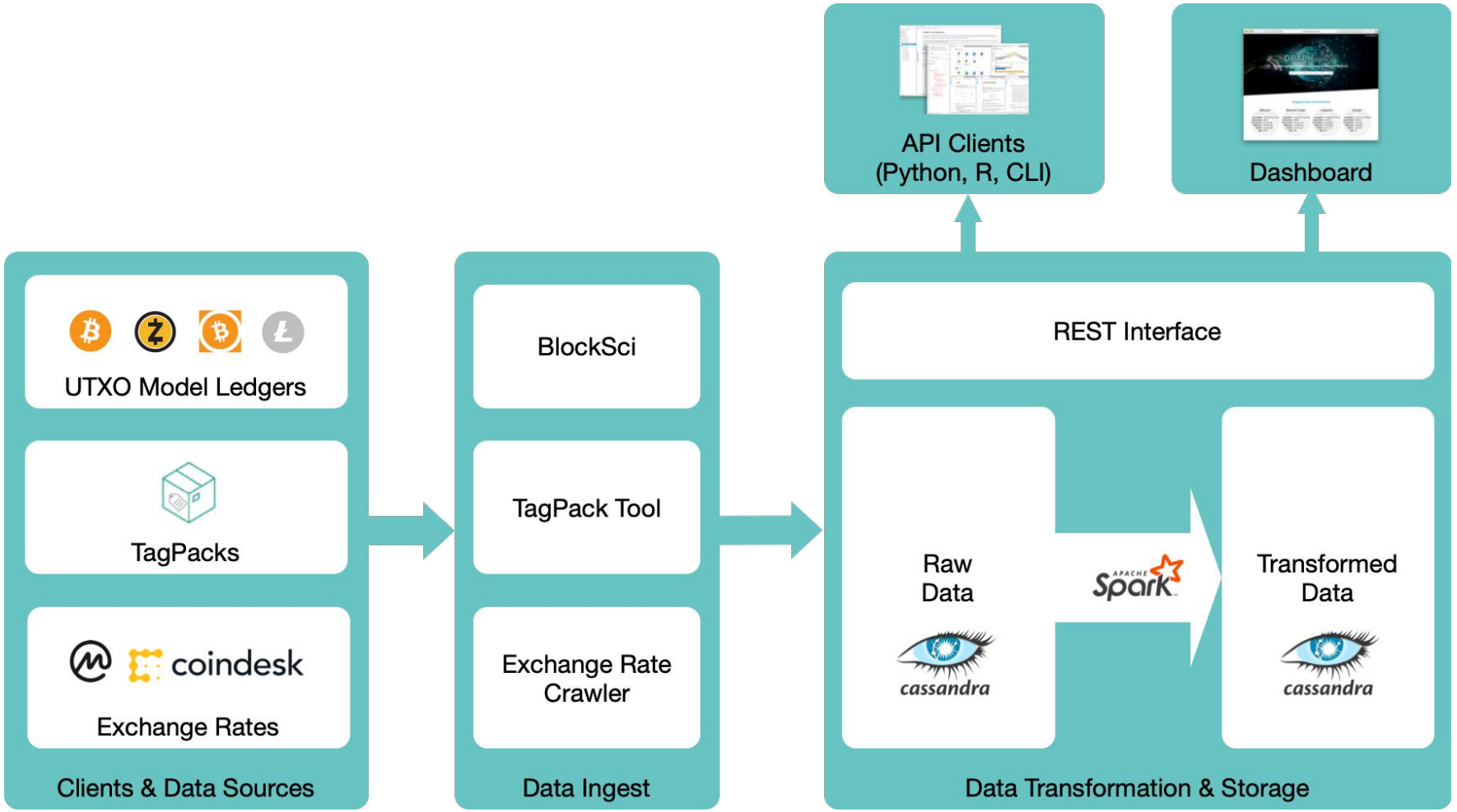
In [3]:
```
address_obj = addresses_api.get_address_with_tags(currency, address_string)
print('Address', address_obj.address, 'received', address_obj.total_received.eur, 'EUR and',
      address_obj.no_incoming_txs, 'incoming txs from',
      address_obj.in_degree, 'incoming neighbors.')
```
executed in 738ms, finished 17:08:12 2020-11-09

```
Address 18NSAybFEhLa6AG3gxEN1hiaRJoSvvbnDb received 57741 EUR and 34 incoming txs from 62 incoming neighbors.
```

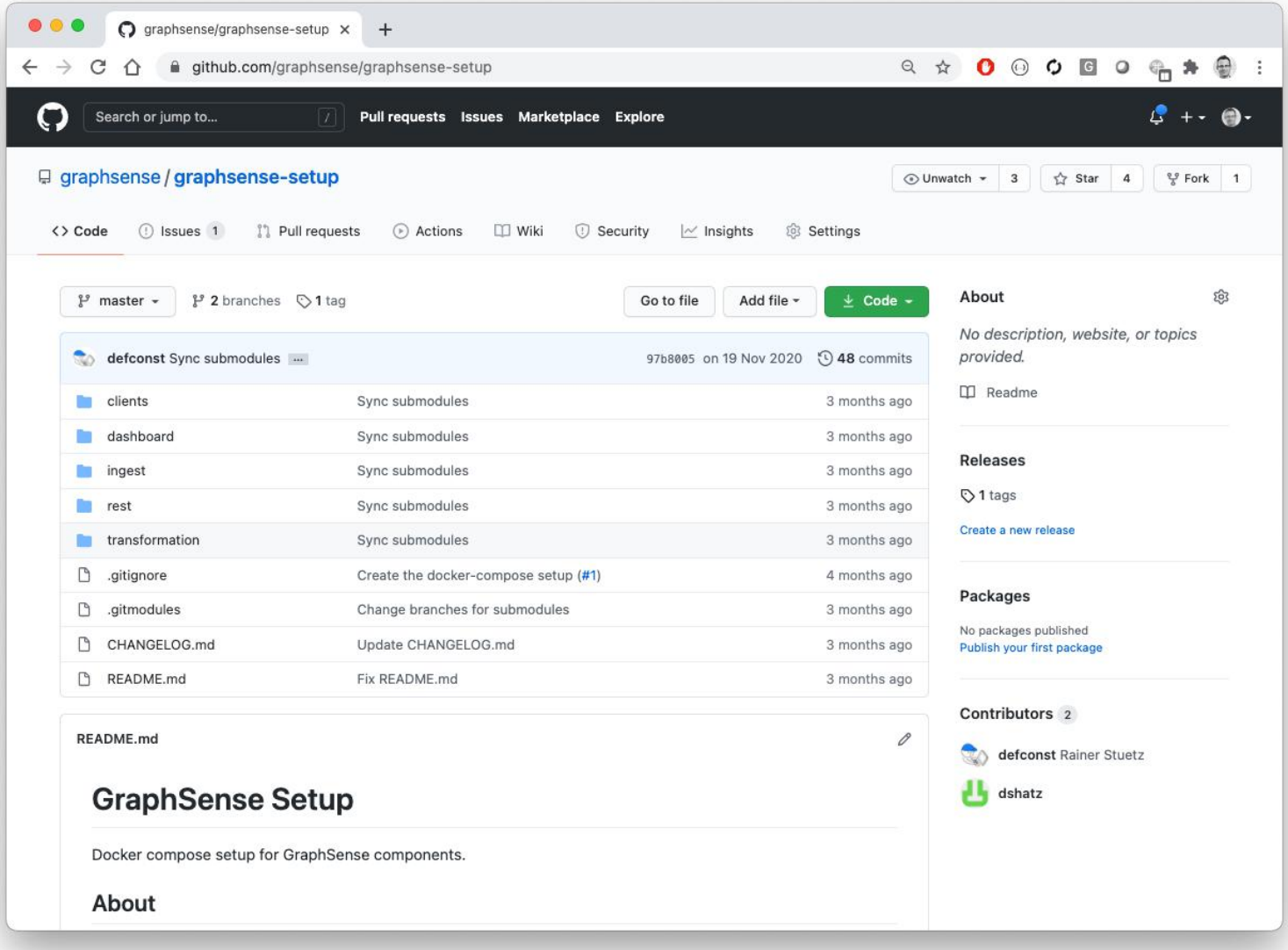
In [4]:
```
entity_obj = addresses_api.get_address_entity(currency, address_string)
print('Entity', entity_obj.entity, 'received', entity_obj.total_received.eur, 'EUR and',
      entity_obj.no_incoming_txs, 'incoming txs from',
      entity_obj.in_degree, 'incoming neighbors.')
```
executed in 913ms, finished 17:08:13 2020-11-09

```
Entity 203719034 received 57741 EUR and 34 incoming txs from 31 incoming neighbors.
```

GRAPHSENSE | ARCHITECTURE



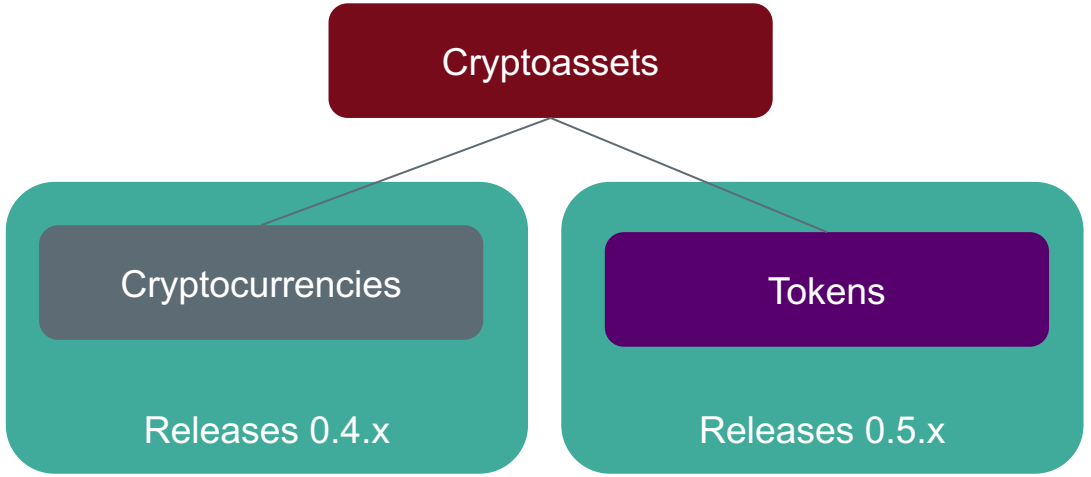
GRAPHSENSE | SETUP



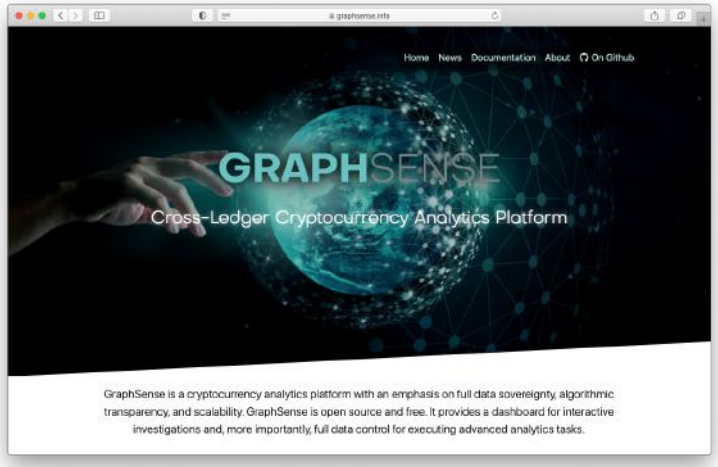
GRAPHSENSE | STATUS AND OUTLOOK

Layer 2
Payment Channel
Networks

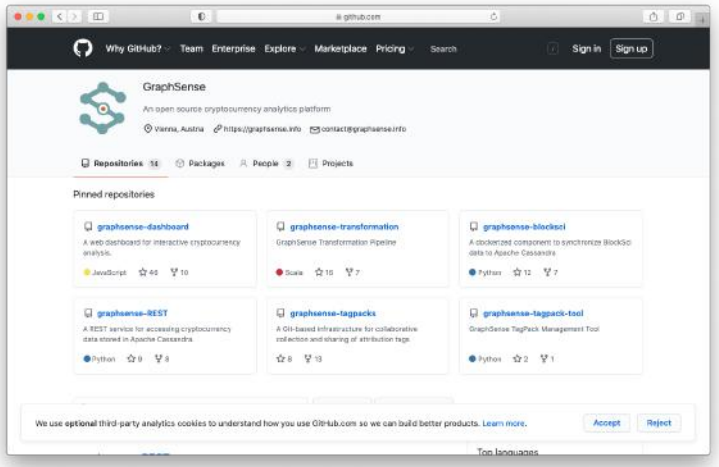
Layer 1
Blockchain



GRAPHSENSE | FURTHER INFORMATION



https://graphsense.info



https://github.com/graphsense

contact@graphsense.info
graphsense-users@googlegroups.com