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?

ELLIPTIC

Who we are

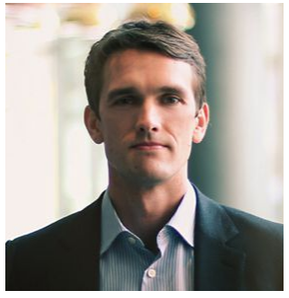
Elliptic is (now) a blockchain intelligence company.

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

ELLIPTIC

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

ELLIPTIC

Who we are

Life at a bitcoin startup?...

ELLIPTIC

Agenda

Who we are

Bitcoin + Financial compliance

What and who are the entities?

How are entities interacting?

ELLIPTIC

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

ELLIPTIC

Bitcoin

Transaction View information about a bitcoin transaction

d3cae27c0bc6613b0ce75628212c60e1133aacfaf7cc243670327757e6b0e9b7

19mastjWtPGXNCYbwDUXKEtMwPGSBNU9LT (0.007187 BTC - Output)	1G7naee3UJxvMcjb574KNB8VfpkSNedRTL - (Unspent)	0.00024276 BTC
1MgdfLTkL9bHapkiicYzhZ1CjHp3b3f9XT (0.56824276 BTC - Output)	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

ELLIPTIC

Agenda

Who we are

Bitcoin + Financial compliance

What and who are the entities?

How are entities interacting?

ELLIPTIC

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

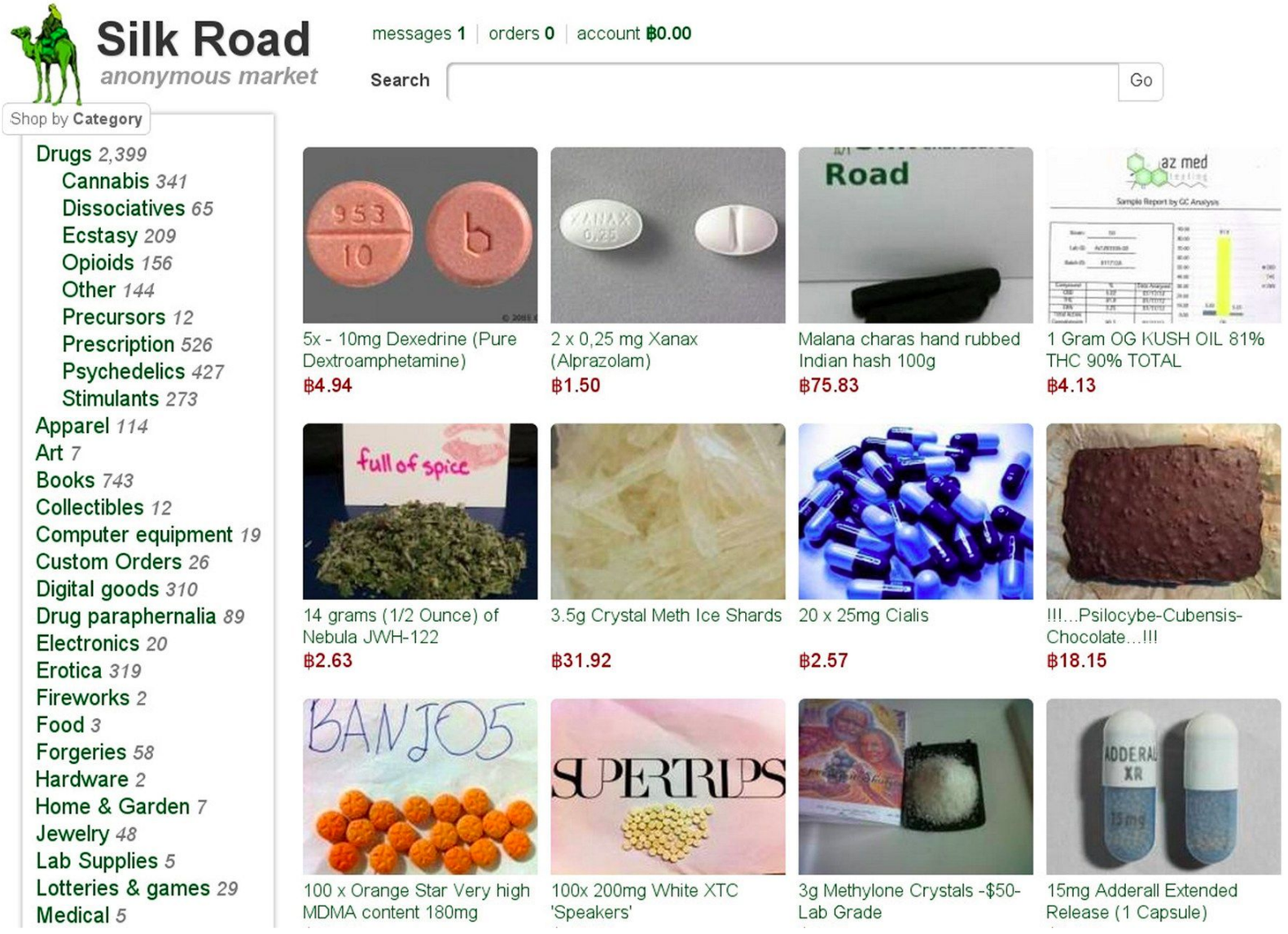
- Limited knowledge of identities
- Perfect knowledge of transactions
- Open and “permissionless”
- Global system with pre-defined monetary supply
- Transparent
- Traditional regulation being applied

ELLIPTIC

Theft

ELLIPTIC

Dark Marketplaces



ELLIPTIC

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.....

ELLIPTIC

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?

ELLIPTIC

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?

ELLIPTIC

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

ELLIPTIC

Agenda

Who we are

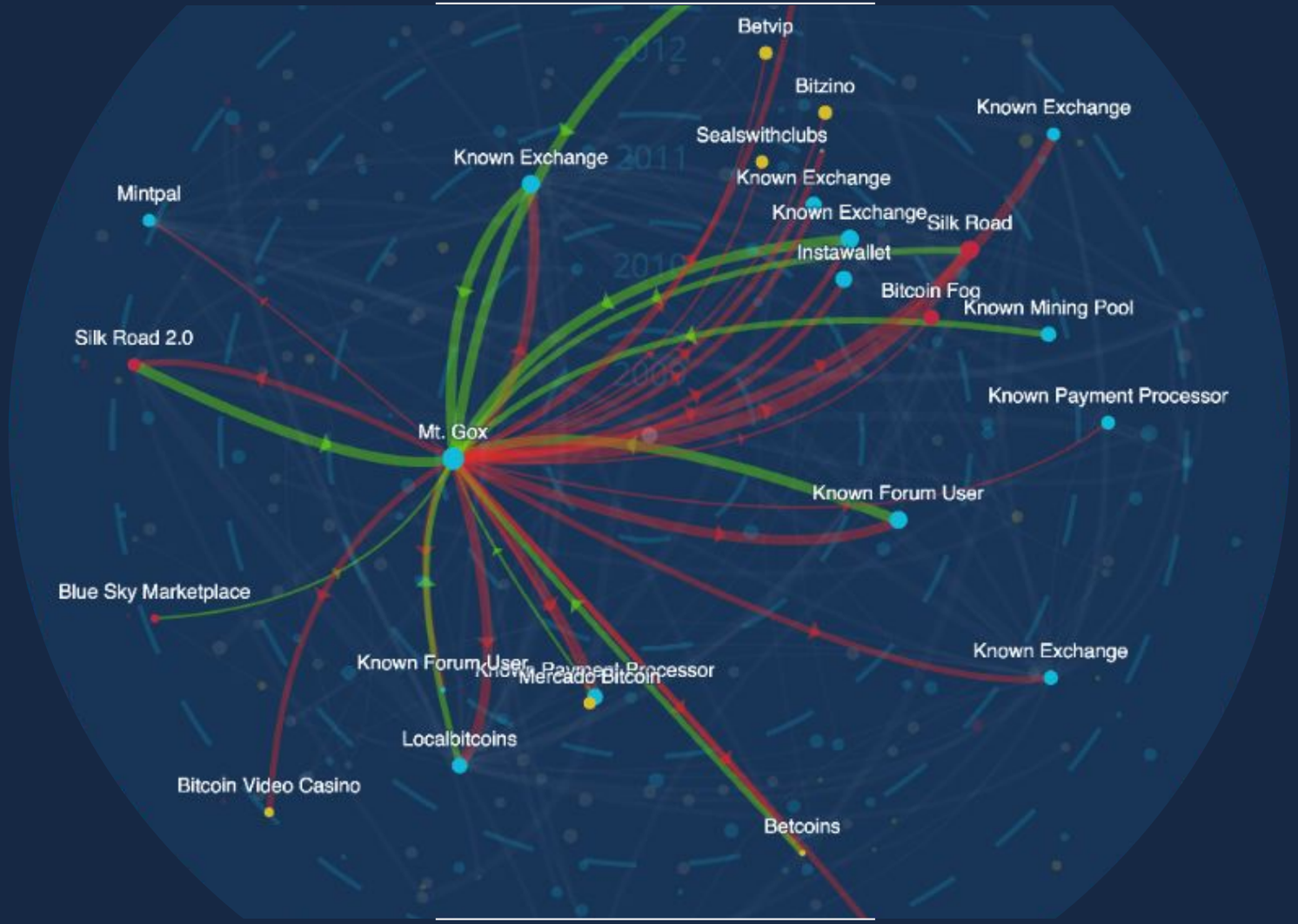
Bitcoin + Financial compliance

What and who are the entities?

How are entities interacting?

ELLIPTIC

Identifying Clusters



ELLIPTIC

Beyond Pseudonyms - Mapping the Blockchain

ELLIPTIC

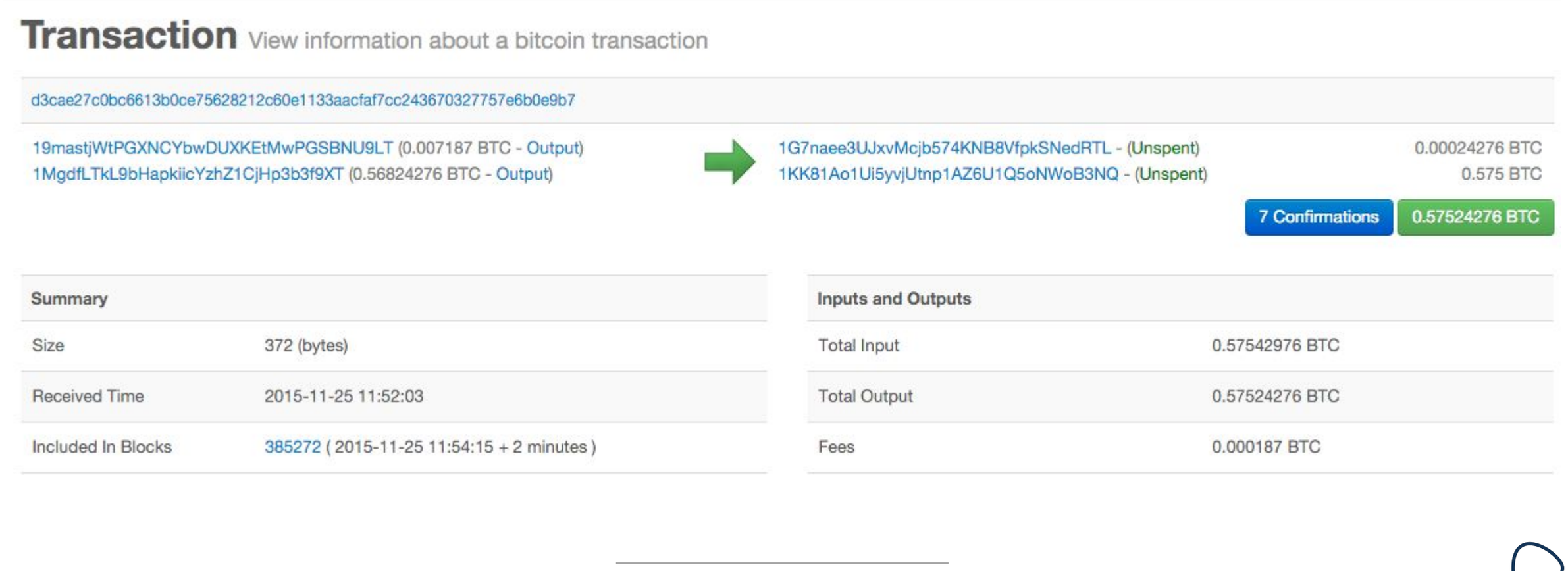
Beyond Pseudonyms

Clustering

Tagging

ELLIPTIC

Clustering



Transaction View information about a bitcoin transaction

d3cae27c0bc6613b0ce75628212c60e1133aacfaf7cc243670327757e6b0e9b7

19mastjWtPGXNCYbwDUXKEtMwPGSBNU9LT (0.007187 BTC - Output)	1G7naee3UJxvMcjb574KNB8VfpkSNedRTL - (Unspent)	0.00024276 BTC
1MgdfLTkL9bHapkiicYzhZ1CjHp3b3f9XT (0.56824276 BTC - Output)	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

ELLIPTIC

Clustering

ELLIPTIC

Clustering

1HLoD9E4SDFFPDiYfNYnkBLQ85Y51J3Zb1

18bAjW3tvSX8QK3XLdcApug71nNKmB4jnU

1PRozi3UhpXtC4kZtPD1nfCFXJkXrV27Wp

1LVjAedtEDShR4zVNL2thjPKZ9dooEhkZ6

1B2m9g77KvqUdfzL8dG3y8aoMWCrh5LfZ6

1PcFKvehsUgdrkjynZDL1oSMmZ5CXgkHVo

1EXoDusjGwvnjZUyKkxZ4UHEf77z6A5S4P

1HLoD9E4SDFFPDiYfNYnkBLQ85Y51J3Zb1

?

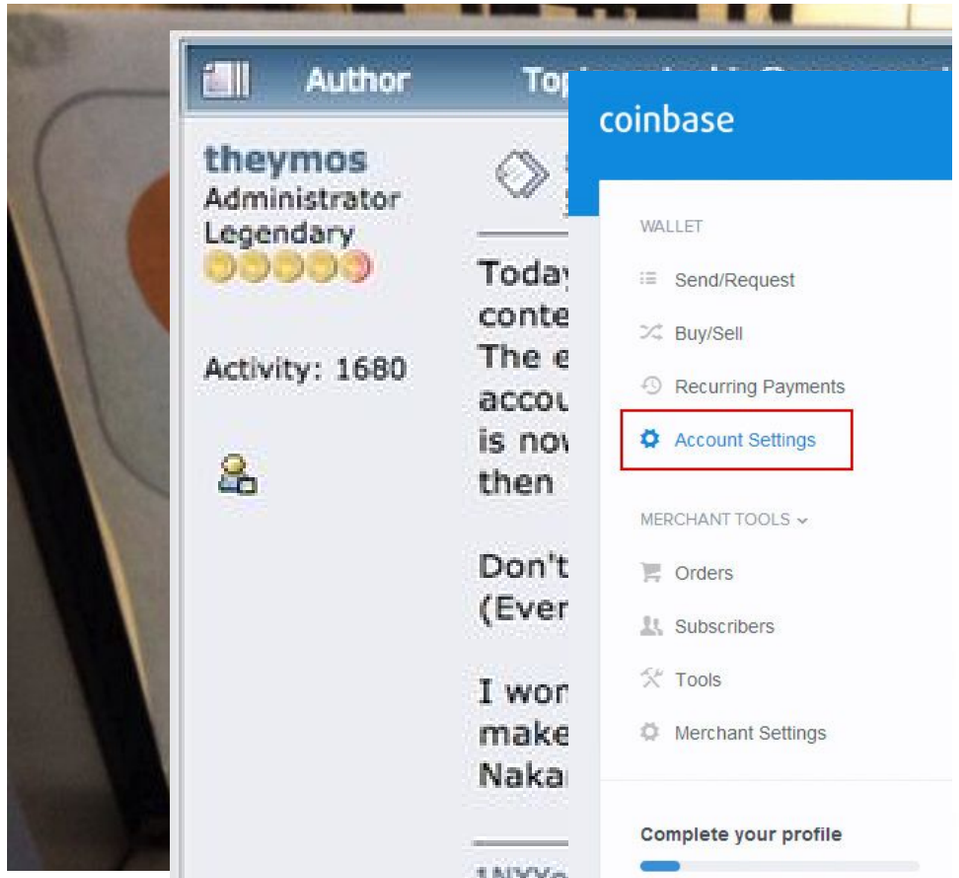
13m4qvDLNXaYTLxG9i7y6bNWARZAdigDSV

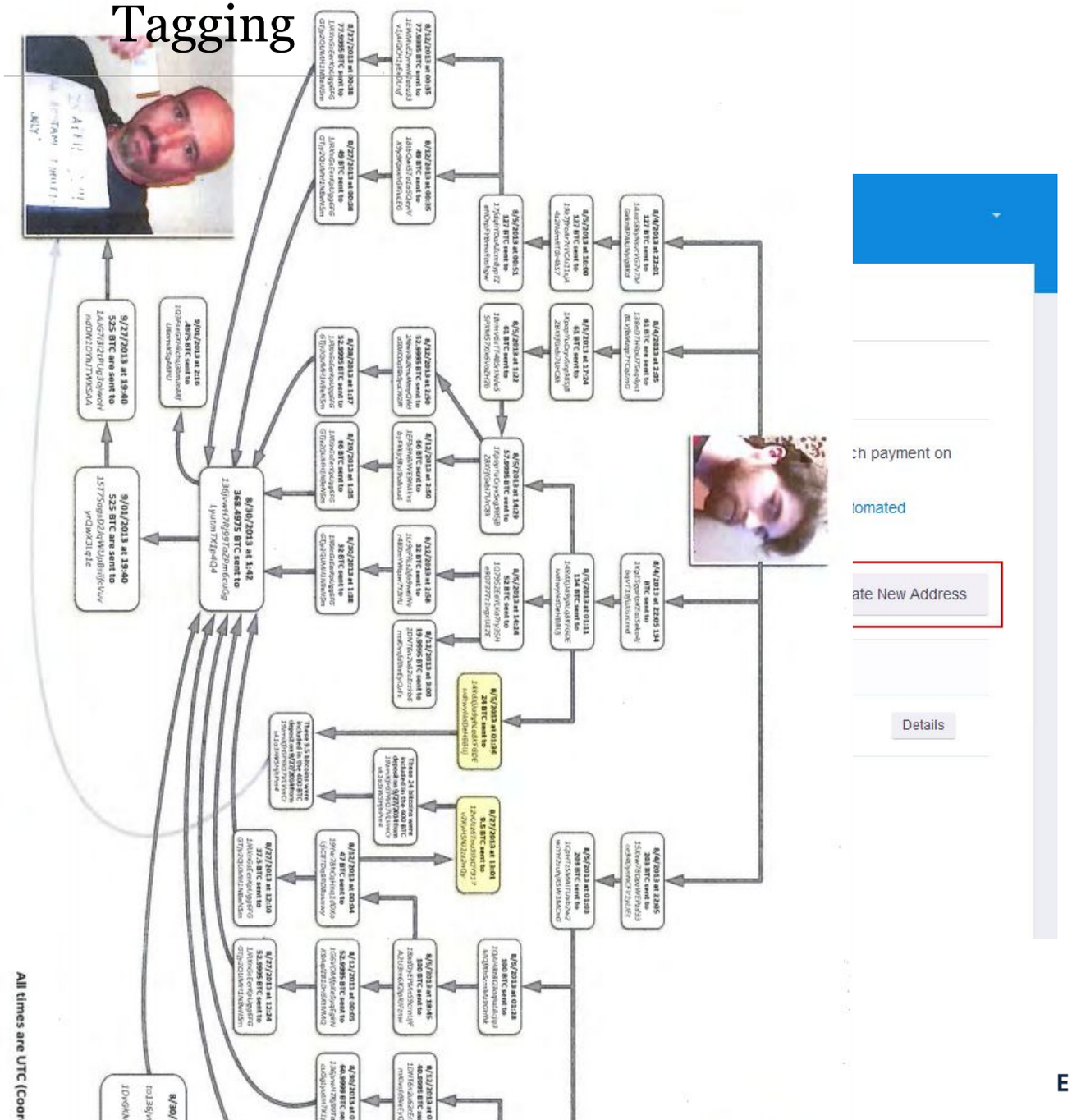
1Po1oWkD2LmodfkBYiAktwh76vkF93LKnh

1KubhW6wcoqHd2aEoSsUASjUTFTBDQCNe1

ELLIPTIC

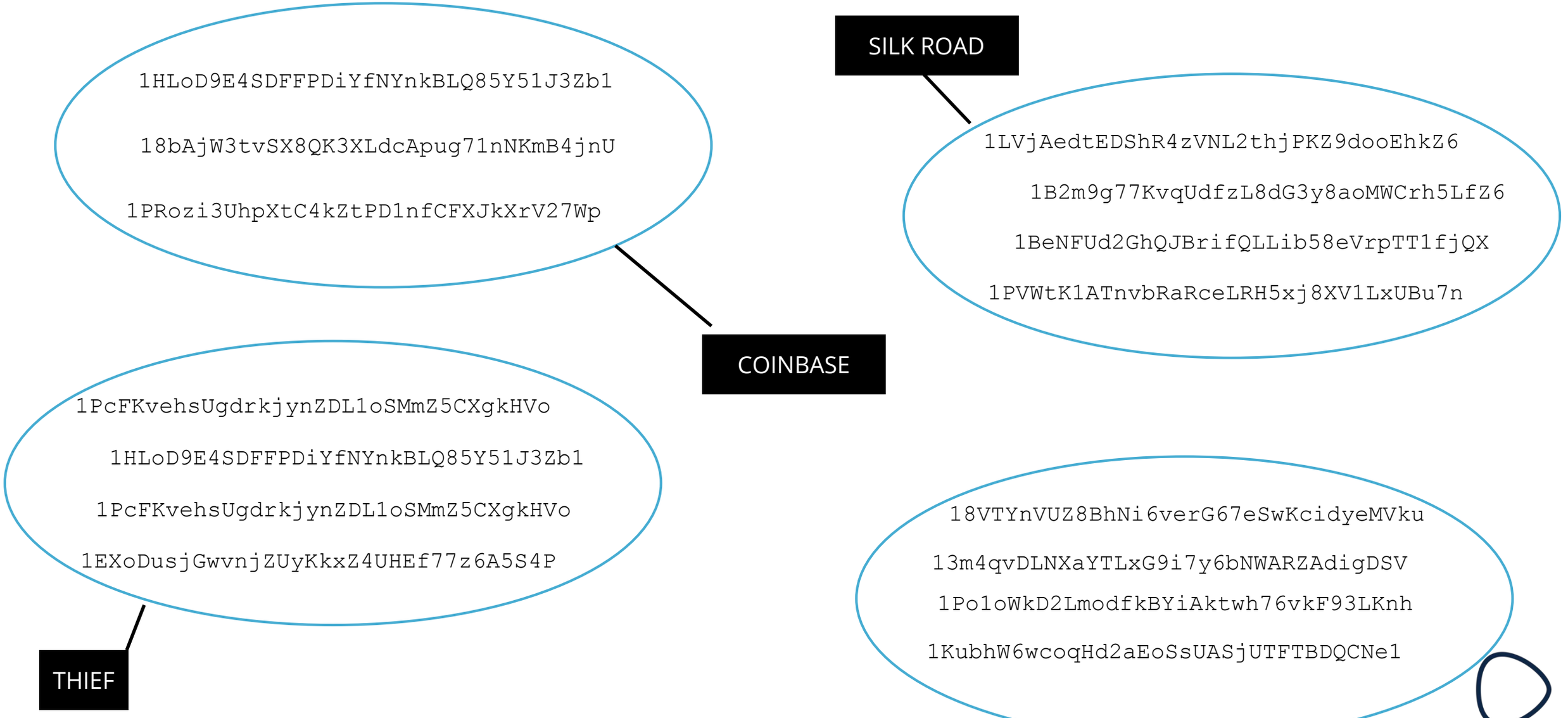
Tagging





ELLIPTIC

Tagging



ELLIPTIC

Agenda

Who we are

Bitcoin

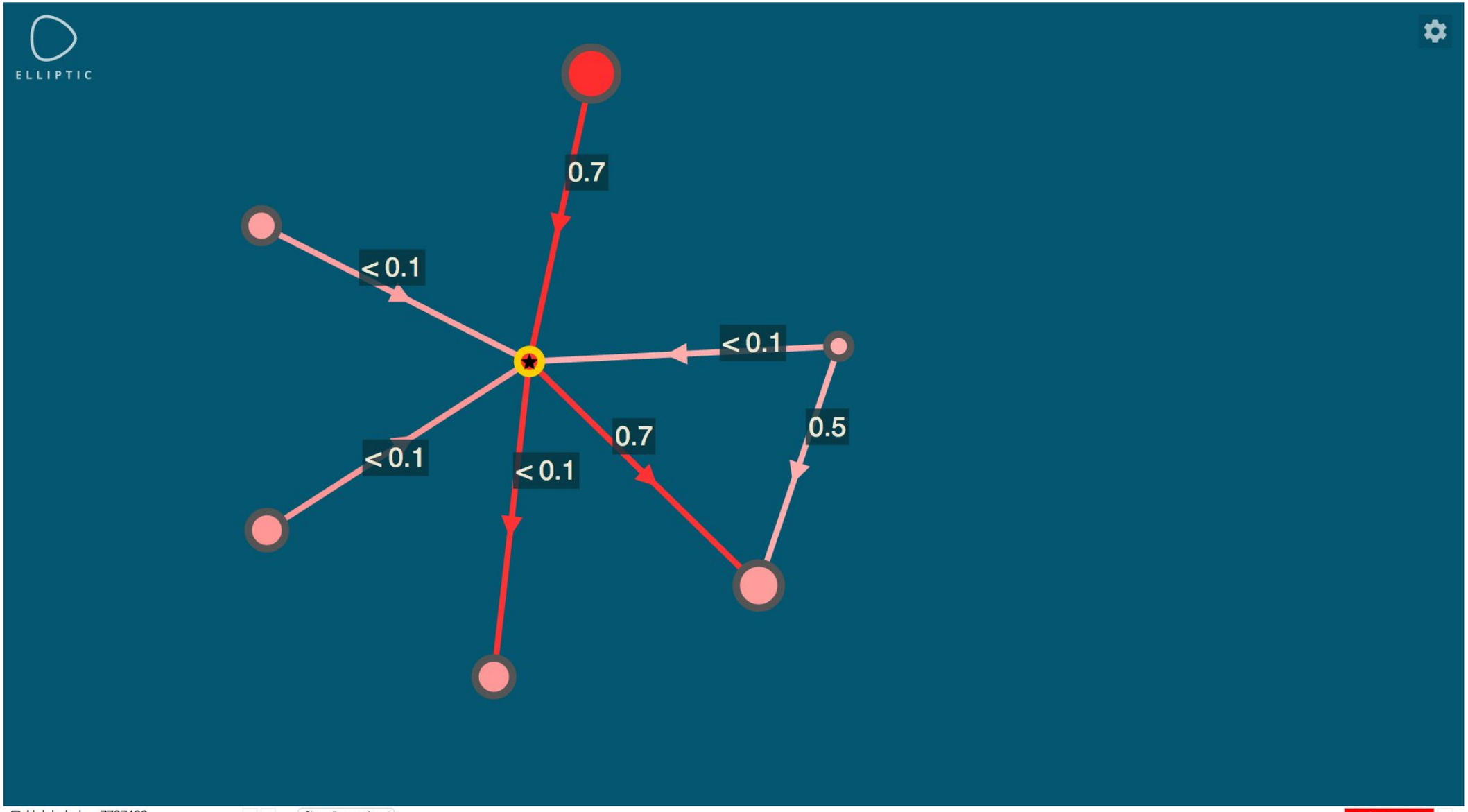
Financial compliance

What and who are the entities?

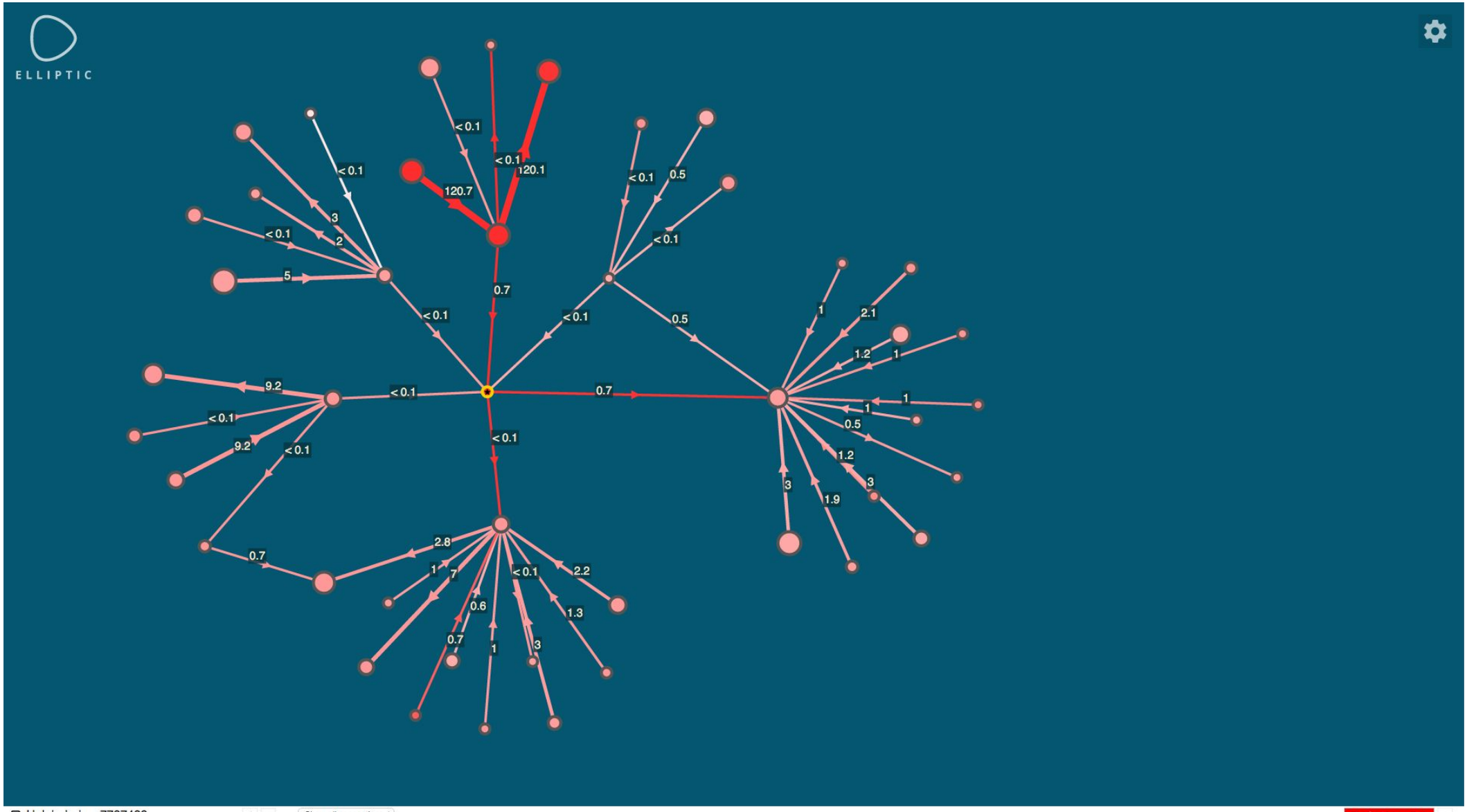
How are entities interacting?

ELLIPTIC

One hop: 6 counterparties



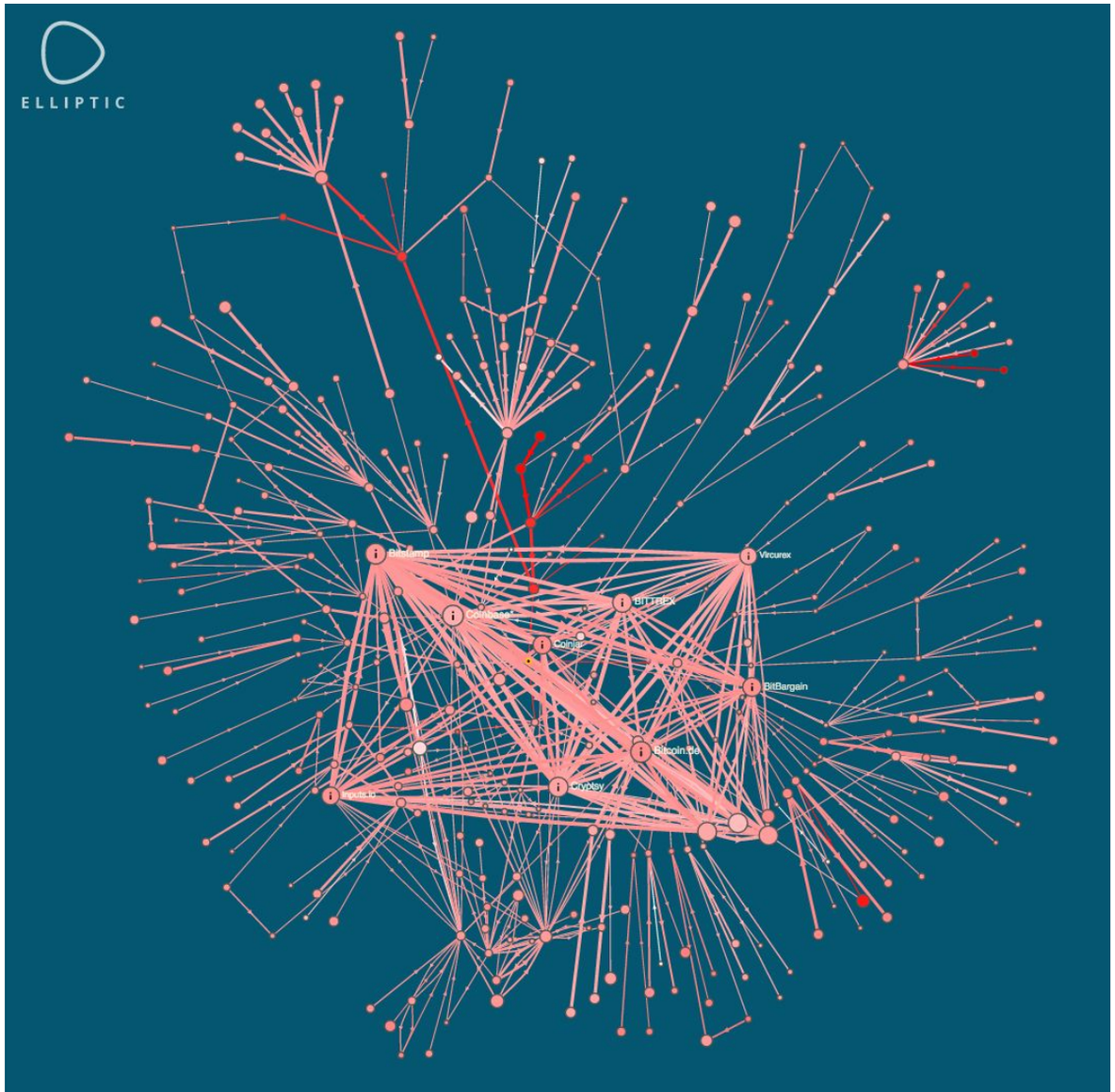
Two hops: 37 entities



Three hops: 131 entities

Four hops: Many entities

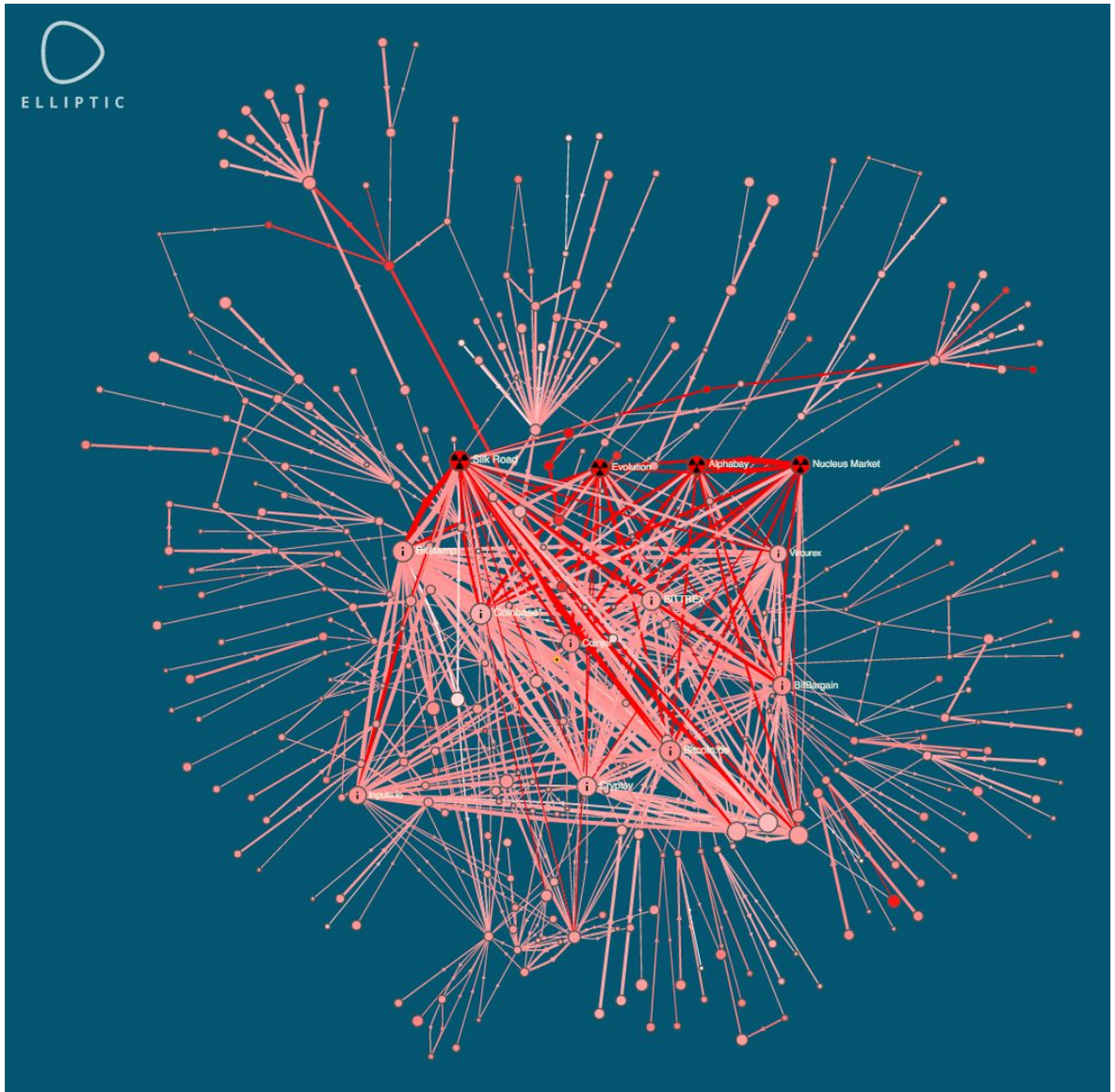
Hitting exchanges complicates the graph.



Exchanges are highly connected nodes.

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

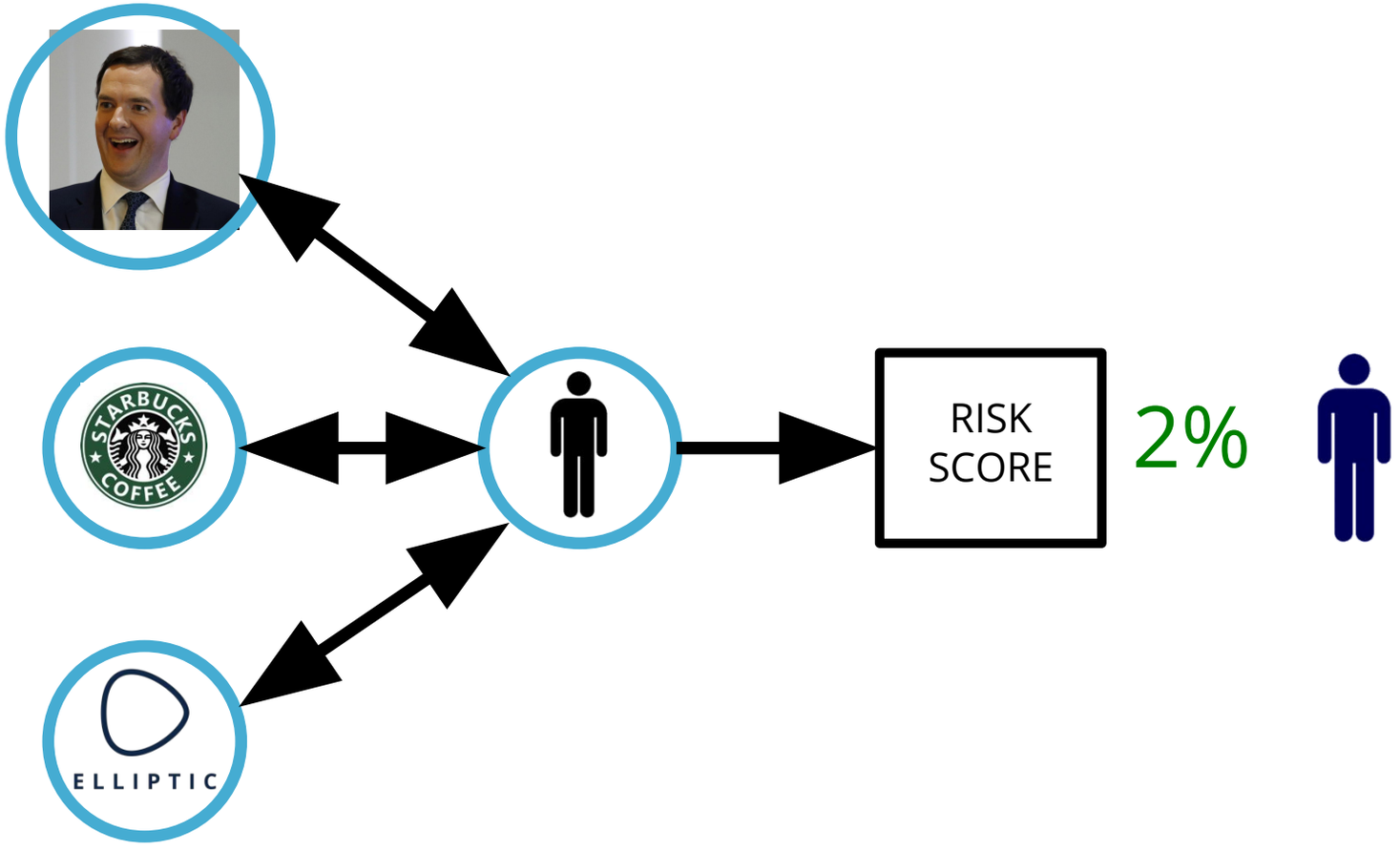
Adding dark markets makes it even more complicated



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

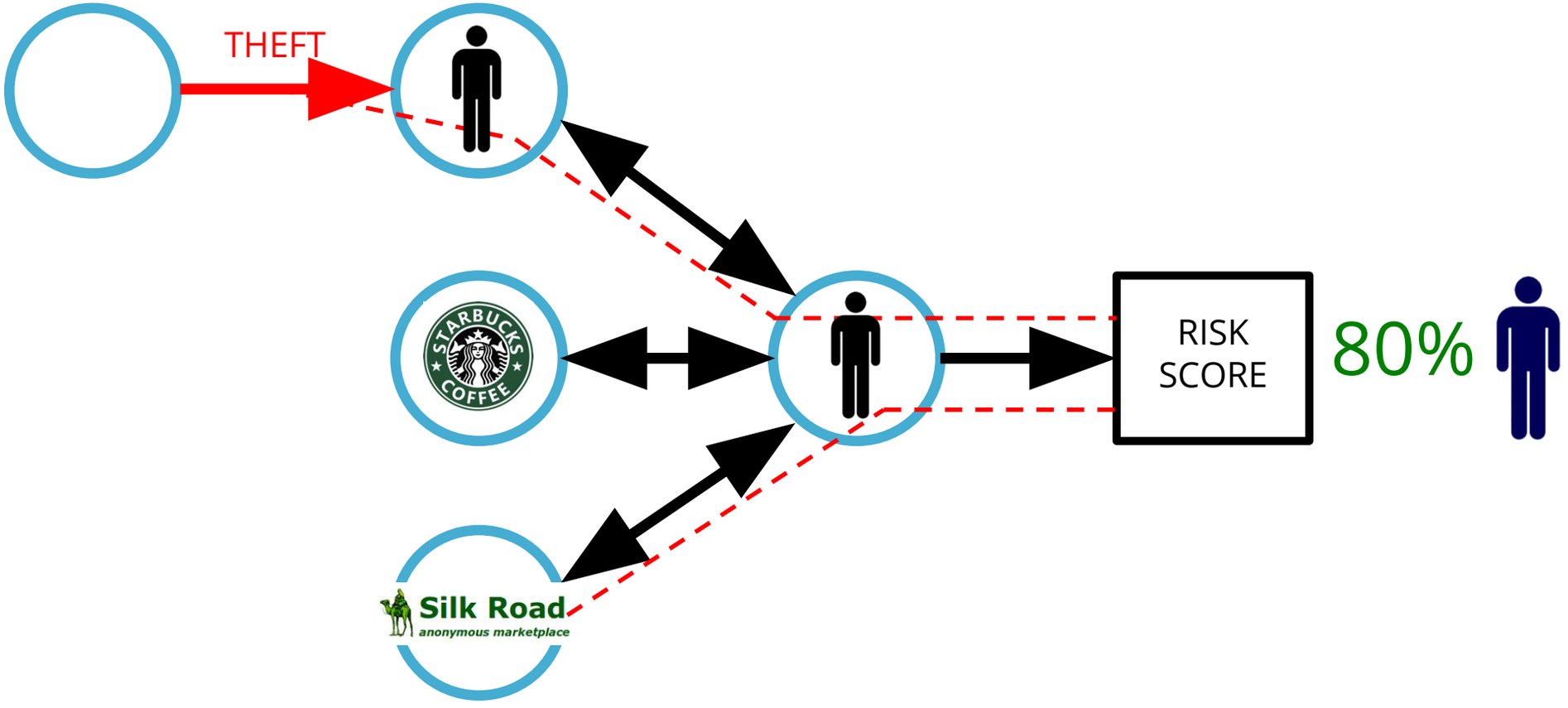
1. Which connections are more important now?

Risk-scoring of entities, transactions



ELLIPTIC

Risk-scoring of entities, transactions

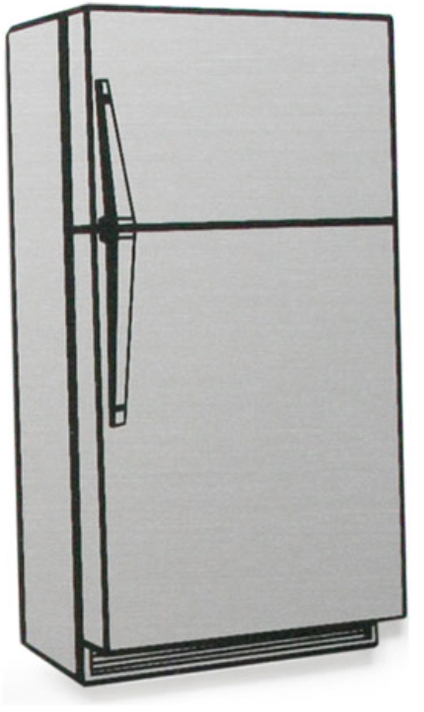


"Towards Risk Scoring of Bitcoin Transactions", Malte Moser et al. (2014)

ELLIPTIC

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 $$$?



ELLIPTIC

Thank you. Questions?

ELLIPTIC