Analyzing Blockchain Transaction Graphs for Fraudulent Activities

Alper Şen, Boğaziçi University (BOUN)

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632

Outline

- Objectives and Motivation
- Blockchain Adoption in EU
- Pilot Architecture
- Innovations in the Pilot
- Demo

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632

Motivation

- As of Feb 16, 2021, market capitalization of crypto assets has reached **1.49 trillion** dollars.

- Institutional interest in crypto assets increasing (e.g. recent Tesla investment, Mastercard support in 2021) .
  - Mastercard: "We are here to enable customers, merchants and businesses to move digital value — traditional or crypto — however they want. It should be your choice, it's your money."

- New blockchain use cases DeFi, stablecoins, savings accounts, lending, content management, KYC etc. are appearing.

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632

Motivation

Blockchain regulations are being developed for “public blockchain” and “traditional finance” integration and interfacing.

- US Treasury guidance “Banks may provide custody services to crypto assets”
- Global money laundering and terrorist financing watchdog (FATF) published Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs)
  - *“VASPs be regulated for anti-money laundering and combating the financing of terrorism (AML/CFT) purposes, licensed or registered, and subject to effective systems for monitoring or supervision”*


Office of the Comptroller of the Currency

ABOUT NEWS & EVENTS PUBLICATIONS & RESOURCES TOPIC

Home > News & Events > Newsroom

News Release 2020-98 | July 22, 2020

Federally Chartered Banks and Thrifts May Provide Custody Services For Crypto Assets

SHARE THIS PAGE:

Print

WASHINGTON—The Office of the Comptroller of the Currency (OCC) today published a letter clarifying national banks' and federal savings associations' authority to provide cryptocurrency custody services for customers.

National and state banks and thrifts have long provided safekeeping and custody services, including both physical objects and electronic assets. The OCC has specifically recognized the importance of digital assets and the authority for banks to provide safekeeping for such assets since 1998. In the letter published today, the OCC concludes that providing cryptocurrency custody services, including holding unique cryptographic keys associated with cryptocurrency, is a modern form of traditional bank activities related to custody services. Crypto custody services may extend beyond passively holding "keys."

"From safe-deposit boxes to virtual vaults, we must ensure banks can meet the financial services needs of their customers today," said Acting Comptroller of the Currency Brian P. Brooks. "This opinion clarifies that banks can continue satisfying their customers' needs for safeguarding their most valuable assets, which today for tens of millions of Americans includes cryptocurrency."

The OCC also recognizes that, as the financial markets are increasingly digitized, the need will increase for banks and other service providers to leverage new technology and innovative ways to serve their customers' needs. By doing so, banks can

Media Contact

Bryan Hubbard

(202) 649-6870

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement no 856632

Blockchain Adoption in EU

- The recent EC Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets dated September 24, 2020 states that it :

  "*supports a holistic approach to blockchain and DLT, which aims at positioning Europe at the forefront of blockchain innovation and uptake*"

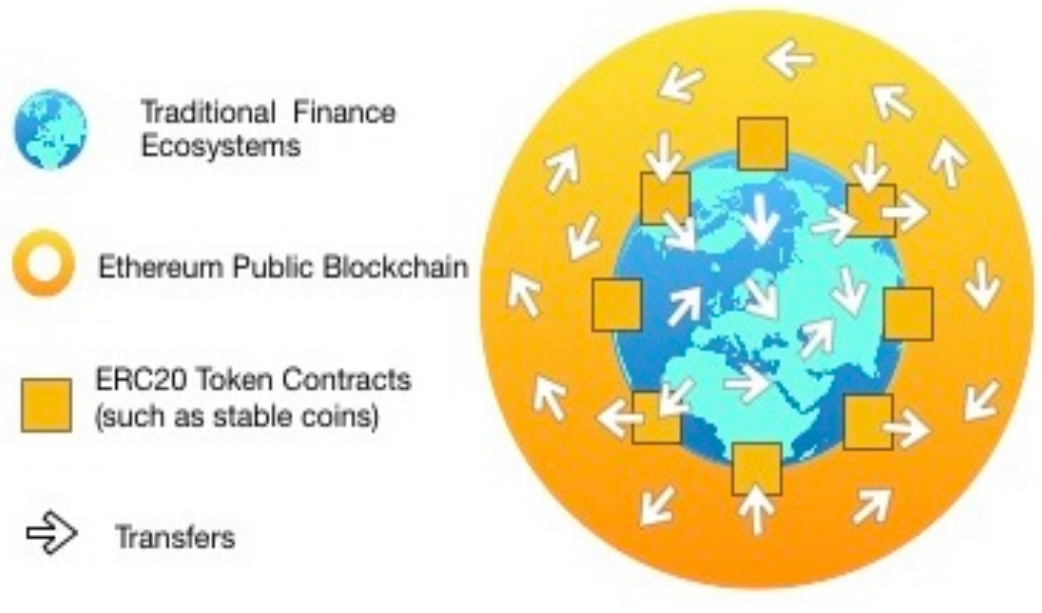
- EC blockchain strategy: https://ec.europa.eu/digital-single-market/en/blockchain-technologies
- European Blockchain Services Infrastructure (EBSI) "a network of distributed nodes across Europe that will deliver cross-border public services "
  - Services: trusted-data sharing, notarization, diplomas, self-sovereign identity
  - Technology: Ethereum Enterprise with the Hyperledger Besu Client and Hyperledger Fabric

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632

Analyzing Blockchain Transaction Graphs for Fraudulent Activities

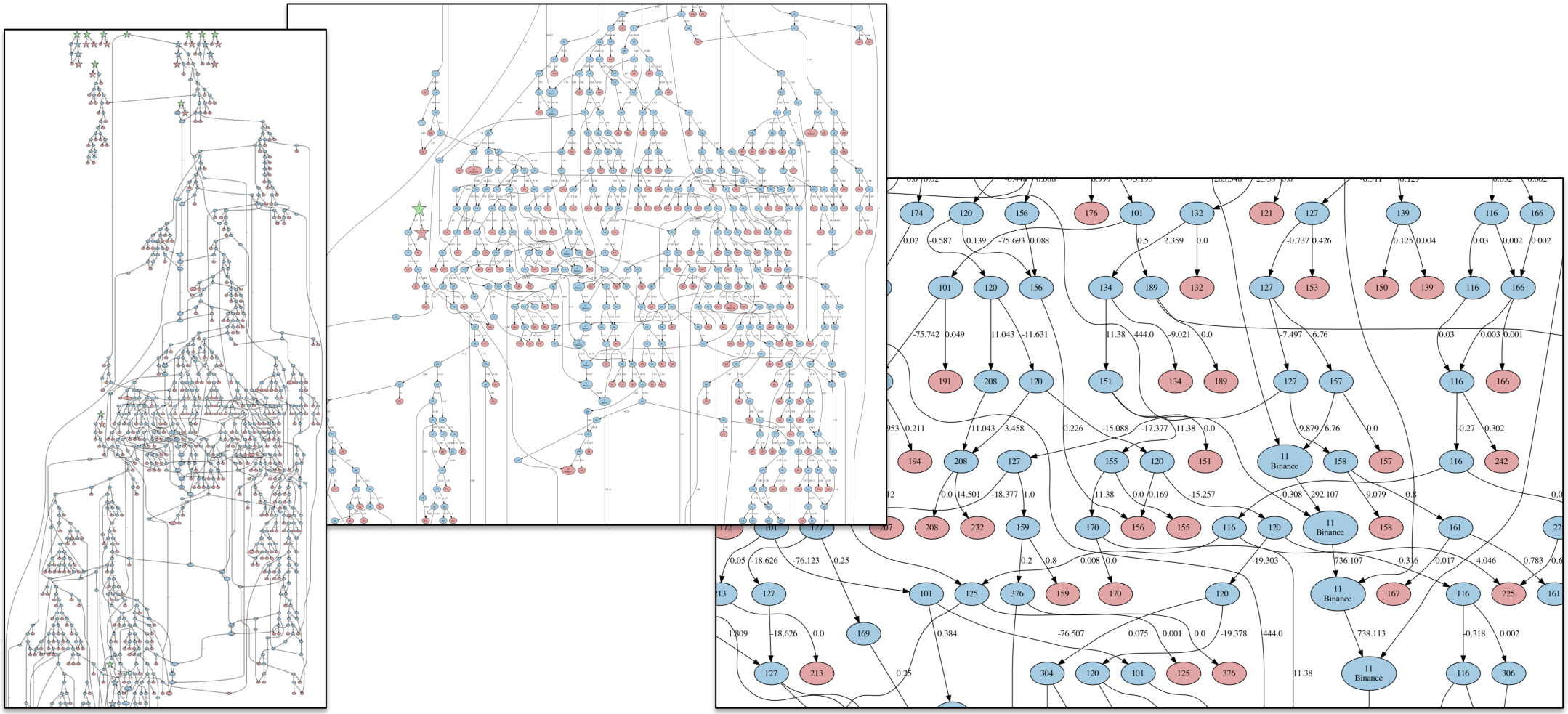
- Blockchain crypto currencies and tokenized assets that are obtained fraudulently can go through various transfers on the blockchain and enter the financial systems in different jurisdictions.

- Infinitech Pilot 9 is developing effective systems for monitoring of blockchain transactions:
  1. Scalable parallel transaction graph construction and analysis tools on an HPC cluster and
  2. User interface that provides transaction graph visualization.



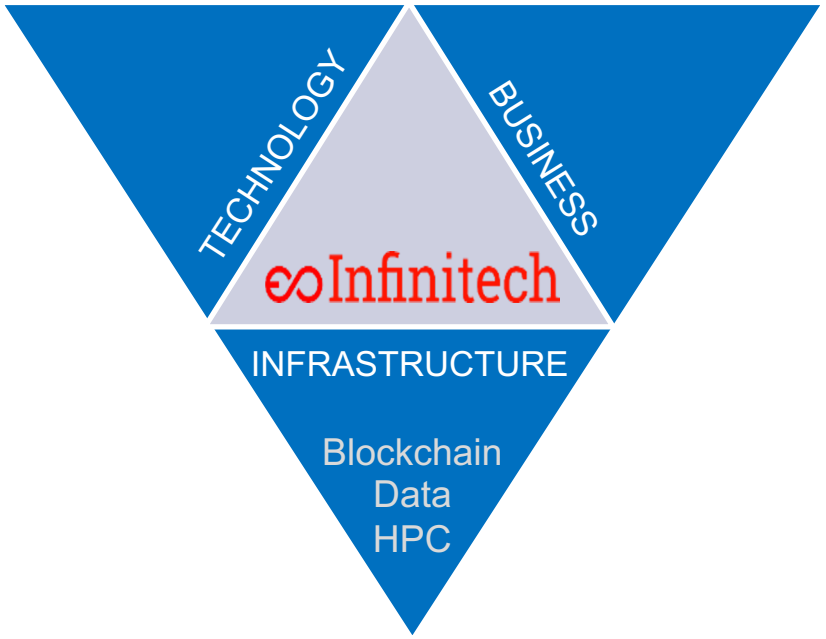
This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632

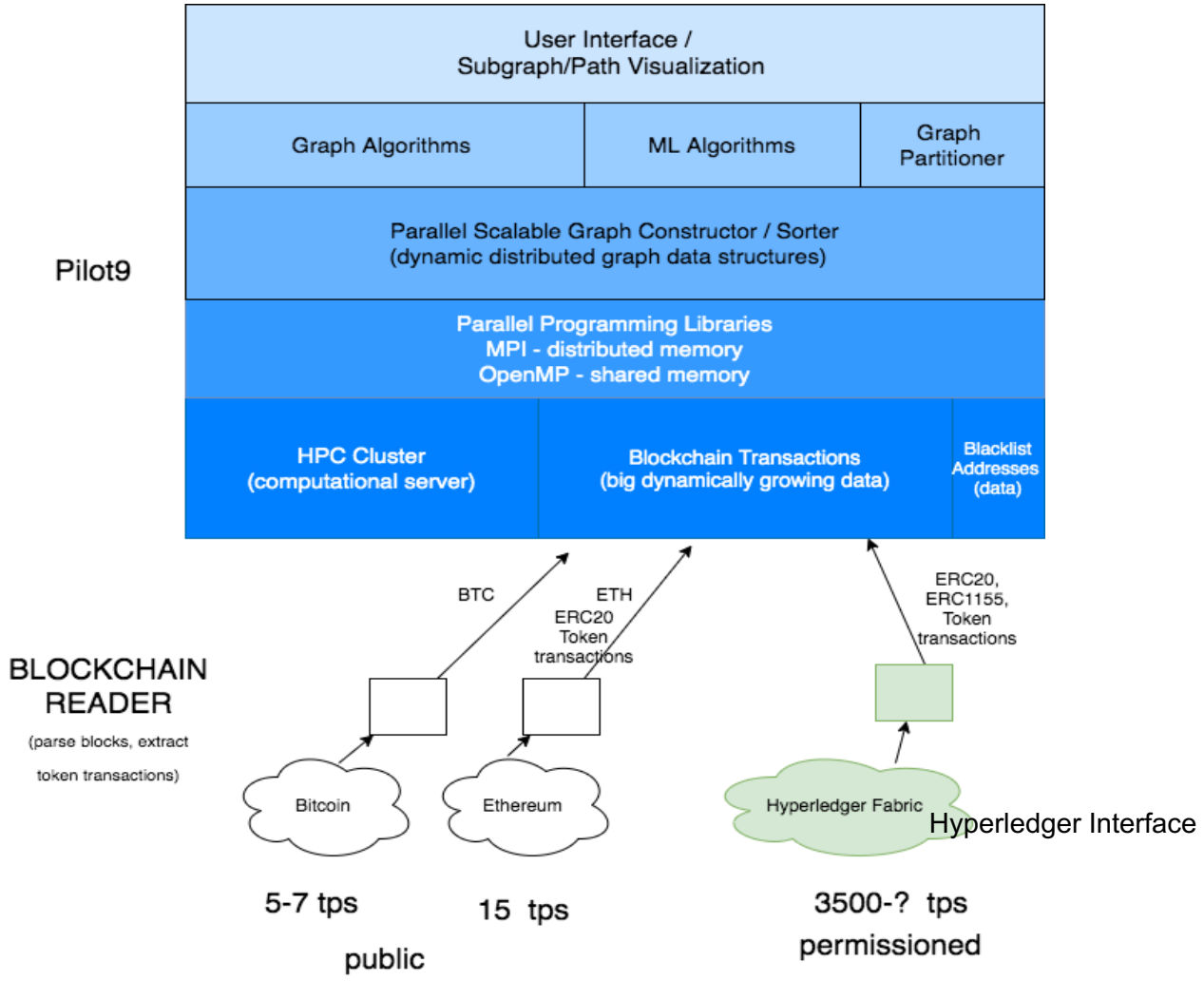
Crypto Asset / Token Transaction Graphs



This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632

Pilot 9 Architecture





This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632

Innovations in the Pilot

- Scalability: HPC
- Faster processing: parallelism
- Accurate results: complete transaction graph analysis
- Cost effective solution : open source libraries
- Other potential uses: IBAN transactions, business intelligence

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632

Technical Innovation

- Big Data management:
  - Ability to manage and process dynamically growing transaction graphs with billions of edges
  - Distributed graph and processing (no single node bottleneck/wall)
- Graph algorithms:
  - Parallel feature extraction on massive graphs to be used in ML
  - Perform traversals on massive graphs and extract subgraphs
  - Scalable graph construction, whole graph operations like PageRank.
- High Performance Computing
  - Developed software using MPI (de-facto parallel programming library for distributed memory programming)
  - System can run on a wide variety of systems ranging from cheap clusters that are formed from office machines on LAN, cloud instances as well as on high end supercomputers
- Blockchain solutions:
  - Process standardized smart token transactions
  - Support ERC20 token contract standard
  - Trace stable coin transactions (national currencies that are provided as ERC20 tokens on Ethereum). These are provided by companies that are regulated with custodian services provided by banks. Examples: (USDT, GUSD, USDC, TRYB)

Parallel Graph Construction

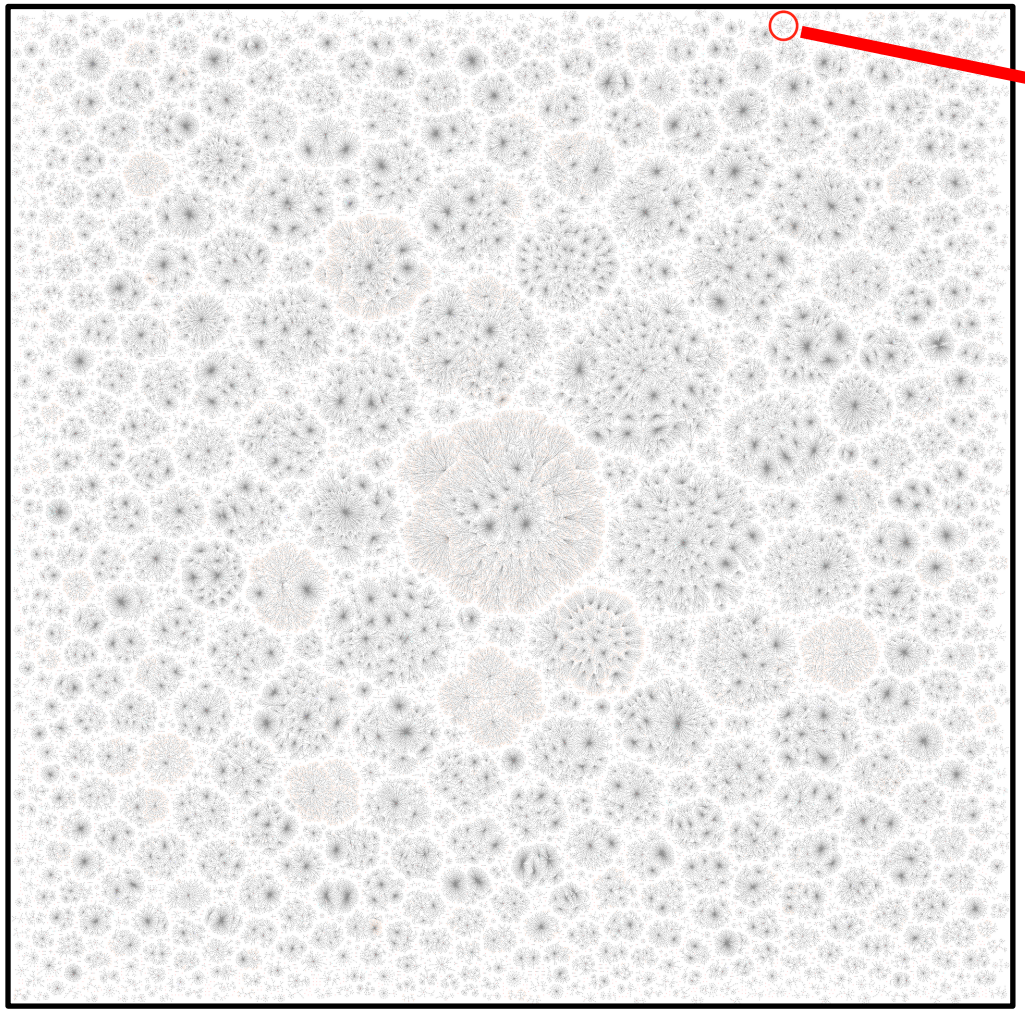
No. of Nodes X No. of processes per node	Total No. of processes	Time (sec)
4 x 1	4	832
8 x 1	8	514
12 x 1	12	483
16 x 1	16	324
16 x 16	256	279

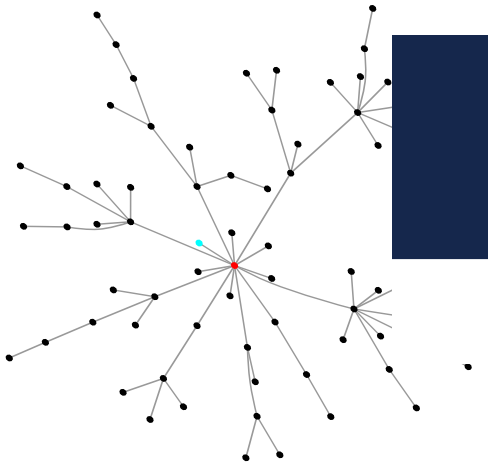
Performance of Parallel Graph Algorithms Ethereum Blockchain Dataset

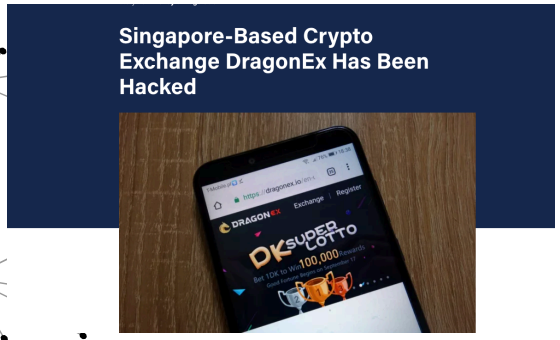
- Using 16 nodes 16 MPI processes, parallel timings for:
  - Distributed transaction graph construction : **279 sec**
  - Pagerank calculation : **130 sec**
  - Metis Partitioning: **3090 sec** (1 MPI process per node)
  - Queries such as degree distribution, summing total number of ERC20 transactions (involving very little communication): **28 sec, 6 sec**
  - Subgraphs showing tracing to fraudulent blacklisted addresses : **2 - 13 sec**
  - Connected components : **164 sec**

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632

Blacklist Address Traces







DragonEx hacker
0xa7f72Bf63EDeCa25636F0B13Ec5135296ca2eBb2

261.4 Ether — Mar-26-2019 05:51:59 AM

0x0Aa773832e0234F360101Cb41f361D5B29265c1E

1 Ether — Mar-26-2019 10:59:01 AM

0x0C4d76487Da235Efd624519a159fC8DEFc8a2eF9

0.995 Ether — Mar-28-2019 06:49:16 AM

0x0ebE87971e2756079279EB490727422D56E852B6

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632

Demo

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 856632