Red Flag

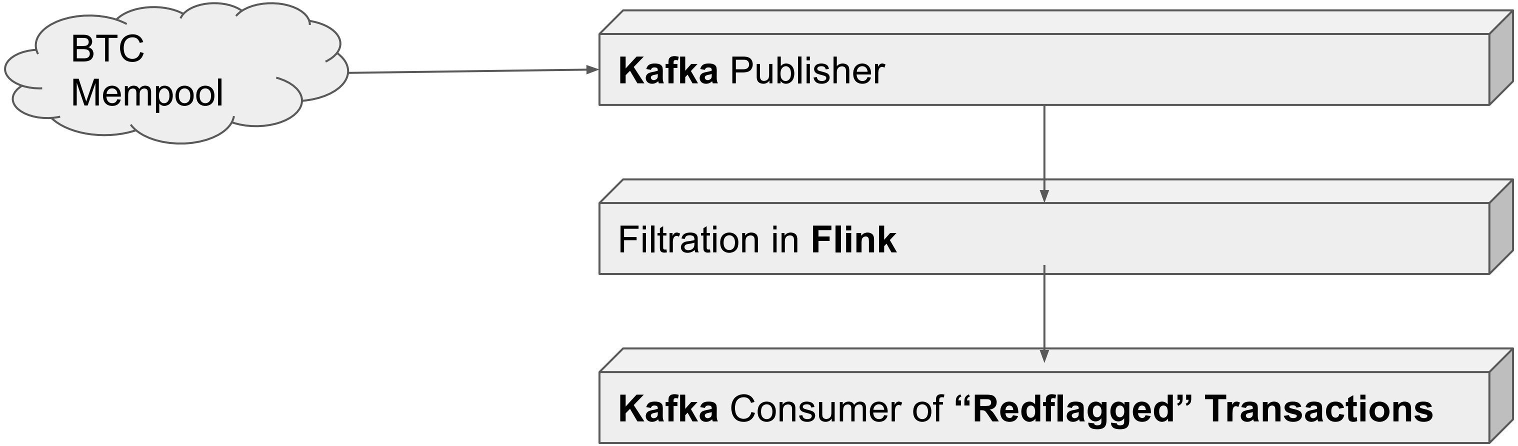
TRISA Hackathon Project

Peter Hauck
Alex Mologoko
Saulo Ricci
Alex Barreto

Crypto can easily Skirt the Spirit of Travel Rule

- Fan-in / Fan-out
- Time-delaying large transactions
- Use of non VASP address as a middleman

“Redflagging” Prototype Architecture



BTC Mempool

Kafka Publisher

Filtration in **Flink**

Kafka Consumer of **“Redflagged” Transactions**

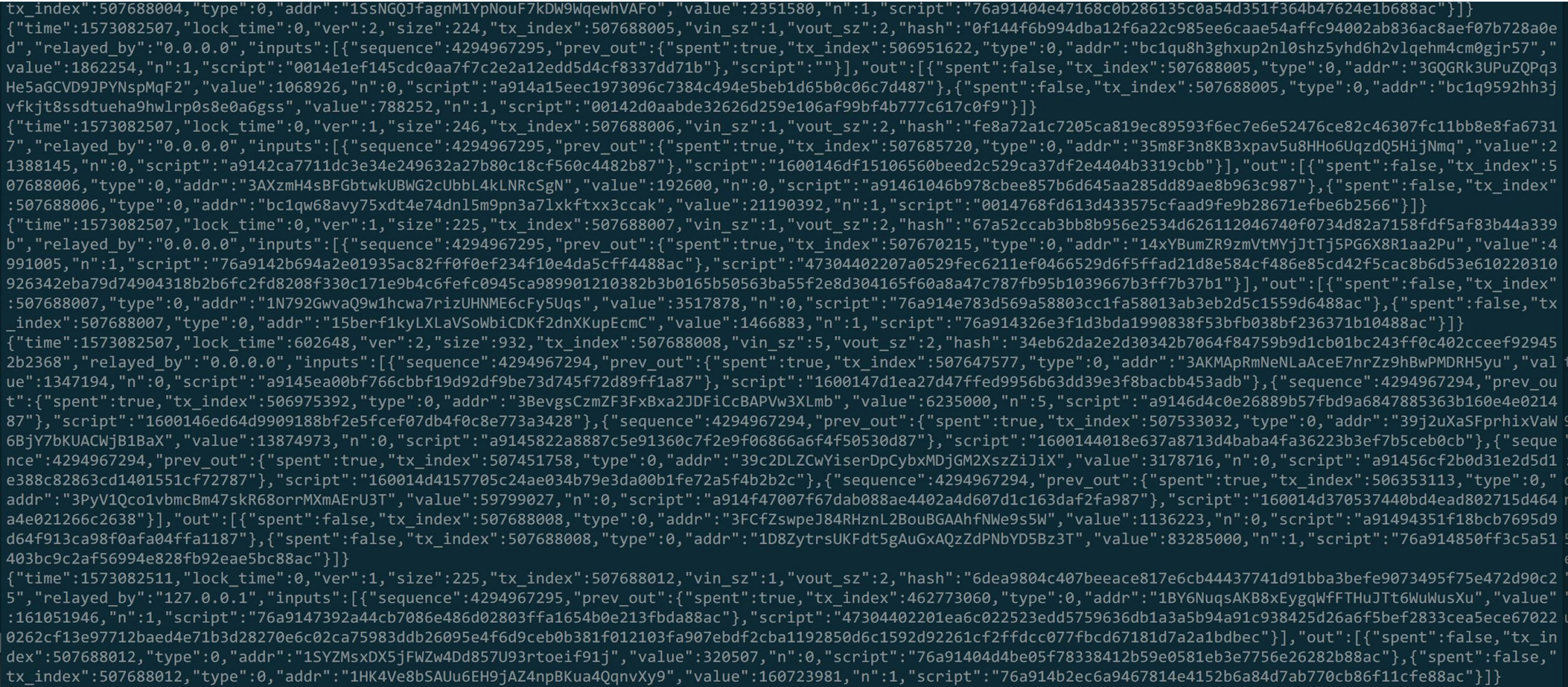
Proposed Filter Logic

- Time-based **“look back”** for a set of transactions that breaks the spirit of TRISA.

- Detection of Fan-out-Fan-In pattern for UTXO’s sent to a VASP.

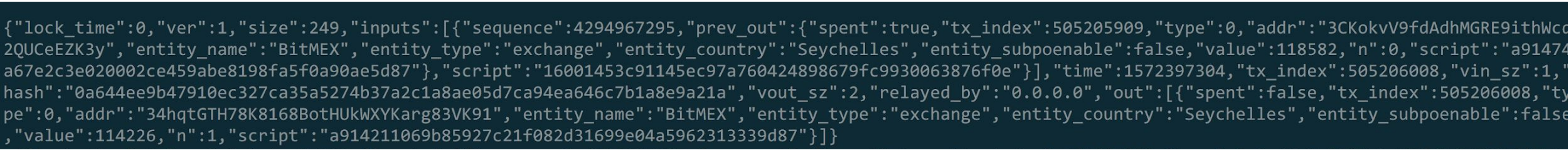
- Detection of simple “man-in-the-middle” between VASP1 and VASP2.
    - (**Using Ciphertrace Analytics to identify VASPs.)**

Prototype Inputs - Excerpt



```
tx_index":507688004,"type":0,"addr":"1SsNGQJfagnM1YpNouF7kDW9WqewhVAFo","value":2351580,"n":1,"script":"76a91404e47168c0b286135c0a54d351f364b47624e1b688ac"}]}
{"time":1573082507,"lock_time":0,"ver":2,"size":224,"tx_index":507688005,"vin_sz":1,"vout_sz":2,"hash":"0f144f6b994dba12f6a22c985ee6caae54affc94002ab836ac8aef07b728a0e
d","relayed_by":"0.0.0.0","inputs":[{"sequence":4294967295,"prev_out":{"spent":true,"tx_index":506951622,"type":0,"addr":"bc1qu8h3ghxup2nl0shz5yhd6h2vlqehm4cm0gjr57","
value":1862254,"n":1,"script":"0014e1ef145cdc0aa7f7c2e2a12edd5d4cf8337dd71b"},"script":""}],"out":[{"spent":false,"tx_index":507688005,"type":0,"addr":"3GQGRk3UPuZQPq3
He5aGCVD9JPYNspMqF2","value":1068926,"n":0,"script":"a914a15eec1973096c7384c494e5beb1d65b0c06c7d487"},{"spent":false,"tx_index":507688005,"type":0,"addr":"bc1q9592hh3j
vfkjt8ssdtueha9hwlrp0s8e0a6gss","value":788252,"n":1,"script":"00142d0aabde32626d259e106af99bf4b777c617c0f9"}]}
{"time":1573082507,"lock_time":0,"ver":1,"size":246,"tx_index":507688006,"vin_sz":1,"vout_sz":2,"hash":"fe8a72a1c7205ca819ec89593f6ec7e6e52476ce82c46307fc11bb8e8fa6731
7","relayed_by":"0.0.0.0","inputs":[{"sequence":4294967295,"prev_out":{"spent":true,"tx_index":507685720,"type":0,"addr":"35m8F3n8KB3xpav5u8HHo6UqzdQ5HijNmq","value":2
1388145,"n":0,"script":"a9142ca7711dc3e34e249632a27b80c18cf560c4482b87"},"script":"1600146df15106560beed2c529ca37df2e4404b3319cbb"}],"out":[{"spent":false,"tx_index":5
07688006,"type":0,"addr":"3AXzmH4sBFGbtwkUBWG2cUbbL4kLNRcSgN","value":192600,"n":0,"script":"a91461046b978cbee857b6d645aa285dd89ae8b963c987"},{"spent":false,"tx_index"
:507688006,"type":0,"addr":"bc1qw68avy75xdt4e74dnl5m9pn3a7lxkftxx3ccak","value":21190392,"n":1,"script":"0014768fd613d433575cfaad9fe9b28671efbe6b2566"}]}
{"time":1573082507,"lock_time":0,"ver":1,"size":225,"tx_index":507688007,"vin_sz":1,"vout_sz":2,"hash":"67a52ccab3bb8b956e2534d626112046740f0734d82a7158fdf5af83b44a339
b","relayed_by":"0.0.0.0","inputs":[{"sequence":4294967295,"prev_out":{"spent":true,"tx_index":507670215,"type":0,"addr":"14xYBumZR9zmVtMYjJtTj5PG6X8R1aa2Pu","value":4
991005,"n":1,"script":"76a9142b694a2e01935ac82ff0f0ef234f10e4da5cff4488ac"},"script":"47304402207a0529fec6211ef0466529d6f5ffad21d8e584cf486e85cd42f5cac8b6d53e610220310
926342eba79d74904318b2b6fc2fd8208f330c171e9b4c6fefc0945ca989901210382b3b0165b50563ba55f2e8d304165f60a8a47c787fb95b1039667b3ff7b37b1"}],"out":[{"spent":false,"tx_index"
:507688007,"type":0,"addr":"1N792GwvaQ9w1hcwa7rizUHNME6cFy5Uqs","value":3517878,"n":0,"script":"76a914e783d569a58803cc1fa58013ab3eb2d5c1559d6488ac"},{"spent":false,"tx
_index":507688007,"type":0,"addr":"15berf1kyLXLaVSoWbiCDKf2dnXKupEcmC","value":1466883,"n":1,"script":"76a914326e3f1d3bda1990838f53bfb038bf236371b10488ac"}]}
{"time":1573082507,"lock_time":602648,"ver":2,"size":932,"tx_index":507688008,"vin_sz":5,"vout_sz":2,"hash":"34eb62da2e2d30342b7064f84759b9d1cb01bc243ff0c402cceef92945
2b2368","relayed_by":"0.0.0.0","inputs":[{"sequence":4294967294,"prev_out":{"spent":true,"tx_index":507647577,"type":0,"addr":"3AKMApRmNeNLaAceE7nrZz9hBwPMDRH5yu","val
ue":1347194,"n":0,"script":"a9145ea00bf766cbbf19d92df9be73d745f72d89ff1a87"},"script":"1600147d1ea27d47ffed9956b63dd39e3f8bacbb453adb"},{"sequence":4294967294,"prev_ou
t":{"spent":true,"tx_index":506975392,"type":0,"addr":"3BevgsCzmZF3FxBxa2JDFiCcBAPVw3XLmb","value":6235000,"n":5,"script":"a9146d4c0e26889b57fbd9a6847885363b160e4e0214
87"},"script":"1600146ed64d9909188bf2e5fcef07db4f0c8e773a3428"},{"sequence":4294967294,"prev_out":{"spent":true,"tx_index":507533032,"type":0,"addr":"39j2uXaSFprhixVaW
6BjY7bKUACWjB1BaX","value":13874973,"n":0,"script":"a9145822a8887c5e91360c7f2e9f06866a6f4f50530d87"},"script":"1600144018e637a8713d4baba4fa36223b3ef7b5ceb0cb"},{"seque
nce":4294967294,"prev_out":{"spent":true,"tx_index":507451758,"type":0,"addr":"39c2DLZCwYiserDpCybxMDjGM2XszZiJiX","value":3178716,"n":0,"script":"a91456cf2b0d31e2d5d1
e388c82863cd1401551cf72787"},"script":"160014d4157705c24ae034b79e3da00b1fe72a5f4b2b2c"},{"sequence":4294967294,"prev_out":{"spent":true,"tx_index":506353113,"type":0,"
addr":"3PyV1Qco1vbmcBm47skR68orrMXmAErU3T","value":59799027,"n":0,"script":"a914f47007f67dab088ae4402a4d607d1c163daf2fa987"},"script":"160014d370537440bd4ead802715d464
a4e021266c2638"}],"out":[{"spent":false,"tx_index":507688008,"type":0,"addr":"3FCfZswpeJ84RHznL2BouBGAAhfNWe9s5W","value":1136223,"n":0,"script":"a91494351f18bcb7695d9
d64f913ca98f0afa04ffa1187"},{"spent":false,"tx_index":507688008,"type":0,"addr":"1D8ZytrsUKFdt5gAuGxAQzZdPNbYD5Bz3T","value":83285000,"n":1,"script":"76a914850ff3c5a51
403bc9c2af56994e828fb92eae5bc88ac"}]}
{"time":1573082511,"lock_time":0,"ver":1,"size":225,"tx_index":507688012,"vin_sz":1,"vout_sz":2,"hash":"6dea9804c407beeace817e6cb44437741d91bba3befe9073495f75e472d90c2
5","relayed_by":"127.0.0.1","inputs":[{"sequence":4294967295,"prev_out":{"spent":true,"tx_index":462773060,"type":0,"addr":"1BY6NuqsAKB8xEygqWfFTHuJTt6WuWusXu","value"
:161051946,"n":1,"script":"76a9147392a44cb7086e486d02803ffa1654b0e213fbda88ac"},"script":"47304402201ea6c022523edd5759636db1a3a5b94a91c938425d26a6f5bef2833cea5ece67022
0262cf13e97712baed4e71b3d28270e6c02ca75983ddb26095e4f6d9ceb0b381f012103fa907ebdf2cba1192850d6c1592d92261cf2ffdcc077fbcd67181d7a2a1bdbec"}],"out":[{"spent":false,"tx_in
dex":507688012,"type":0,"addr":"1SYZMsxDX5jFWZw4Dd857U93rtoeif91j","value":320507,"n":0,"script":"76a91404d4be05f78338412b59e0581eb3e7756e26282b88ac"},{"spent":false,"
tx_index":507688012,"type":0,"addr":"1HK4Ve8bSAUu6EH9jAZ4npBKua4QqnvXy9","value":160723981,"n":1,"script":"76a914b2ec6a9467814e4152b6a84d7ab770cb86f11cfe88ac"}]}
```

Prototype Outputs

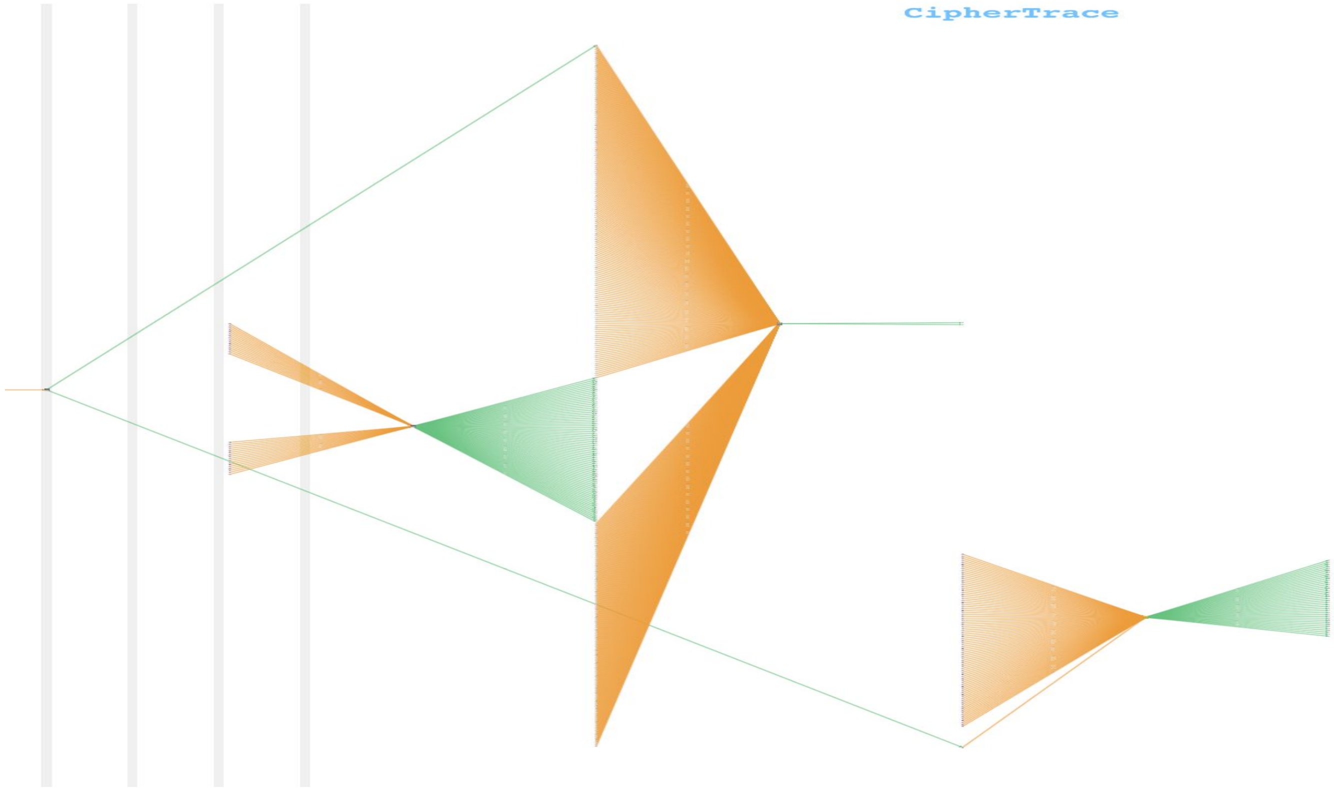


```
{"lock_time":0,"ver":1,"size":249,"inputs":[{"sequence":4294967295,"prev_out":{"spent":true,"tx_index":505205909,"type":0,"addr":"3CKokvV9fdAdhMGRE9ithWcc
2QUCeEZK3y","entity_name":"BitMEX","entity_type":"exchange","entity_country":"Seychelles","entity_subpoenable":false,"value":118582,"n":0,"script":"a91474
a67e2c3e020002ce459abe8198fa5f0a90ae5d87"},"script":"16001453c91145ec97a760424898679fc9930063876f0e"}],"time":1572397304,"tx_index":505206008,"vin_sz":1,"
hash":"0a644ee9b47910ec327ca35a5274b37a2c1a8ae05d7ca94ea646c7b1a8e9a21a","vout_sz":2,"relayed_by":"0.0.0.0","out":[{"spent":false,"tx_index":505206008,"ty
pe":0,"addr":"34hqtGTH78K8168BotHUkWXYKarg83VK91","entity_name":"BitMEX","entity_type":"exchange","entity_country":"Seychelles","entity_subpoenable":false
,"value":114226,"n":1,"script":"a914211069b85927c21f082d31699e04a5962313339d87"}]}
```

Our Prototype Caught this TX (Fan-out-Fan-in)

```
{
       "message": {
           "time": "2019-11-06T00:40:18",
           "lock_time": 0,
           "tx_hash": "93ece0d455e0f9a9da4365abf51a1ba778ef80006d0ee6efdf2b2e351a8c3bfe",
           "relayed_by": "0.0.0.0",
           "input": true,
           "addr": "3Nhce5TVhmazvyAmWXHRjcPTeRHG6n8xKx",
           "value": 0.0155214,
           "n": 0,
           "entity_name": "Paxful.com",
           "entity_type": "high risk exchange",
           "entity_country": "US",
           "entity_subpoenable": true
       },
       "offset": 507388028
   }
```

Our Prototype Caught this Fan-out-Fan-in



Potential Use Cases

- Detect Mixers and other obfuscators in the network

- Detect parties using these obfuscation methods
    - Multiple degrees of separation

- Score obfuscation in the blockchain

Thank you.