



ELLIPTIC

Blockchain Intelligence and Anonymity

Dr. Adam Joyce

Agenda

Who we are

Bitcoin + Financial compliance

What and who are the entities?

How are entities interacting?

Who we are

Elliptic is (now) a blockchain intelligence company.

We work with financial institutions and law enforcement agencies
to identity illicit activity on the Bitcoin blockchain.

Our team



Dr. James Smith
CEO



Dr. Tom Robinson
COO



Yacoob Kurimbokus
CTO



Dr. Adam Joyce,
Chief Scientist



Kevin Beardsley
Head of Business
Development



Matthew Leon
Senior Software
Engineer



Tuan Anh Le
Software Engineer



Nathan Jessop
Analyst



Dr. Christoph Fretter
Data scientist



Dr. Martin Harrigan
Data scientist

Who we are

Life at a bitcoin startup?...

Agenda

Who we are

Bitcoin + Financial compliance

What and who are the entities?

How are entities interacting?

Bitcoin

- A transparent, global ledger of ownership and value-transfer.
- Decentralized and distributed
- Open and permissionless
- ~150M addresses, ~130M transactions, ~50Gb compressed raw ledger, ~520 .dat block files.
- 82% of txs have < 2 inputs, 89% of txs have < 2 outputs

Bitcoin

Transaction View information about a bitcoin transaction

d3cae27c0bc6613b0ce75628212c60e1133aacfaf7cc243670327757e6b0e9b7

19mastjWtPGXNCYbwDUXKEtMwPGSBNU9LT (0.007187 BTC - Output)
1MgdfLTkL9bHapkiicYzhZ1CjHp3b3f9XT (0.56824276 BTC - Output)



1G7naee3UJxvMcjb574KNB8VfpkSNedRTL - (Unspent) 0.00024276 BTC
1KK81Ao1Ui5yvJUtnp1AZ6U1Q5oNWob3NQ - (Unspent) 0.575 BTC

7 Confirmations

0.57524276 BTC

Summary

Size	372 (bytes)
Received Time	2015-11-25 11:52:03
Included In Blocks	385272 (2015-11-25 11:54:15 + 2 minutes)

Inputs and Outputs

Total Input	0.57542976 BTC
Total Output	0.57524276 BTC
Fees	0.000187 BTC

Agenda

Who we are

Bitcoin + Financial compliance

What and who are the entities?

How are entities interacting?

Financial Comparison

Traditional finance/payments systems

- Very good knowledge of identities (KYC)
- Incomplete knowledge of transactions
- Banking gate-keepers
- National and corporate borders, central bank control.
- Opaque
- Highly regulated

Bitcoin

- Limited knowledge of identities
- Perfect knowledge of transactions
- Open and “permissionless”
- Global system with pre-defined monetary supply
- Transparent
- Traditional regulation being applied

Theft



Dark Marketplaces



messages 1 | orders 0 | account \$0.00

Search

Go

Shop by Category

Drugs 2,399

Cannabis 341

Dissociatives 65

Ecstasy 209

Opioids 156

Other 144

Precursors 12

Prescription 526

Psychedelics 427

Stimulants 273

Apparel 114

Art 7

Books 743

Collectibles 12

Computer equipment 19

Custom Orders 26

Digital goods 310

Drug paraphernalia 89

Electronics 20

Erotica 319

Fireworks 2

Food 3

Forgeries 58

Hardware 2

Home & Garden 7

Jewelry 48

Lab Supplies 5

Lotteries & games 29

Medical 5



5x - 10mg Dexedrine (Pure Dextroamphetamine)

\$4.94



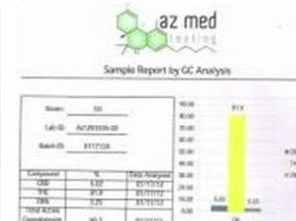
2 x 0,25 mg Xanax (Alprazolam)

\$1.50



Malana charas hand rubbed Indian hash 100g

\$75.83



1 Gram OG KUSH OIL 81% THC 90% TOTAL

\$4.13



14 grams (1/2 Ounce) of Nebula JWH-122

\$2.63



3.5g Crystal Meth Ice Shards

\$31.92



20 x 25mg Cialis

\$2.57



!!!...Psilocybe-Cubensis-Chocolate...!!!

\$18.15



100 x Orange Star Very high MDMA content 180mg



100x 200mg White XTC 'Speakers'



3g Methylone Crystals -\$50- Lab Grade



15mg Adderall Extended Release (1 Capsule)

Ransomware / Extortion

hello,

Unfortunately, your data was leaked in the recent hacking of Ashley Madison and I now have your information.

If you would like to prevent me from finding and sharing this information with your significant other send exactly 1.0000001 Bitcoins (approx. value \$225 USD) to the following address:

1B8eH7HR87vbVbMzX4gk9nYyus3KnXs4Ez [link added]

Sending the wrong amount means I won't know it's you who paid.

You have 7 days from receipt of this email to send the BTC [bitcoins]. If you need help locating a place to purchase BTC, you can start here.....

Financial Regulation

- Consumer protection issues
- Risk of criminal misuse
- Do existing frameworks 'fit' cryptocurrencies?
- Will compliance costs kill the industry? How to balance innovation vs. risk?

Regulatory challenges around identity + ownership

On a blockchain, everybody looks the same.

This perception of anonymity presents a new world of problems for money laundering, fraud and other criminal activity.

How to deal with identity on a blockchain?

The Immediate Problem

All enterprises that handle digital currency
must comply with anti-money laundering regulation.

The inability to identify proceeds of crime is a major roadblock
for enterprises that wish to engage with blockchains.

“HSBC Breaks Ties with Bitcoin Fund Over Money Laundering Concerns”
- Inside Bitcoins

“FinCEN Fines Ripple Labs Over AML”
- American Banker

Agenda

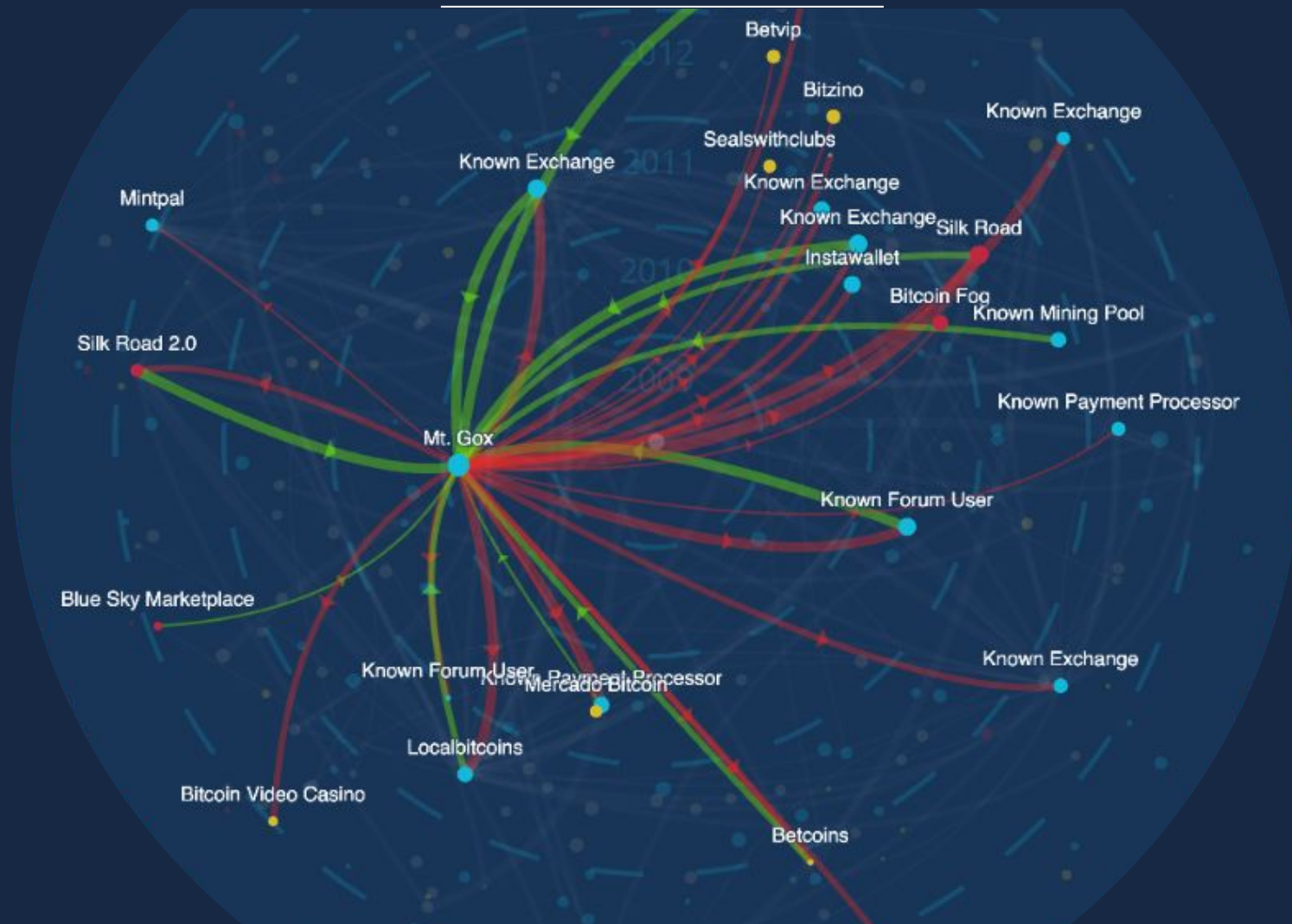
Who we are

Bitcoin + Financial compliance

What and who are the entities?

How are entities interacting?

Identifying Clusters

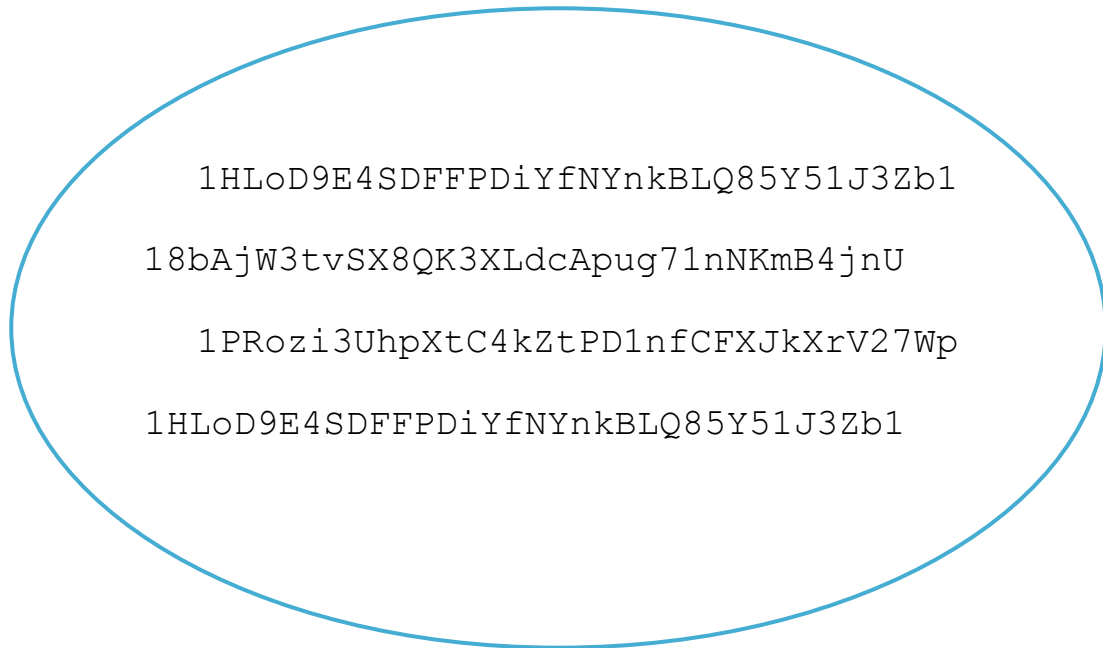


Beyond Pseudonyms - Mapping the Blockchain

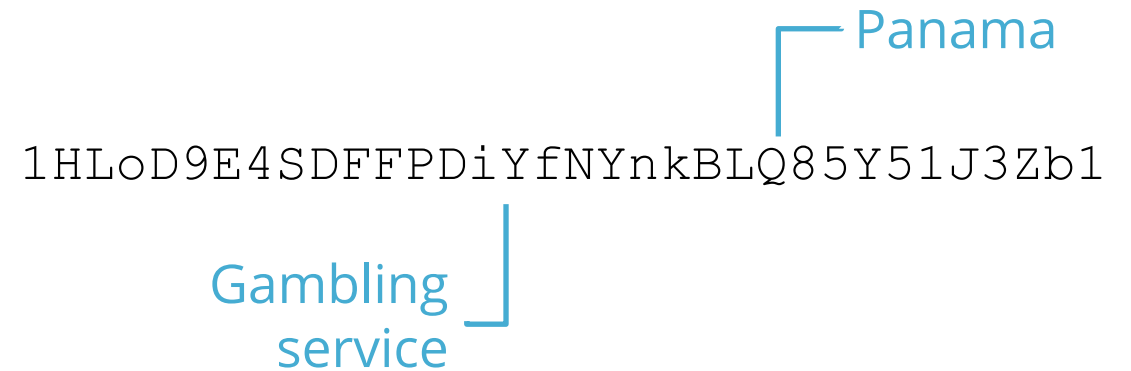


Beyond Pseudonyms

Clustering



Tagging



Clustering

Transaction View information about a bitcoin transaction

d3cae27c0bc6613b0ce75628212c60e1133aacfaf7cc243670327757e6b0e9b7

19mastjWtPGXNCYbwDUXKEtMwPGSBNU9LT (0.007187 BTC - Output)
1MgdfLTkL9bHapkiicYzhZ1CjHp3b3f9XT (0.56824276 BTC - Output)



1G7naee3UJxvMcjb574KNB8VfpkSNedRTL - (Unspent) 0.00024276 BTC
1KK81Ao1Ui5yvJUtnp1AZ6U1Q5oNWob3NQ - (Unspent) 0.575 BTC

7 Confirmations

0.57524276 BTC

Summary

Size	372 (bytes)
Received Time	2015-11-25 11:52:03
Included In Blocks	385272 (2015-11-25 11:54:15 + 2 minutes)

Inputs and Outputs

Total Input	0.57542976 BTC
Total Output	0.57524276 BTC
Fees	0.000187 BTC

Clustering



Clustering

1HLoD9E4SDFFPDiYfNYnkBLQ85Y51J3Zb1

18bAjW3tvSX8QK3XLdcApug71nNKmB4jnU

1PRozi3UhpXtC4kZtPD1nfCFXJkXrV27Wp

1LVjAedtEDShR4zVNL2thjPKZ9dooEhkZ6

1B2m9g77KvqUdfzL8dG3y8aoMWCrh5LfZ6

1PcFKvehsUgdrkjynZDL1oSMmZ5CXgkHVo

1EXoDusjGwvnjZUyKkxZ4UHEf77z6A5S4P

1HLoD9E4SDFFPDiYfNYnkBLQ85Y51J3Zb1

13m4qvDLNXaYTLxG9i7y6bNWARZAdigDSV

1Po1oWkD2LmodfkBYiAktwh76vkF93LKnH

1KubhW6wcoqHd2aEoSsUASjUTFTBDQCNe1

?

Author

Top

theymos

Administrator

Legendary

Activity: 1680

Today's content

The account is now then

Don't (Ever)

I won't make Naka

1NXYo

coinbase

WALLET

Send/Request

Buy/Sell

Recurring Payments

Account Settings

MERCHANT TOOLS

Orders

Subscribers

Tools

Merchant Settings

Complete your profile

Next step: verify your phone

Tagging

h payment on

omated

ate New Address

Details

All times are UTC (Coor

Tagging

SILK ROAD

1LVjAedtEDShR4zVNL2thjPKZ9dooEhkZ6

1B2m9g77KvqUdfzL8dG3y8aoMWCrh5LfZ6

1BeNFUd2GhQJBriFQLLib58eVrpTT1fjQX

1PVWtK1ATnvbRaRceLRH5xj8XV1LxUBu7n

COINBASE

1HLoD9E4SDFFPDiYfNYnkBLQ85Y51J3Zb1

18bAjW3tvSX8QK3XLdcApug71nNKmB4jnU

1PRozi3UhpXtC4kZtPD1nfCFXJkXrV27Wp

1PcFKvehsUgdrkjynZDL1oSMmZ5CXgkHVo

1HLoD9E4SDFFPDiYfNYnkBLQ85Y51J3Zb1

1PcFKvehsUgdrkjynZDL1oSMmZ5CXgkHVo

1EXoDusjGwvnjZUyKkxZ4UHEf77z6A5S4P

THIEF

18VTYnVUZ8BhNi6verG67eSwKcidyeMVku

13m4qvDLNXaYTLxG9i7y6bNWARZAdigDSV

1Po1oWkD2LmodfkBYiAktwh76vkF93LKnH

1KubhW6wcoqHd2aEoSsUASjUTFTBDQCNe1

Agenda

Who we are

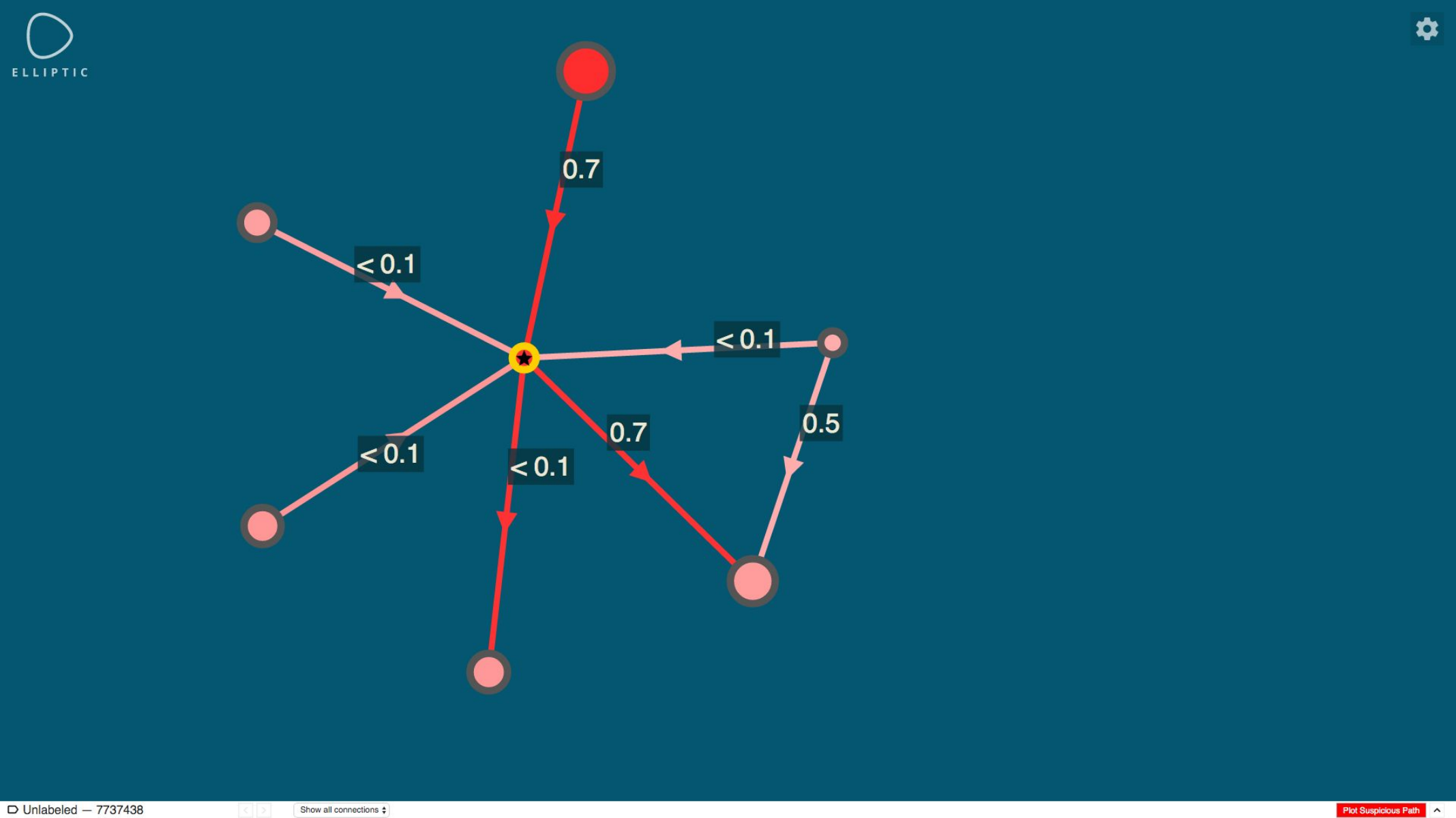
Bitcoin

Financial compliance

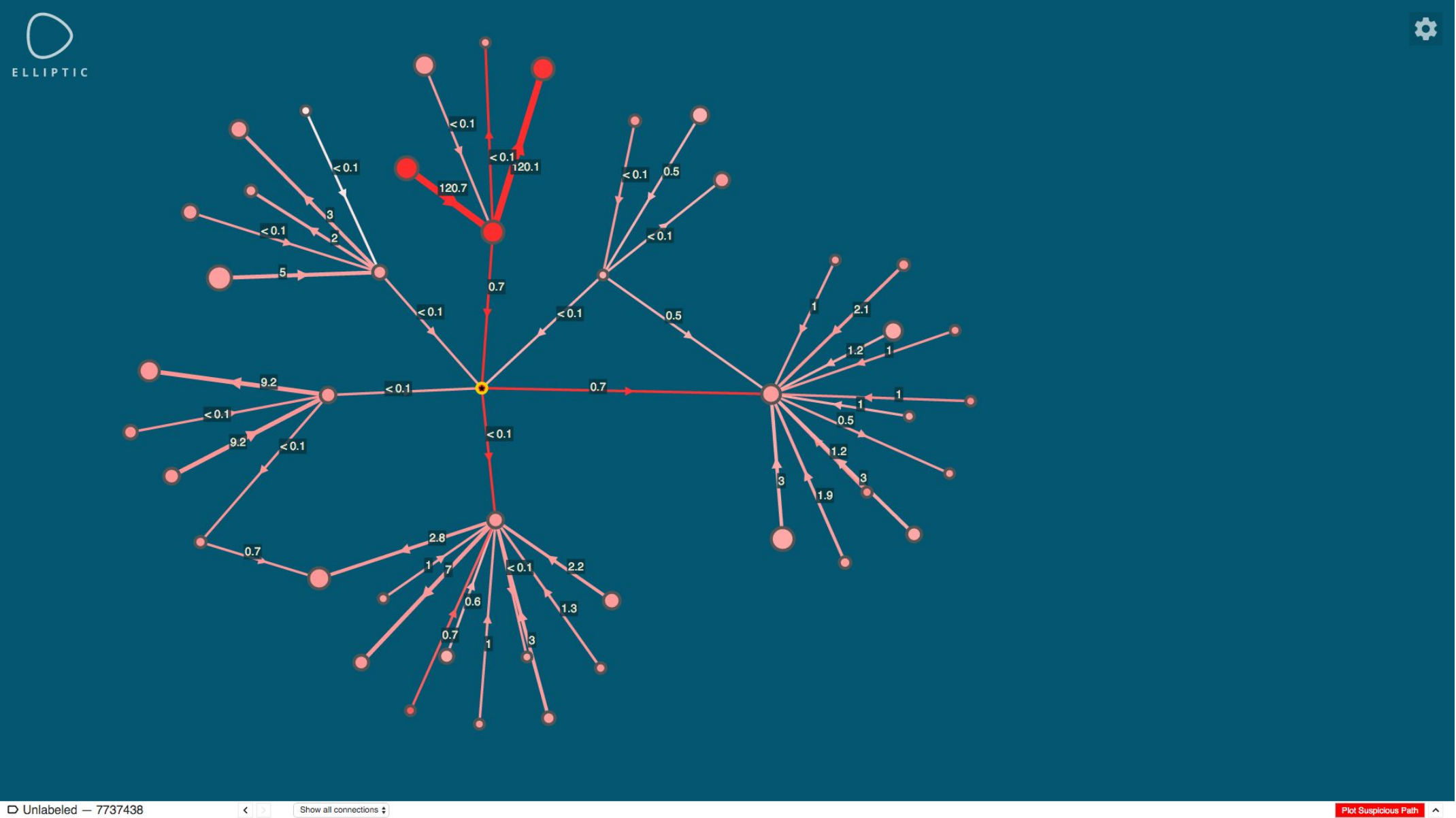
What and who are the entities?

How are entities interacting?

One hop: 6 counterparties



Two hops: 37 entities



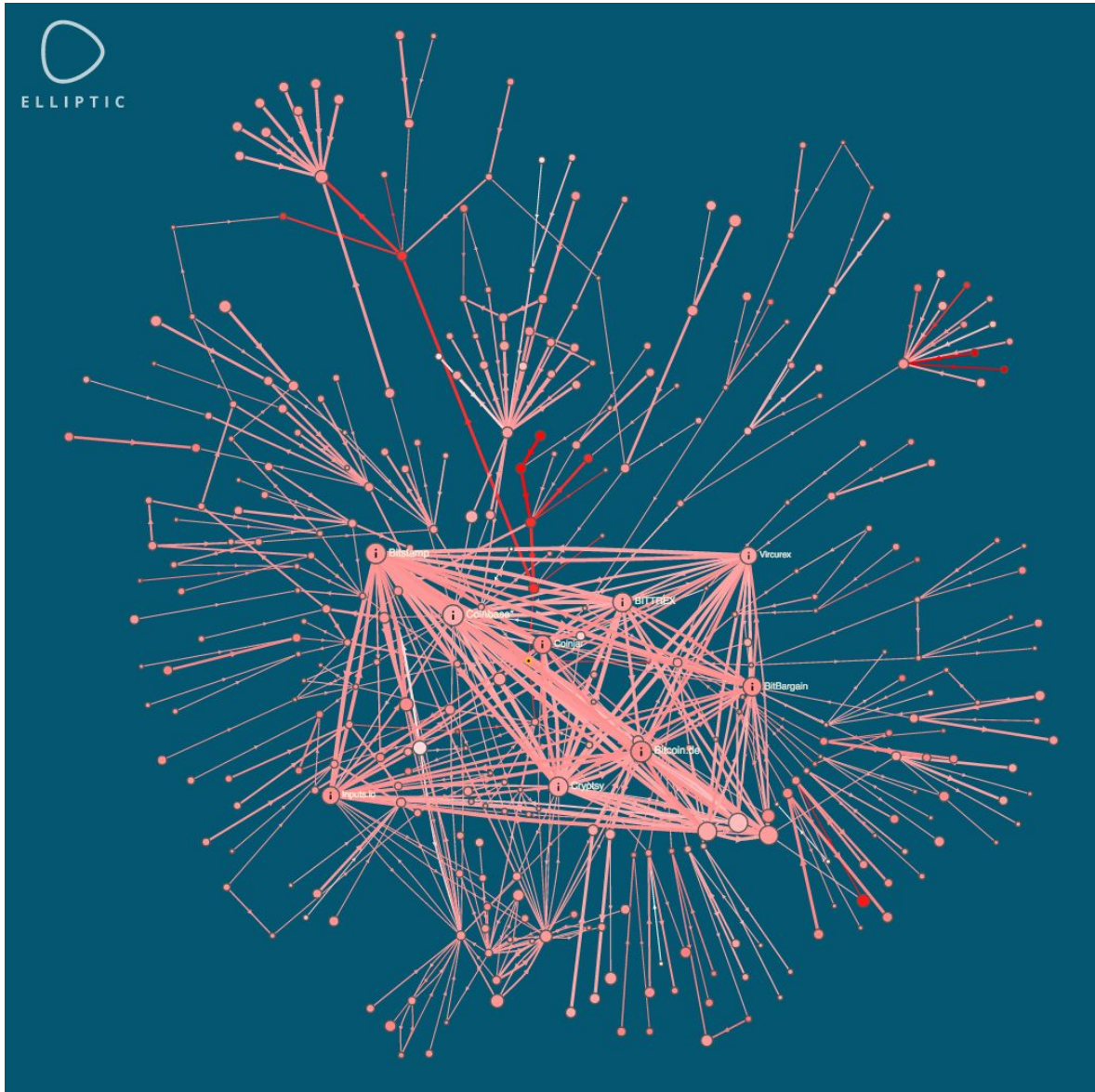
Three hops: 131 entities



Four hops: Many entities



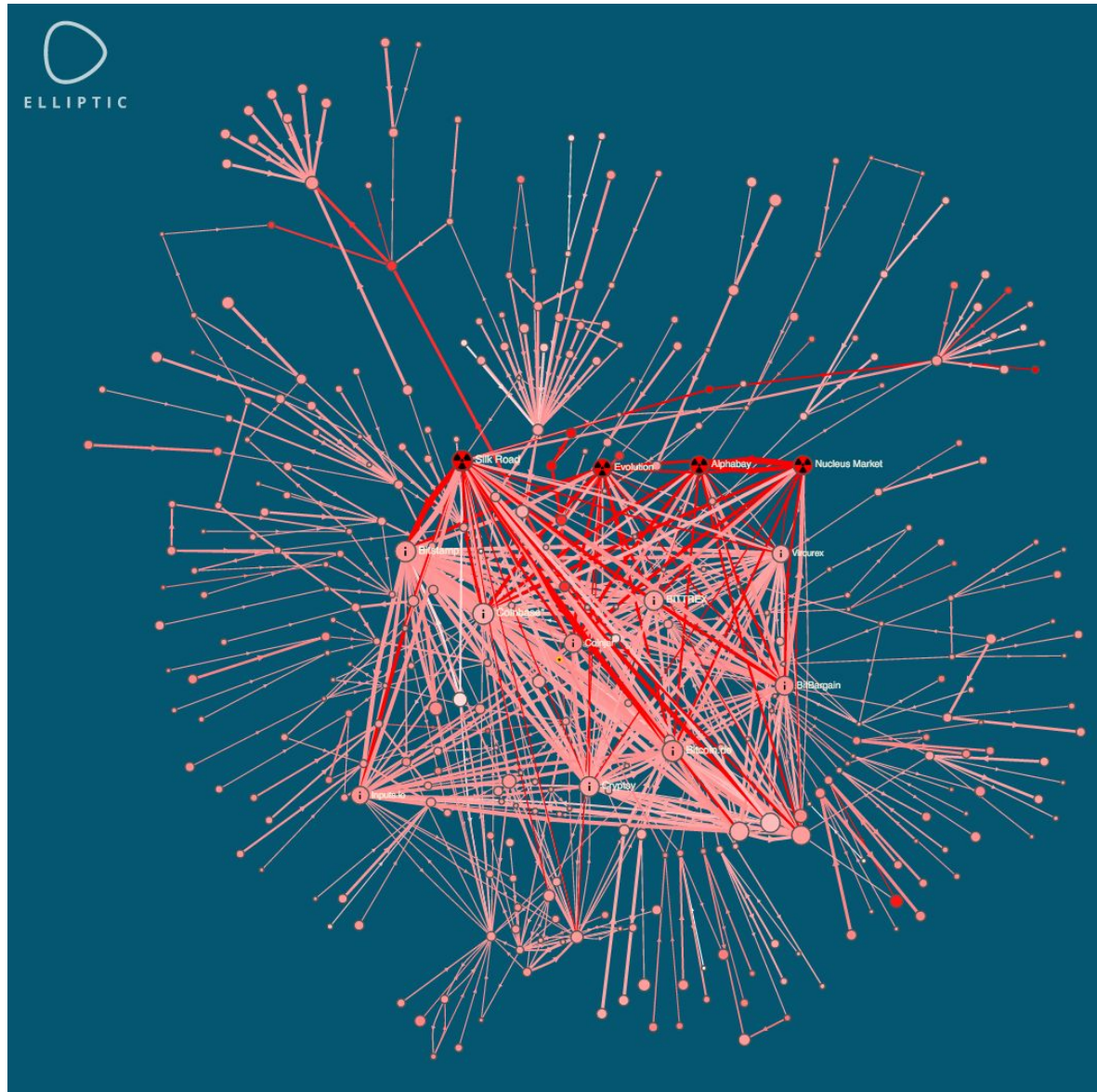
Hitting exchanges complicates the graph.



Exchanges are highly connected nodes.

1. How do you quickly decipher the connection?
2. How do you know if the connection is important?

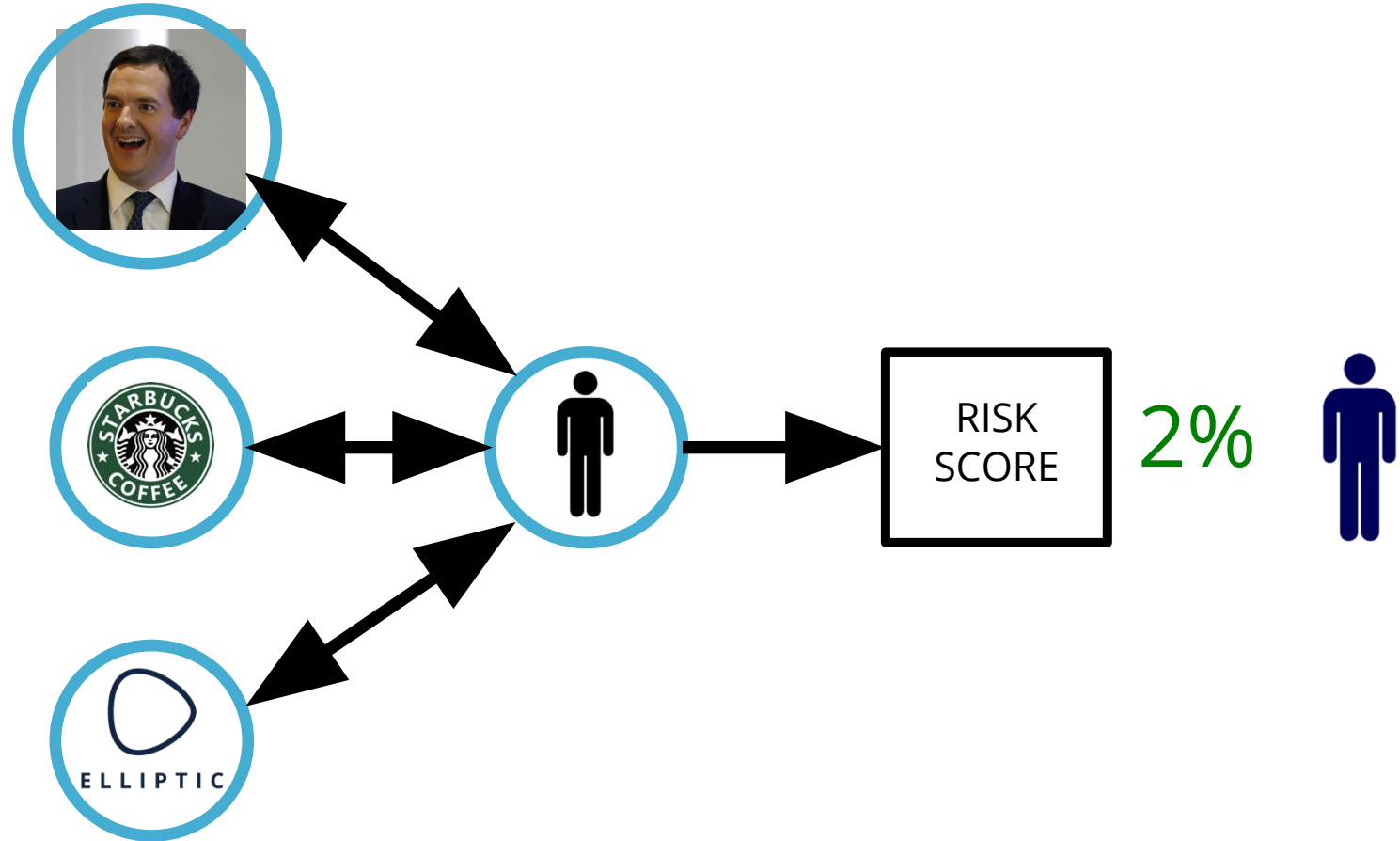
Adding dark markets makes it even more complicated



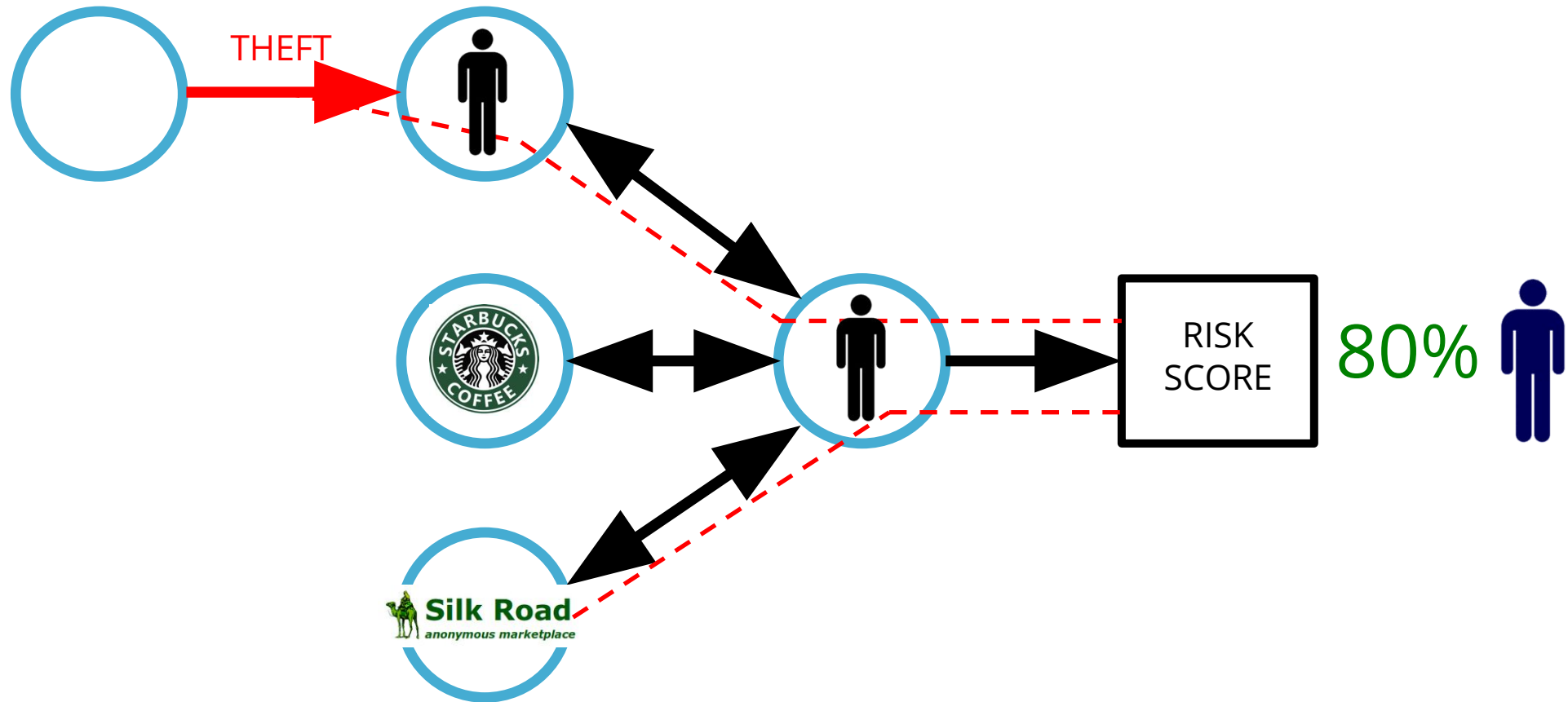
Dark marketplaces are represented with the red ‘nuclear’ symbol.

1. Which connections are more important now?

Risk-scoring of entities, transactions



Risk-scoring of entities, transactions



“Towards Risk Scoring of Bitcoin Transactions”, Malte Moser et al. (2014)

Project ideas! Work with us!

- Just how rich is Satoshi?
- On a blockchain, does anybody know you're a fridge?
- Is it all just in Silicon Valley?
- Will Elliptic have to use Spark eventually?
- How many txs are just in \$\$\$?



