ITUEvents

Insights on Digital Financial Services during COVID-19 Webinar Series

Tracking Digital Financial Crimes and Fraud

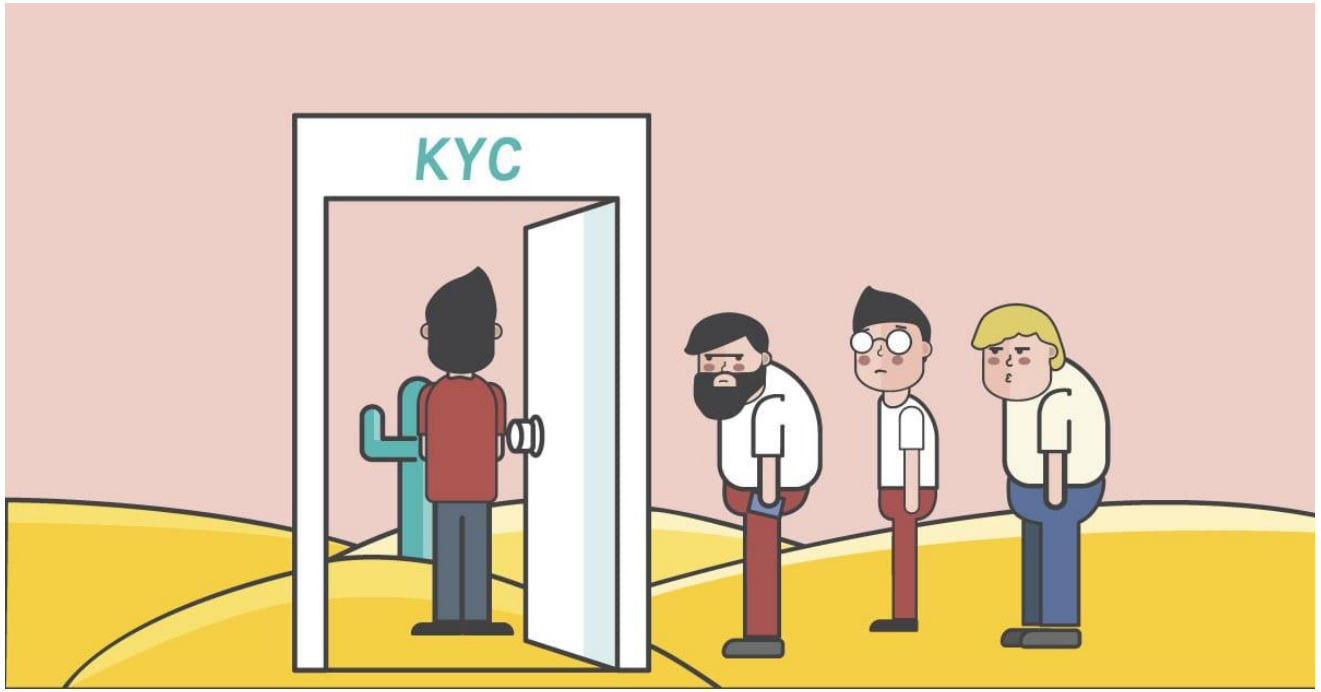
Tracking Crypto Ponzi example

@Assaf Klinger

A little about myself

- Husband, father (+2), geek 8-)
- Security researcher for the last 18 years
  - Specialize in telecom and blockchain
- CEO @Naboo (blockchain AML)
- A member of ITU-T Study Group 11
- Handles:
  - Assaf.klinger@gmail.com
  - @AssafKlinger
  - https://www.linkedin.com/in/assaf-klinger-8a0b7159/

UDIS and cryptocurrency



- Cryptocurrencies are an alternative to the centralized, regulated financial systems
- Using cryptocurrencies fraudsters enjoy the freedom to move money around without regulation or monitoring

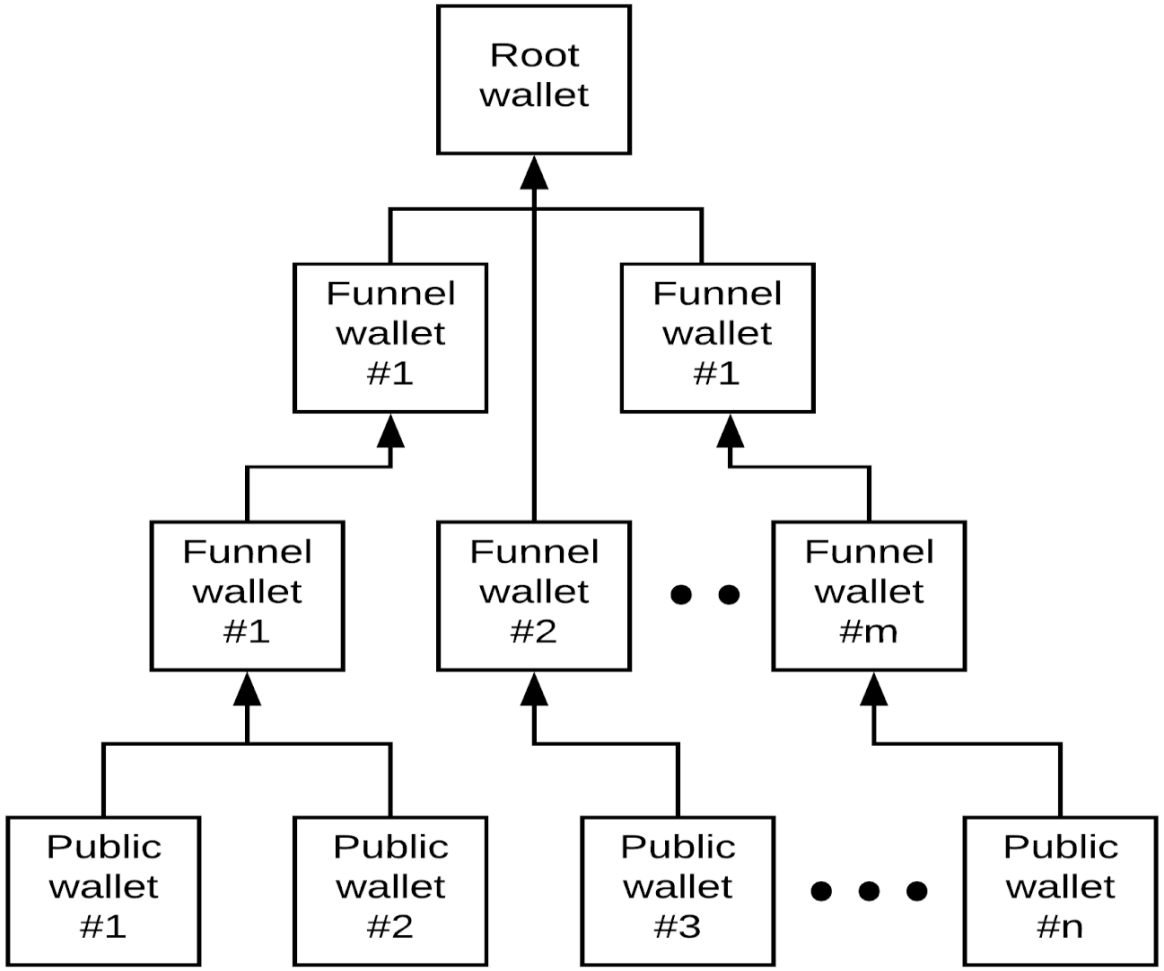
Crypto scams

- Crypto scams are build like trees (simple) or graphs (complex)
- The leafs are the “public facing wallets” i.e. the wallets that are publicly shared in order to collect the funds from the victims.
- The “public facing wallets” appear in the ponzi websites and IM groups (Telegram, WhatsApp, etc...)
- Funds from the “public facing wallets” are then funneled through a series of “funneling” wallets in order to hide the tracks of the money gotten from the illegal activity.
- From the “funneling wallets” the funds are collected in “root wallets” from where the money is laundered via exchanges or token swaps

Getting intelligence

- Scan the web, IM groups (WhatsApp, Telegram) and dark web
- Use aggregator databases if possible, for example:
  - https://etherscamdb.info/scams
  - https://www.bitcoinabuse.com/reports
- These sites are far from complete, they are community generated…

Simple funneling tree of a scam



Complications to the simple tree

- Exchange pools
  - Centralized exchanges work with inbound and outbound pool, with a private internal database for keeping each user's funds separate.
- Coin Mixers
  - In BTC there is a possibility to perform many-2-many transactions, with multiple inputs and multiple outputs, which complicates tracking
- Token Swaps (atomic swaps)
  - An atomic swap is two users exchanging coins via four private wallets, two in the source coin / token and two in the target coin / token. An atomic swap is comprised of two supposedly unrelated transactions on two different blockchains

End point of the tracking process

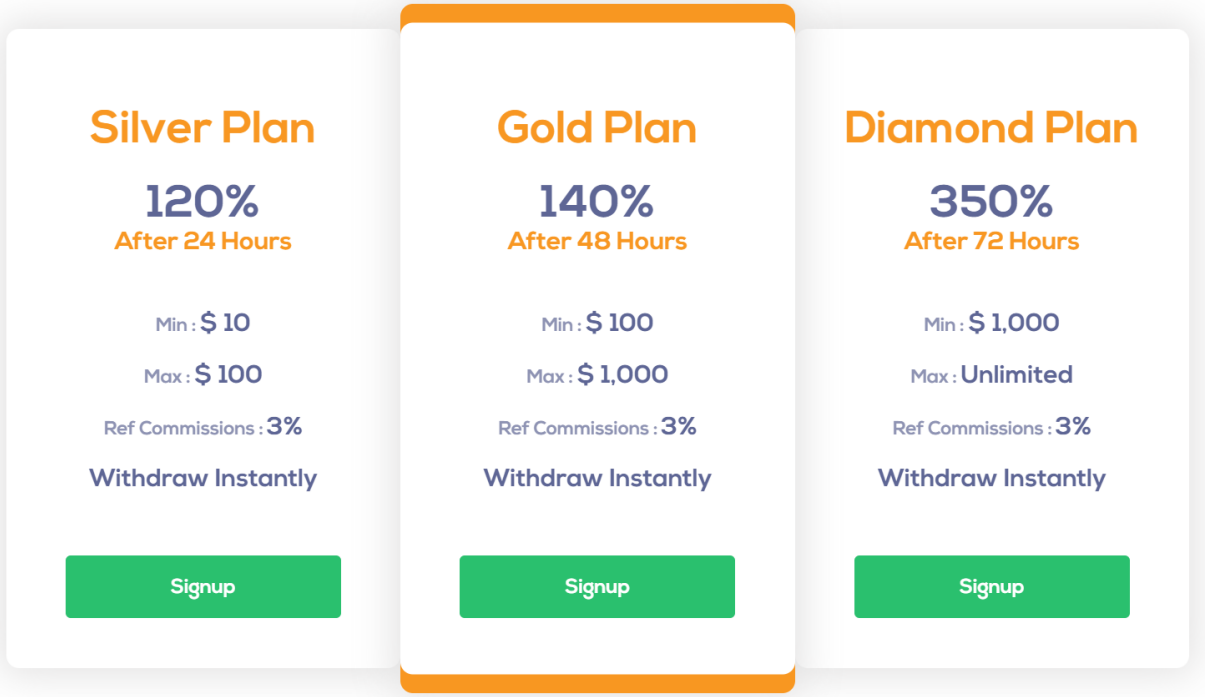
- We’ve reached a “root” wallet with positive balance and no outgoing transactions
- We’ve reached an exchange pool and it’s safe to assume the funds we’re converted to fiat

Example use case

- Let’s pull a scam from the EtherScamDB

Scamming	Investments	Active	bit-donor.com

- This looks like an active ponzi ☺:



Leaf wallet – bit-donor.com

- 1Fr2VJ2pgMsAktcLonHUqBnZbu7H1zZLpH

Wallet [89dfe7747d] (show wallet addresses)

Page 1 / 5 Next... Last (total transactions: 465) Download as CSV

date	received/sent	balance	transaction
2019-11-22 20:58:44	-0.0032601 [13c3c3935d] (-0.00012112) fee	0.00783349	2c75169c03509e2b98a0...
2019-11-21 11:47:57	[1e8c4515b5] +0.00126514	0.01121471	95071e5245ed7ff56205...
2019-10-31 15:40:38	[0961215f90] +0.00420394	0.00994957	d32ec25761ec5af933c3...
2019-10-31 11:05:04	-0.00166639 [0961215f90] (-0.0000748) fee	0.00574563	040fd5d87d60dc3439e7...
2019-10-27 17:13:47	[05ce2fb190] +0.00209474	0.00748682	5d6ded87d8c386f0e445...
2019-10-26 13:23:28	-0.00130492 [1a989000a6] (-0.00013334) fee	0.00539208	2edfa7090c7e93193213...
2019-10-25 11:34:20	[05ce2fb190] +0.00263958	0.00683034	6fea8e4b617524b08383...
2019-10-25 08:08:54	[1a989000a6] +0.00133744	0.00419076	b1e8198982de02da6398...
2019-10-21 14:10:59	-0.00339296 CoinPayments.net (-0.0000052) fee	0.00285332	a8e1afe00b228e02130d...
2019-10-18 16:06:26	[8045f562a3] +0.00252122	0.00625148	71bc8d8f44d03c4dca77...
2019-10-09 20:58:30	[85821394ed] +0.00116224	0.00373026	48ec87c4e310777fcb79...

Leaf wallet – bit-donor.com

- 1Fr2VJ2pgMsAktcLonHUqBnZbu7H1zZLpH
- Busy wallet, active from Mar. 2019, transacted ~2 BTC (~$14K)
- Direct exfiltration of 600$ from deposits made by victims (14 txs) to:
  - https://www.luno.com
  - https://www.coinpayments.net
- ~75% of the funds were funneled to: 1DKYRgUVvQhFb3rb1DjejRxyDGkC211xU9

Funneling wallet – bit-donor.com

- Let's look at the funneling wallet: [1DKYRgUVvQhFb3rb1DjejRxyDGkC211xU9]

Wallet [97742e2c02] (show wallet addresses)

Page 1 / 1 (total transactions: 46) Download as CSV

date	received/sent	balance	transaction
2019-09-16 03:06:26	[89dfe7747d] +0.00964091	0.01002401	b88a71ed5b51f6105808…
2019-08-18 16:04:25	-0.03862224 [35ef9bfe3e] (-0.00014212) fee	0.0003831	43bfd59c57f54ab1c6d6…
2019-08-18 08:23:12	-0.00147688 [22709c48fc] (-0.00000452) fee	0.03914746	17c7ffd6d9aaa89da240…
2019-08-15 15:47:07	[89dfe7747d] +0.03970846	0.04062886	eb30406b92d59eafb5b1…
2019-08-14 16:08:21	-0.00379916 [89dfe7747d] (-0.00001044) fee	0.0009204	8acaa5cf33bfcff66b8c…
2019-08-11 15:27:08	-0.00123097 [b56fea8dca] (-0.00000226) fee	0.00473	d50ff096b808f37a4348…
2019-08-11 14:37:34	-0.04429288 [35ef9bfe3e] (-0.00001496) fee	0.00596323	c1bf2fb0e265cdbdff63…
2019-08-08 20:06:23	[89dfe7747d] +0.04305134	0.05027107	95b562e9d641b955929f…
2019-08-06 21:18:20	-0.25733424 [00cedcb2e5] (-0.00001044) fee	0.00721973	0f7fccf14b160f74495c…
2019-08-06 12:00:51	[89dfe7747d] +0.19509646	0.26456441	752c4244d161c48df9f5…
2019-08-05 19:10:48	[89dfe7747d] +0.02376351	0.06946795	86f3c1f5fd0c24ee81a9…
2019-08-05 12:58:53	[89dfe7747d] +0.04250565	0.04570444	60e05cd5d8d7aafec3b5…
2019-08-04 16:35:26	-0.12787501 [004bd96c19] (-0.0001474) fee	0.00319879	e4cd54f1bcc7139df15c…
2019-08-04 09:53:58	[89dfe7747d] +0.01400997	0.1312212	8593e2dcbf0223b26baa…
2019-08-03 14:19:11	[89dfe7747d] +0.02790269	0.11721123	0455d4b32097fa97d7b2…
2019-07-30 08:57:23	[89dfe7747d] +0.08413091	0.08930854	19e1f503e9e7d82d47c5…

Funneling wallet – bit-donor.com

- Let's look at the funneling wallet: 1DKYRgUVvQhFb3rb1DjejRxyDGkC211xU9
  - 46 transactions
  - 12 funneling cycles
- The large amounts we're funneled to:
  - https://www.walletexplorer.com/wallet/00cedcb2e5d97202 → this is a **root** wallet, from here funds are exfiltrated to fiat
  - https://www.walletexplorer.com/wallet/004bd96c19bf9f13 → another funneling wallet
  - https://www.walletexplorer.com/wallet/04eb430860b8a3d5 → another funneling wallet that also exfiltrates funds to fiat

Root wallet – bit-donor.com

- Let's look at the root wallet: https://www.walletexplorer.com/wallet/00cedcb2e5d97202
- This is a hot wallet that exfiltrates funds via https://www.huobi.com
- This wallet probably works in tandem with several other wallets, the major one being:
  - https://www.walletexplorer.com/wallet/0010b7a31eb4bfd5 (hot) which currently holds ~15 BTC (over $100K)
- From https://www.walletexplorer.com/wallet/0010b7a31eb4bfd5 we can get to the jackpot wallet which is: https://www.walletexplorer.com/wallet/00b078bc1fe43cca this wallet currently holds **~19K BTC (over $138M)** → this is the one to go after

What's next ?

- This campaign can be further mapped, to find additional funnels and leaves, starting with the jackpot wallet and going down from there
- These wallets interact directly with regulated exchanges:
  - https://www.walletexplorer.com/wallet/00cedcb2e5d97202
  - https://www.walletexplorer.com/wallet/0010b7a31eb4bfd5
  - https://www.walletexplorer.com/wallet/04eb430860b8a3d5
  - https://www.walletexplorer.com/wallet/89dfe7747d589779
- Law enforcement can retrieve KYC data and investigate the owners of these wallets.

Q&A