

# FIGI Security Clinic

## Tracking Crypto Ponzi scams

Assaf Klinger

4-5 December 2019  
#financialinclusion

Sponsored by

BILL & MELINDA  
GATES foundation

FIGI > FINANCIAL INCLUSION  
GLOBAL INITIATIVE



Organized by



# 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@naboo.id](mailto:assaf@naboo.id)
  - @AssafKlinger
  - <https://www.linkedin.com/in/assaf-klinger-8a0b7159/>



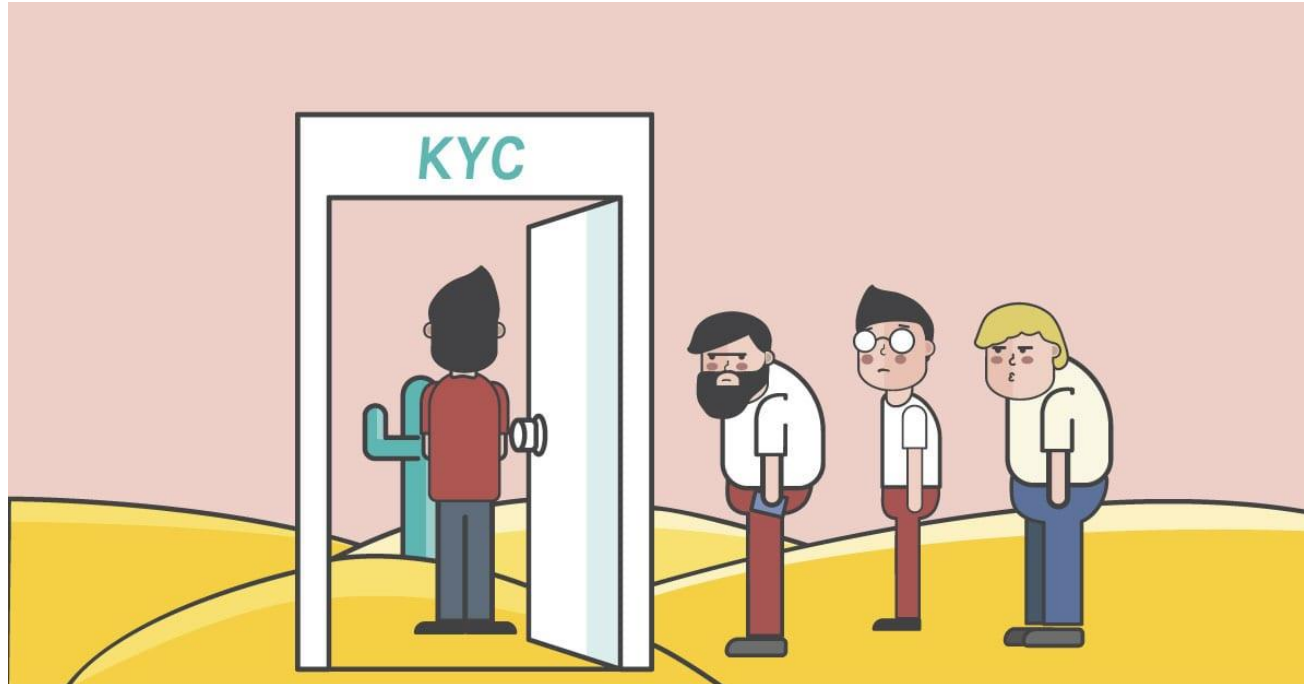


# What is cryptocurrency?

- Cryptocurrency (or crypto for short) is a digital asset designed to work as a medium of exchange using mathematical cryptography models to secure the transaction and control the creation of units of the currency
- Public cryptocurrencies are in almost all decentralized, e.g. not owned or governed by a single entity, essentially crypto has no governing body thus is not regulated
- The engine that drives crypto is DLT (Distributed Ledger Technology) a subset of DLTs that drives the most popular cryptocurrencies today is called the Blockchain



# UDIS and cryptocurrency

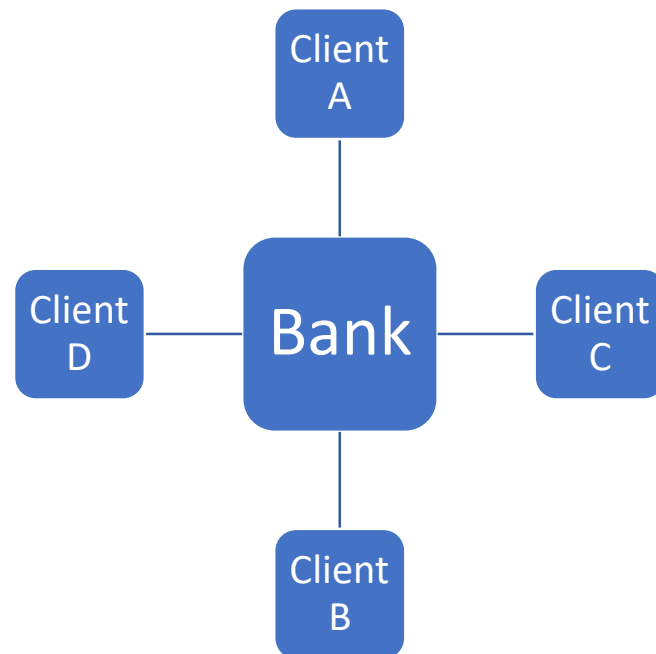


- Cryptocurrencies are an alternative to the centralized, regulated financial systems
- Using cryptocurrencies fraudsters enjoy the freedom to move money around without regulation or monitoring



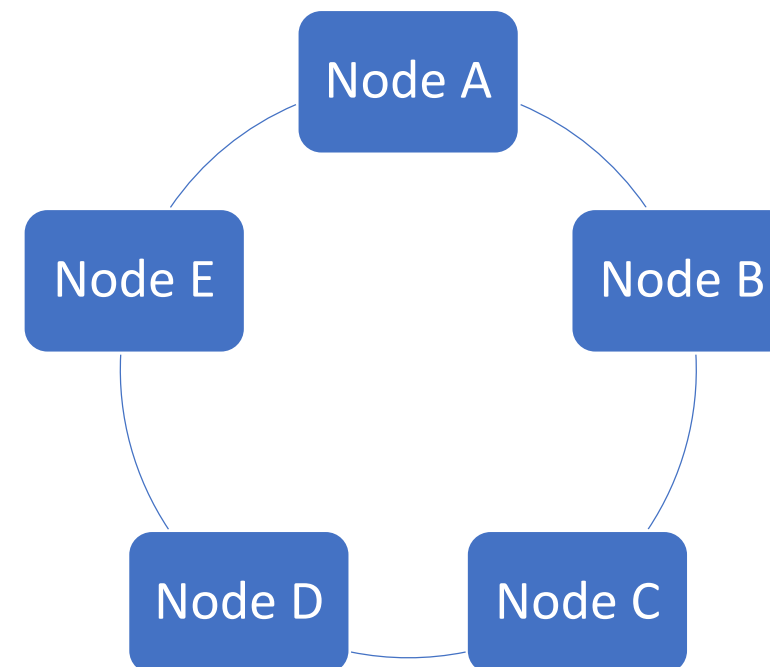
# What is a distributed ledger?

## Centralized ledger



- There are multiple ledgers, but Bank holds the “golden record”
- Client B must reconcile its own ledger against that of Bank, and must convince Bank of the “true state” of the Bank ledger if discrepancies arise

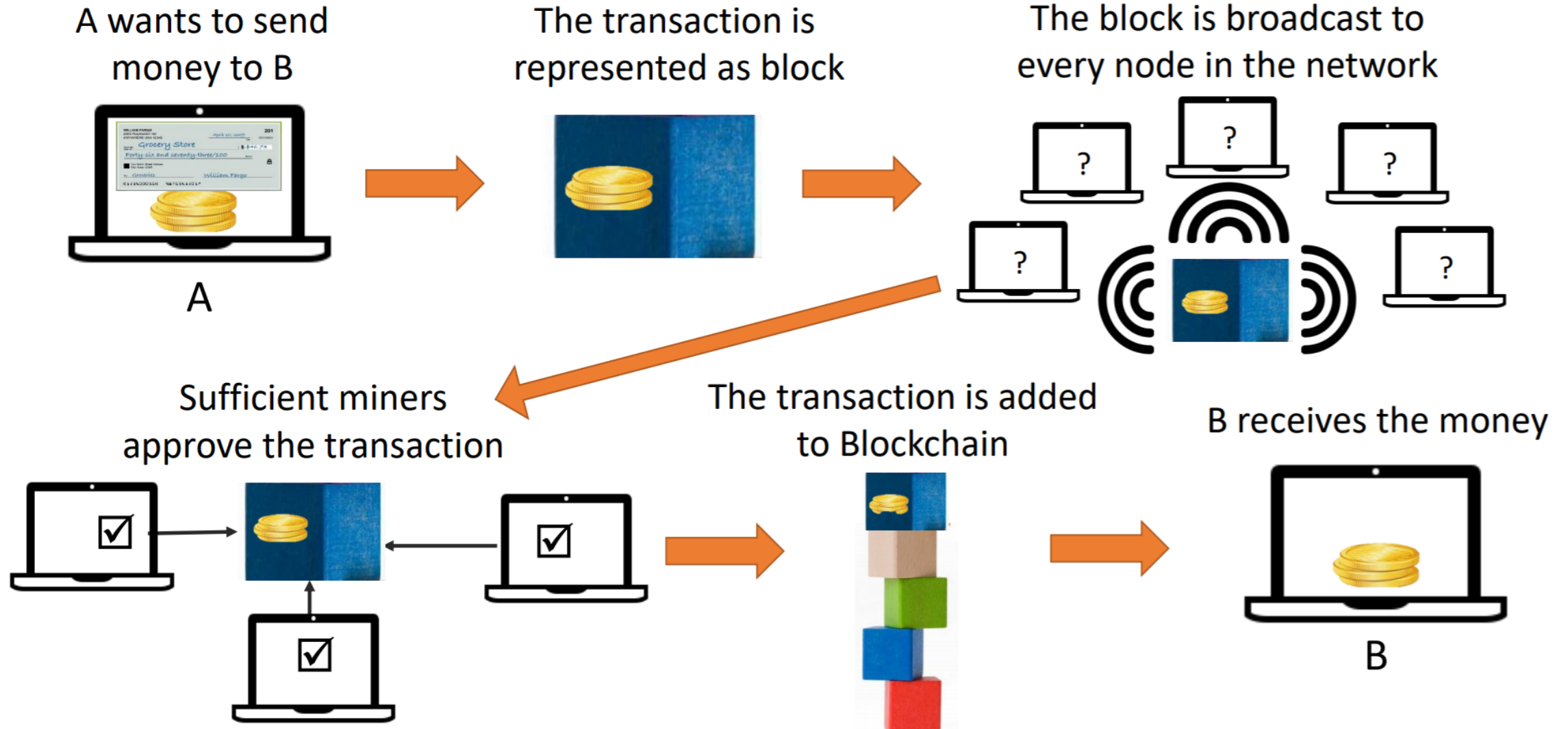
## Distributed ledger



- There is one ledger. All Nodes have some level of access to that ledger.
- All Nodes agree to a protocol that determines the “true state” of the ledger at any point in time. The application of this protocol is sometimes called “achieving consensus.”

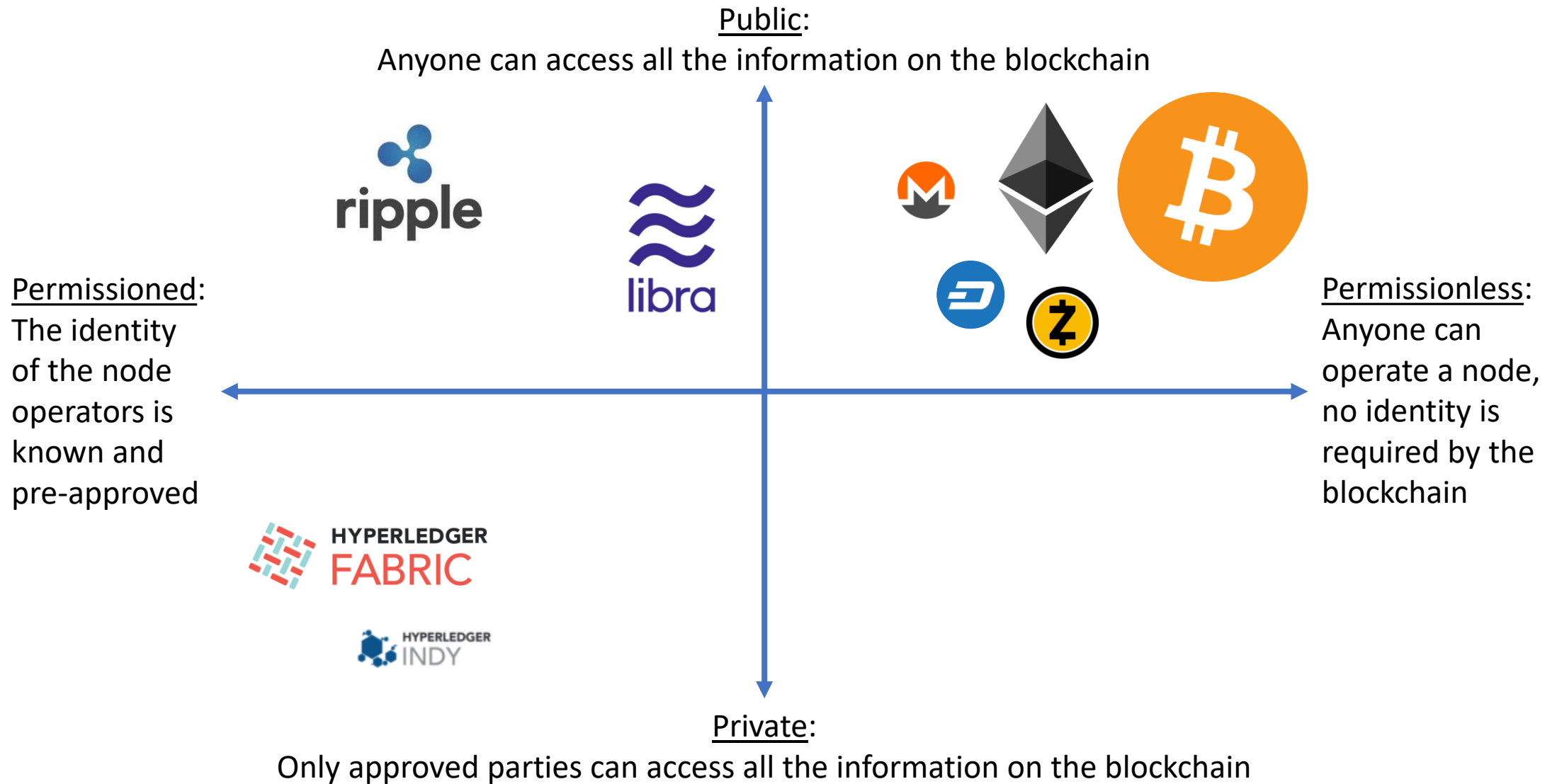


# How blockchain works?



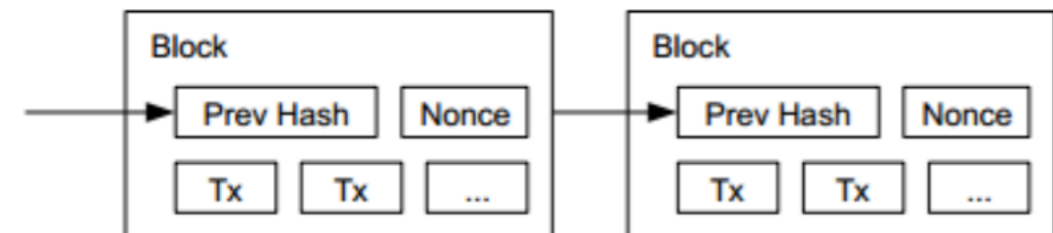


# There are several types of blockchains



# Bitcoin

- The first realization of blockchain (started in 2009)
- A protocol that supports decentralized anonymous peer-to-peer digital currency
- Every viable transaction is stored in a public ledger
- Transactions are placed in blocks, which are linked by SHA256 hashes
- A reward driven system for achieving consensus (mining) based on
  - "Longest chain for consensus"
  - "Proofs of Work" for helping to secure the network

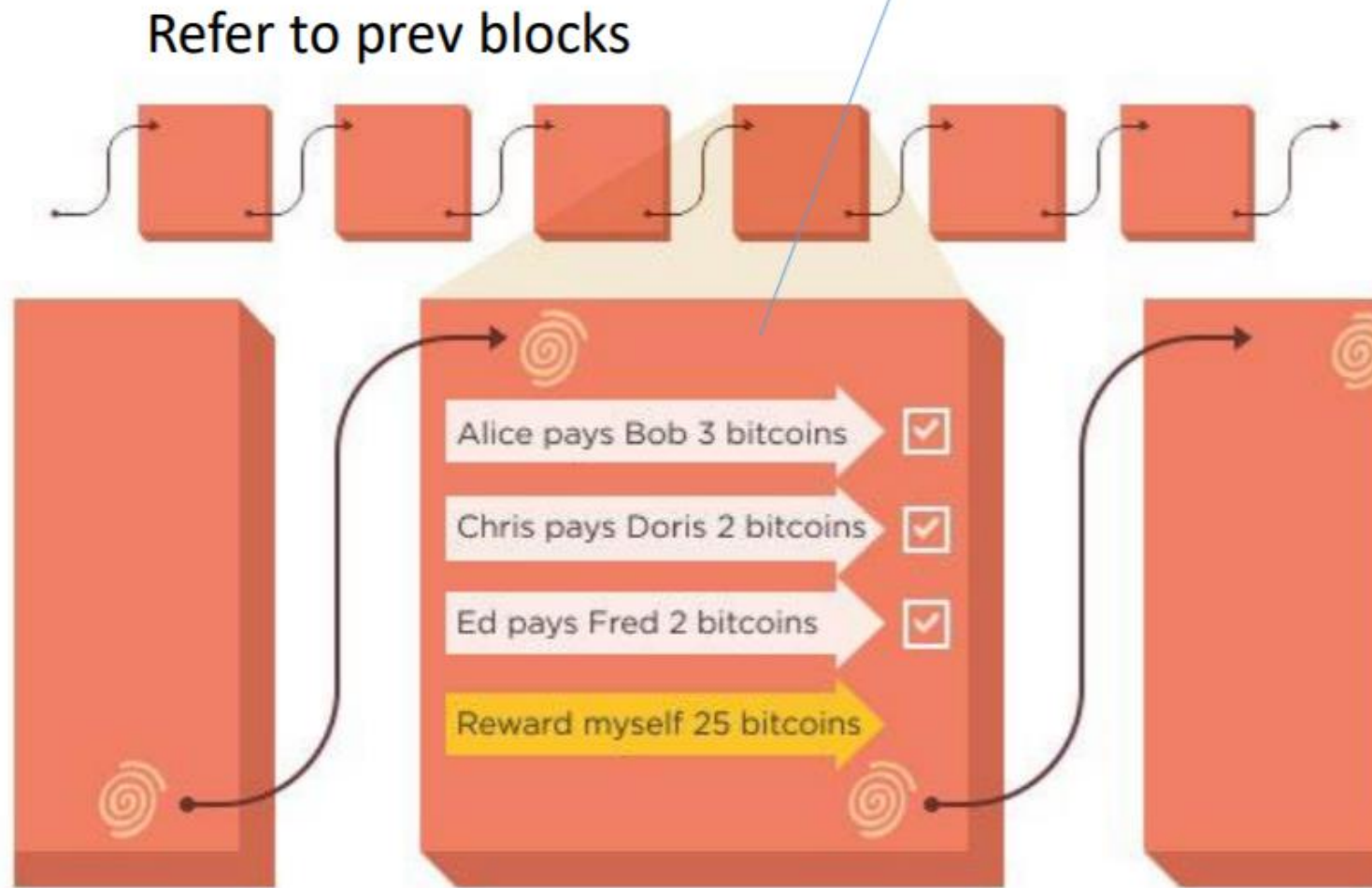






# The bitcoin blockchain

The header of the block contains unique hash



# Ethereum

- A decentralized platform that runs smart contracts
- Released in 2015
- Each block is a turning complete virtual machine (smart contract) that runs code, the code is validated by the nodes as “true” in the consensus process, signed and added to the chain.
- Supports the creation of additional currencies / tokens on the same infrastructure (using ERC-20)
- Smart contracts offer more powerful transactions:
  - Exchange, Auction, Games, Bets, Legal agreements,...



# Privacy blockchains (Monero & Zcash)

- Released in 2014 (Monero) and 2016 (Zcash)
- A new type of blockchain that obfuscates some of the public ledger data to increase the end-user's privacy.
- These are public-permissionless blockchains, but the address data in each transaction is encrypted in order to block outside observers view on the transaction data.
- This feature negates the outside observer's capability to track transactions between wallets and to assess the balance of each wallet.





# Must know blockchain terms

- **Bitcoin:** Bitcoin is the first cryptocurrency that came into existence in 2009 by Satoshi Nakamoto. It is a digital currency that doesn't require a centralized authority to work or function.
- **Altcoin:** Altcoin is any cryptocurrency other than Bitcoin.
- **Fiat:** Fiat is the government-controlled currency and is declared as legal tender.
- **Address:** the location of funds, the key used to store value on the blockchain
- **Wallet:** An address or group of addresses (depending on the blockchain) associated with a blockchain user.
- **ERC-20:** ERC-20 is a technical standard for issuing tokens on Ethereum blockchain.
- **Ether:** Ether is the fuel that powers distributed Ethereum network.
- **Mainnet:** Mainnet is a working blockchain product that also provides the ability to transfer digital currencies between users in a blockchain environment.

Questions so far ?





Coffee break



# Tracking Crypto



# Block explorers

- All public-permissionless blockchains have block explorers
- Block explorers are the tools used to track crypto
- Privacy blockchains have block explorers too, but they require the view key in order to track
- Block explorers are usually:
  - Free
  - Maintained by the non-profit that runs the blockchain
  - Open source
  - Have machine APIs



# Tools used in this clinic



<https://naboo.io/>  
<https://www.walletexplorer.com/>



<https://bloxy.info/>  
<https://naboo.io/>

# Block explorer 101

- Input: address / wallet / hash / transaction id
- Output: the value and history (if any) of the searched item
  
- For example, we will use this BTC address:
  - [1HWeepQYBEYV8ZRnpRzZs1homLW3tqfXhD](#)
- Now let's look at the Ethereum explorer:
  - [0x2b5634c42055806a59e9107ed44d43c426e58258](#)

# Crypto scams

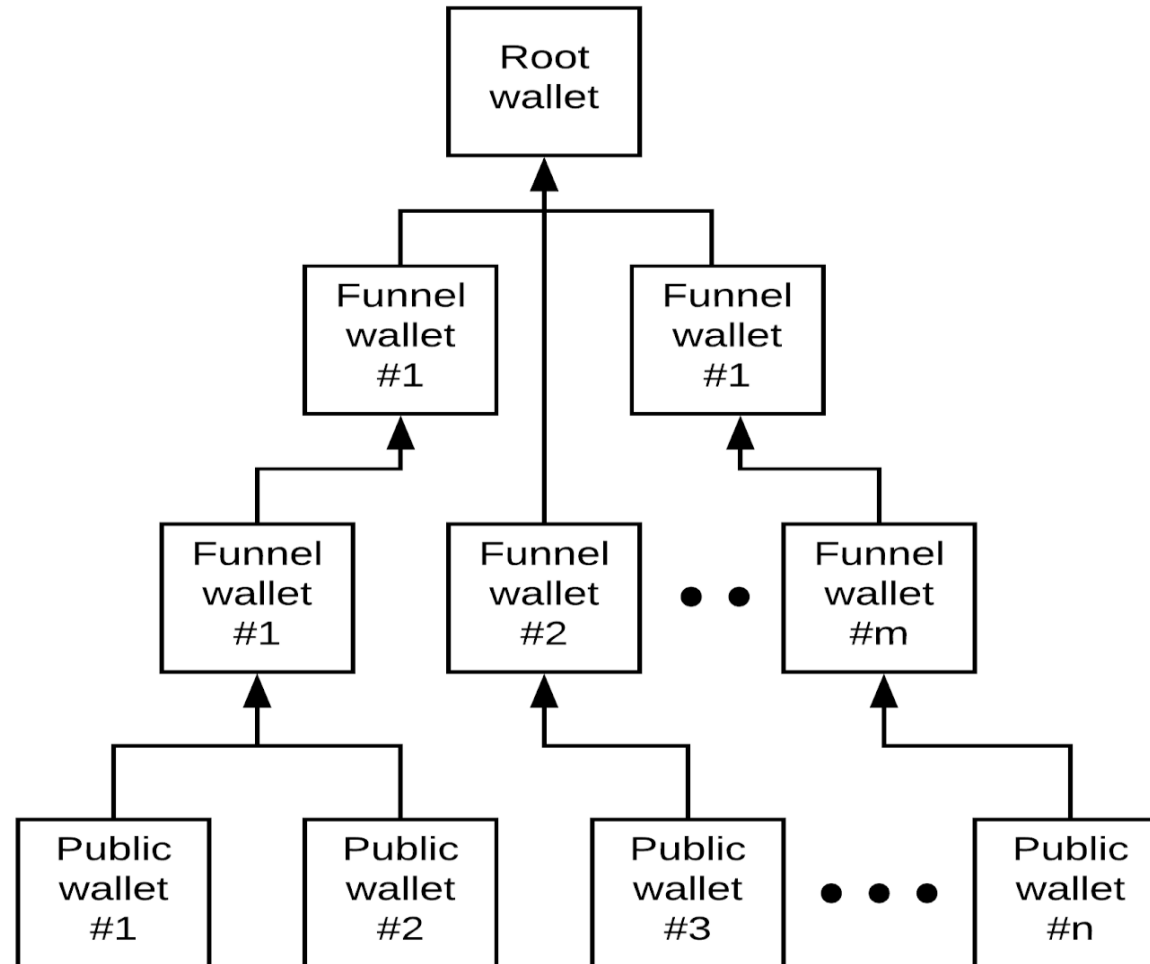
- Crypto scams are build like trees (simple) or graphs (complex)
- The leafs are the “public facing wallets” i.e. the wallets that are publicly shared in order to collect the funds from the victims.
- The “public facing wallets” appear in the ponzi websites and IM groups (Telegram, WhatsApp, etc...)
- 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

# Use case – MMM leaf wallet

- From intelligence we discover a leaf wallet, for example:
- [1BQZA4AGhAqpGhfKTnPk99n4pBNRjmvwmwX](#)

Wallet [4f95d462dc] ([show wallet addresses](#))

Page 1 / 1 (total transactions: 6)

[Download as CSV](#)

date		received/sent	balance	transaction
2015-12-26 05:19:00		-4.80956873 (-0.0001) <span style="color: red;">fee</span>	0.	<a href="#">48243a995726b2d4cc84...</a>
2015-12-24 17:33:51	<span style="background-color: #90EE90; border: 1px solid black; padding: 2px;">[ffd33e64e5]</span>	+2.98171217	4.80966873	<a href="#">f29525168a80309ccfe5...</a>
2015-12-24 09:36:51	<span style="background-color: #808080; border: 1px solid black; padding: 2px;">[93105fb3b3]</span>	+1.56815973	1.82795656	<a href="#">0d01c033e09d37e0db16...</a>
2015-12-18 13:27:20		-19.79588246 (-0.0001) <span style="color: red;">fee</span>	0.25979683	<a href="#">a066cf94649af8f75edb...</a>
2015-12-17 02:47:28		-2.14712071 (-0.0001) <span style="color: red;">fee</span>	20.05577929	<a href="#">3efb1701d2d7d44bc149...</a>
2015-12-16 09:25:58	<span style="background-color: #90EE90; border: 1px solid black; padding: 2px;">[Huobi.com-2]</span>	+22.203	22.203	<a href="#">ebbca839a6eed2c7cb88...</a>

Page 1 / 1 (total transactions: 6)

[Download as CSV](#)





# Use case – MMM leaf wallet

- We see that this wallet received funds from an exchange and two other private wallets

Wallet [4f95d462dc] ([show wallet addresses](#))

Page 1 / 1 (total transactions: 6)

[Download as CSV](#)

date	received/sent	balance	transaction
2015-12-26 05:19:00	-4.80956873 <span style="background-color: #90EE90; border: 1px solid black; padding: 2px;">[ff3105fb3b3]</span> (-0.0001) <i>fee</i>	0.	<a href="#">48243a995726b2d4cc84...</a>
2015-12-24 17:33:51	<span style="background-color: #90EE90; border: 1px solid black; padding: 2px;">[ffd33e64e5]</span> +2.98171217	4.80966873	<a href="#">f29525168a80309ccfe5...</a>
2015-12-24 09:36:51	<span style="background-color: #808080; border: 1px solid black; padding: 2px;">[93105fb3b3]</span> +1.56815973	1.82795656	<a href="#">0d01c033e09d37e0db16...</a>
2015-12-18 13:27:20	-19.79588246 <span style="background-color: #800080; border: 1px solid black; padding: 2px;">[2072460766]</span> (-0.0001) <i>fee</i>	0.25979683	<a href="#">a066cf94649af8f75edb...</a>
2015-12-17 02:47:28	-2.14712071 <span style="background-color: #000000; border: 1px solid black; padding: 2px;">[00001cc410]</span> (-0.0001) <i>fee</i>	20.05577929	<a href="#">3efb1701d2d7d44bc149...</a>
2015-12-16 09:25:58	<span style="background-color: #90EE90; border: 1px solid black; padding: 2px;">[ff3105fb3b3]</span> +22.203	22.203	<a href="#">ebbca839a6eed2c7cb88...</a>

Page 1 / 1 (total transactions: 6)

[Download as CSV](#)



# Use case – MMM leaf wallet

- The first deposit was funneled (22 BTC), and the 2<sup>nd</sup> deposit was directly converted in an exchange (Huobi is a Chinese exchange)

Wallet [4f95d462dc] ([show wallet addresses](#))

Page 1 / 1 (total transactions: 6)

[Download as CSV](#)

date		received/sent	balance	transaction
2015-12-26 05:19:00		-4.80956873 <span style="background-color: #90EE90; border: 1px solid black; padding: 2px;">Huobi.com-2</span> (-0.0001) <i>fee</i>	0.	<a href="#">48243a995726b2d4cc84...</a>
2015-12-24 17:33:51	<span style="background-color: #90EE90; border: 1px solid black; padding: 2px;">[ffd33e64e5]</span>	+2.98171217	4.80966873	<a href="#">f29525168a80309ccfe5...</a>
2015-12-24 09:36:51	<span style="background-color: #808080; border: 1px solid black; padding: 2px;">[93105fb3b3]</span>	+1.56815973	1.82795656	<a href="#">0d01c033e09d37e0db16...</a>
2015-12-18 13:27:20		-19.79588246 <span style="background-color: #6A5ACD; border: 1px solid black; padding: 2px;">[2072460766]</span> (-0.0001) <i>fee</i>	0.25979683	<a href="#">a066cf94649af8f75edb...</a>
2015-12-17 02:47:28		-2.14712071 <span style="background-color: #000080; border: 1px solid black; padding: 2px;">[00001cc410]</span> (-0.0001) <i>fee</i>	20.05577929	<a href="#">3efb1701d2d7d44bc149...</a>
2015-12-16 09:25:58	<span style="background-color: #90EE90; border: 1px solid black; padding: 2px;">Huobi.com-2</span>	+22.203	22.203	<a href="#">ebbca839a6eed2c7cb88...</a>

Page 1 / 1 (total transactions: 6)

[Download as CSV](#)



# Use case – funneling the funds

- Let's look at the funneling wallet: [1egFemyAdNgXzdq9E2UDnejYYtvYNUghc](#)
- A funneling wallet main property is a zero balance with plenty of traffic

2015-12-25 04:25:21		-2.24310805 (-0.0001)	■ [00001cc410] fee	0.01060077	<a href="#">599ad99df033e2908de0...</a>
2015-12-25 03:18:58	■ [9877f5d228]	+2.25		2.25380882	<a href="#">25f73cc2155f907a0828...</a>
2015-12-24 20:09:10		-2.24310805 (-0.0001)	■ [00001cc410] fee	0.00380882	<a href="#">492607522dd42a20bed5...</a>
2015-12-24 20:09:10		-2.24310805 (-0.0001)	■ [00001cc410] fee	2.24701687	<a href="#">868a3c701c675caec646...</a>
2015-12-24 19:59:23		-15.30991645 (-0.0001)	■ [00007d59f2] fee	4.49022492	<a href="#">db0e68100c4c3e4aa4ca...</a>
2015-12-24 17:49:56	■ [9877f5d228]	+19.8		19.80024137	<a href="#">6394b16f57cdcff89c4b...</a>
2015-12-20 07:03:46		-36.82 (-0.0001)	■ [bd89cc0791] fee	0.00024137	<a href="#">95c4622edde309afb00e...</a>
2015-12-19 14:50:46	■ [ffa9b9e2f7]	+17.02445891		36.82034137	<a href="#">c70344d43c1e71758813...</a>
2015-12-18 13:27:20	■ [4f95d462dc]	+19.79588246		19.79588246	<a href="#">a066cf94649af8f75edb...</a>



# Use case – funneling the funds

- Let's dive into the 1<sup>st</sup> funneling cycle:  
[1NGpnazTZR6pE5uprbGfQGGMV4GmYMDtq](https://1NGpnazTZR6pE5uprbGfQGGMV4GmYMDtq)
- This is another funneling wallet, since we see cycles for inputs and outputs with zero balance

Wallet [bd89cc0791] ([show wallet addresses](#))

Page 1 / 1 (total transactions: 71)

[Download as CSV](#)

date		received/sent	balance	transaction
2015-12-21 09:34:34		-73.6699 (-0.0001) <span style="color: green;">[9877f5d228]</span> <i>fee</i>	0.	<a href="#">0c2ba1a9ba169714aab1...</a>
2015-12-20 07:03:46	<span style="background-color: #4b0082; color: white; padding: 2px 5px;">[2072460766]</span>	+36.82	73.67	<a href="#">95c4622edde309afb00e...</a>
2015-12-20 06:39:17	<span style="background-color: #228b22; color: white; padding: 2px 5px;">[c0dc68ffe2]</span>	+36.85	36.85	<a href="#">1fa4b751035249f8d916...</a>
2015-12-19 17:15:15		-268.43155781 (-0.0003) <span style="color: green;">[9877f5d228]</span> <i>fee</i>	0.	<a href="#">bd0566aa1045ff5cfe26...</a>
2015-12-19 13:53:40	<span style="background-color: #003366; color: white; padding: 2px 5px;">[de9c7c16a4]</span>	+31.32	268.43185781	<a href="#">d58c58e932eec13b0b6a...</a>
2015-12-19 13:53:40	<span style="background-color: #008000; color: white; padding: 2px 5px;">[9c15e5dc70]</span>	+34.08	237.11185781	<a href="#">ed383880a590d04fb14d...</a>
2015-12-19 13:42:28	<span style="background-color: #008080; color: white; padding: 2px 5px;">[c1d0c3796b]</span>	+35.748	203.03185781	<a href="#">3cd58643e6e31ba71e29...</a>
2015-12-19 13:42:28	<span style="background-color: #008000; color: white; padding: 2px 5px;">[c192b2721c]</span>	+34.67	167.28385781	<a href="#">eba2b82c7806185f738f...</a>
2015-12-19 10:41:46	<span style="background-color: #3333ff; color: white; padding: 2px 5px;">[8efa0eb0fe]</span>	+33.027	132.61385781	<a href="#">5705ac4fb9e5c81c8ac1...</a>

# Use case – funneling the funds

- Let's dive into the 1<sup>st</sup> funneling cycle:  
[1NGpnazTZR6pE5uprbGfQGGMV4GmYMDtq](https://blockchainexplorer.org/address/1NGpnazTZR6pE5uprbGfQGGMV4GmYMDtq)
- This is another funneling wallet, since we see cycles for inputs and outputs with zero balance
- Looking at this wallet we see additional funneling and some transactions to exchanges for fiat exfiltration
  - 11 BTC to HaoBTC
  - 18 BTC to BTCC
- And the majority of the funds were funneled to:  
[1LVXa7xrFn27qV89WAXW2h9pcHPzkcW7F6](https://blockchainexplorer.org/address/1LVXa7xrFn27qV89WAXW2h9pcHPzkcW7F6)



# Use case – root wallet

- Let's look at the root wallet:  
[1LVXa7xrFn27qV89WAXW2h9pcHPzkcW7F6](https://www.walletexplorer.com/wallet/1LVXa7xrFn27qV89WAXW2h9pcHPzkcW7F6)
- This wallet transacted over 7500 BTC (**\$54M**) from May 2015 until about a week ago
- This is probably a hot wallet working in tandem with a cold wallet:  
<https://www.walletexplorer.com/wallet/0000375430188cff>
- The (probably) cold wallet **currently holds 438.28 BTC (\$3.1M)** and is comprised of 284,307 different addresses, generated to hide the wallet from tracking

# What's next ?

- This campaign can be further mapped, to find additional funnels and leaves
- Law enforcement can contact the regulated exchanges the scammer traded with and ask for the KYC data of the person who owns the root wallet

# Let's look at another use case

- Let's pull a scam from the EtherScamDB

 Scamming	Investments	 Active	bit-donor.com
--	-------------	--	---------------

- This looks like an active ponzi 😊:

Silver Plan	Gold Plan	Diamond Plan
<b>120%</b> After 24 Hours	<b>140%</b> After 48 Hours	<b>350%</b> After 72 Hours
Min: \$ 10	Min: \$ 100	Min: \$ 1,000
Max: \$ 100	Max: \$ 1,000	Max: Unlimited
Ref Commissions : 3%	Ref Commissions : 3%	Ref Commissions : 3%
Withdraw Instantly	Withdraw Instantly	Withdraw Instantly
<a href="#">Signup</a>	<a href="#">Signup</a>	<a href="#">Signup</a>





# 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 <span style="color: red;">■</span> <a href="#">[13c3c3935d]</a> (-0.00012112) <i>fee</i>	0.00783349	<a href="#">2c75169c03509e2b98a0...</a>
2019-11-21 11:47:57	<span style="color: teal;">■</span> <a href="#">[1e8c4515b5]</a>	+0.00126514	0.01121471	<a href="#">95071e5245ed7ff56205...</a>
2019-10-31 15:40:38	<span style="color: purple;">■</span> <a href="#">[0961215f90]</a>	+0.00420394	0.00994957	<a href="#">d32ec25761ec5af933c3...</a>
2019-10-31 11:05:04		-0.00166639 <span style="color: purple;">■</span> <a href="#">[0961215f90]</a> (-0.0000748) <i>fee</i>	0.00574563	<a href="#">040fd5d87d60dc3439e7...</a>
2019-10-27 17:13:47	<span style="color: purple;">■</span> <a href="#">[05ce2fb190]</a>	+0.00209474	0.00748682	<a href="#">5d6ded87d8c386f0e445...</a>
2019-10-26 13:23:28		-0.00130492 <span style="color: lightgreen;">■</span> <a href="#">[1a989000a6]</a> (-0.00013334) <i>fee</i>	0.00539208	<a href="#">2edfa7090c7e93193213...</a>
2019-10-25 11:34:20	<span style="color: purple;">■</span> <a href="#">[05ce2fb190]</a>	+0.00263958	0.00683034	<a href="#">6fea8e4b617524b08383...</a>
2019-10-25 08:08:54	<span style="color: lightgreen;">■</span> <a href="#">[1a989000a6]</a>	+0.00133744	0.00419076	<a href="#">b1e8198982de02da6398...</a>
2019-10-21 14:10:59		-0.00339296 <span style="color: darkgreen;">■</span> <a href="#">CoinPayments.net</a> (-0.0000052) <i>fee</i>	0.00285332	<a href="#">a8e1afe00b228e02130d...</a>
2019-10-18 16:06:26	<span style="color: purple;">■</span> <a href="#">[8045f562a3]</a>	+0.00252122	0.00625148	<a href="#">71bc8d8f44d03c4dca77...</a>
2019-10-09 20:58:30	<span style="color: brown;">■</span> <a href="#">[85821394ed]</a>	+0.00116224	0.00373026	<a href="#">48ec87c4e310777fcb79...</a>



# Leaf wallet – bit-donor.com

- [1Fr2VJ2pgMsAktcLonHUqBnZbu7H1zZLpH](https://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](https://bit-donor.com/1DKYRgUVvQhFb3rb1DjejRxyDGkC211xU9)



# Funneling wallet – bit-donor.com

- Let's look at the funneling wallet:  
[1DKYRgUVvQhFb3rb1DjejRxyDGkC211xU9](https://bit-donor.com/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	<span style="background-color: #89dfe7747d; border: 1px solid #ccc; padding: 2px;">[89dfe7747d]</span> +0.00964091	0.01002401	b88a71ed5b51f6105808...
2019-08-18 16:04:25	-0.03862224 <span style="background-color: #f59e00; border: 1px solid #ccc; padding: 2px;">[35ef9bfe3e]</span> (-0.00014212) fee	0.0003831	43bfd59c57f54abc6d6...
2019-08-18 08:23:12	-0.00147688 <span style="background-color: #c00000; border: 1px solid #ccc; padding: 2px;">[22709c48fc]</span> (-0.00000452) fee	0.03914746	17c7ff6d69aaa89da240...
2019-08-15 15:47:07	<span style="background-color: #89dfe7747d; border: 1px solid #ccc; padding: 2px;">[89dfe7747d]</span> +0.03970846	0.04062886	eb30406b92d59eafb5b1...
2019-08-14 16:08:21	-0.00379916 <span style="background-color: #89dfe7747d; border: 1px solid #ccc; padding: 2px;">[89dfe7747d]</span> (-0.0001044) fee	0.0009204	8acaa5cf33bfcff66b8c...
2019-08-11 15:27:08	-0.00123097 <span style="background-color: #90ee90; border: 1px solid #ccc; padding: 2px;">[b56fea8dca]</span> (-0.00000226) fee	0.00473	d50ff096b808f37a4348...
2019-08-11 14:37:34	-0.04429288 <span style="background-color: #f59e00; border: 1px solid #ccc; padding: 2px;">[35ef9bfe3e]</span> (-0.00001496) fee	0.00596323	c1bf2fb0e265cdbdff63...
2019-08-08 20:06:23	<span style="background-color: #89dfe7747d; border: 1px solid #ccc; padding: 2px;">[89dfe7747d]</span> +0.04305134	0.05027107	95b562e9d641b955929f...
2019-08-06 21:18:20	-0.25733424 <span style="background-color: #f59e00; border: 1px solid #ccc; padding: 2px;">[00cedcb2e5]</span> (-0.00001044) fee	0.00721973	0f7fccf14b160f74495c...
2019-08-06 12:00:51	<span style="background-color: #89dfe7747d; border: 1px solid #ccc; padding: 2px;">[89dfe7747d]</span> +0.19509646	0.26456441	752c4244d161c48df9f5...
2019-08-05 19:10:48	<span style="background-color: #89dfe7747d; border: 1px solid #ccc; padding: 2px;">[89dfe7747d]</span> +0.02376351	0.06946795	06f3c1f5fd0c24ee81a9...
2019-08-05 12:58:53	<span style="background-color: #89dfe7747d; border: 1px solid #ccc; padding: 2px;">[89dfe7747d]</span> +0.04250565	0.04570444	60e05cd5d8d7aafeb3b5...
2019-08-04 16:35:26	-0.12787501 <span style="background-color: #f59e00; border: 1px solid #ccc; padding: 2px;">[004bd96c19]</span> (-0.0001474) fee	0.00319879	e4cd54f1bcc7139df15c...
2019-08-04 09:53:58	<span style="background-color: #89dfe7747d; border: 1px solid #ccc; padding: 2px;">[89dfe7747d]</span> +0.01400997	0.1312212	8593e2dcbf0223b26baa...
2019-08-03 14:19:11	<span style="background-color: #89dfe7747d; border: 1px solid #ccc; padding: 2px;">[89dfe7747d]</span> +0.02790269	0.11721123	0d55ddb32097fa97d7b2...
2019-07-30 08:57:23	<span style="background-color: #89dfe7747d; border: 1px solid #ccc; padding: 2px;">[89dfe7747d]</span> +0.08413091	0.08930854	19e1f503e9e7d82d47c5...



# Funneling wallet – bit-donor.com

- Let's look at the funneling wallet:  
[1DKYRgUVvQhFb3rb1DjejRxyDGkC211xU9](https://www.walletexplorer.com/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.

Questions so far ?





Coffee break







# Excessive – investigate a scam yourself

- Intelligence:
  - Ethereum wallet: 0x4307e7d64a0f936bb719dda5ca177f493f846228
- Tool: <https://dev.naboo.io>
- Credentials:
  - Username: [guest@inspectolabs.com](mailto:guest@inspectolabs.com)
  - Password: QWERTY13



# Use Case - Leaf wallet

- Leaf wallets come up from Intelligence, in this case it's a Ponzi scam

Address **0x4307e7D64a0F936bB719DDa5CA177F493F846228** ●

Balance: 0

Transactions: 4 txns

Meta data

Name: -

Geo location: -

Ip address: -

The wallet is marked in red, meaning it is directly connected to illegal activity

Transactions Expansions Reasons

Latest 4 txns

TxHash	Age	From		To	Value
0xade60cbdd6f564...	1 year ago	● 0x4307e7d64a0f93...	OUT	● 0xf37448a0d9c5d9...	1.093659
0x58fecefa3a2637...	1 year ago	● 0xd551234ae421e3...	IN	● 0x4307e7d64a0f93...	0.993994
0x413167737eb849...	1 year ago	● 0x11a085633e1922...	IN	● 0x4307e7d64a0f93...	0.091618
0xcfce5525326a9e...	1 year ago	● 0x416299aade6443...	IN	● 0x4307e7d64a0f93...	0.01

It is a leaf wallet, since it received funds from "green" wallets (the victims) and funnels all the funds to a funneling wallet



# Use Case - Leaf wallet

By clicking on the “Expansions” tab, the relevant intelligence is displayed

Address 0x4307e7D64a0F936bB719DDa5CA177F493F846228 ●

Balance: 0  
 Transactions: 4 txns

Meta data  
 Name: -  
 Geo location: -  
 Ip address: -

Transactions   **Expansions**   Reasons

Latest 2 expansions

Source GUID	Source Name	Date	Type	Meta
eddc35f9-58a8-4428-9d76-381ad4e83119	BTC Scams	"2019-07-10T16:44:07.000Z"	ETH	{ "id": 459, "url": "https://buterineth.org", "coin": "ETH", "name": "buterineth.org", "category": "Scamming", "reporter": "MyCrypto", "description": "Trust trading scam site", "subcategory": "Trust-Trading" }
396b194c-b1b5-424d-8183-0dd356dda129	EherScamDB	"2019-07-10T16:44:00.000Z"	ETH	{ "id": 4591, "url": "https://buterineth.org", "coin": "ETH", "name": "buterineth.org", "status": "Offline", "category": "Scamming", "reporter": "MyCrypto", "description": "Trust trading scam site", "subcategory": "Trust-Trading" }

This specific scam is offline, it was active during Mar-July, 2018



# Use Case - Follow the money

From the leaf's transactions we see the funds funneled to one wallet

Address ● 0x4307e7D64a0F936bB719DDa5CA177F493F846228 ●

Balance: 0

Transactions: [4 txns](#)

Meta data

Name: -

Geo location: -

Ip address: -

---

Transactions   Expansions   Reasons

Latest 4 txns

TxHash	Age	From	To	Value
<a href="#">0xade60cbdd6f564...</a>	1 year ago	<span style="color: red;">●</span> <a href="#">0x4307e7d64a0f93...</a>	<span style="background-color: orange; padding: 2px;">OUT</span> <span style="color: red;">●</span> <a href="#">0xf37448a0d9c5d9...</a>	1.093659
<a href="#">0x58fecefa3a2637...</a>	1 year ago	<span style="color: green;">●</span> <a href="#">0xd551234ae421e3...</a>	<span style="background-color: green; padding: 2px;">IN</span> <span style="color: red;">●</span> <a href="#">0x4307e7d64a0f93...</a>	0.993994
<a href="#">0x413167737eb849...</a>	1 year ago	<span style="color: green;">●</span> <a href="#">0x11a085633e1922...</a>	<span style="background-color: green; padding: 2px;">IN</span> <span style="color: red;">●</span> <a href="#">0x4307e7d64a0f93...</a>	0.091618
<a href="#">0xcfce5525326a9e...</a>	1 year ago	<span style="color: green;">●</span> <a href="#">0x416299aade6443...</a>	<span style="background-color: green; padding: 2px;">IN</span> <span style="color: red;">●</span> <a href="#">0x4307e7d64a0f93...</a>	0.01

Start tracking...





# Use Case - Funneling wallet

A funneling wallet main function is to funnel out funds it receives

Address ● `0xf37448a0d9c5d976edcdf4544f4601e6b163c3c9`

**Balance:** 0

**Transactions:** 19 txns

**Meta data**

**Name:** -

**Geo location:** -

**Ip address:** -

The wallet is marked in red, meaning it is directly connected to illegal activity

The balance is zero since all funds recieved are funnled out

Transactions	Expansions	Reasons		
Latest 19 txns				
TxHash	Age	From	To	Value
<a href="#">0xc8df196cd15c6f...</a>	1 year ago	<span style="color: red;">●</span> <code>0xf37448a0d9c5d9...</code>	<span style="background-color: #ffc107;">OUT</span> <span style="color: green;">●</span> <code>0x2b5634c4205580...</code>	1.093449
<a href="#">0xade60cbdd6f564...</a>	1 year ago	<span style="color: red;">●</span> <code>0x4307e7d64a0f93...</code>	<span style="background-color: #28a745;">IN</span> <span style="color: red;">●</span> <code>0xf37448a0d9c5d9...</code>	1.093659
<a href="#">0x20aa11de6cf3e8...</a>	1 year ago	<span style="color: red;">●</span> <code>0xf37448a0d9c5d9...</code>	<span style="background-color: #ffc107;">OUT</span> <span style="color: green;">●</span> <code>0x2b5634c4205580...</code>	11.49829



# Use Case - Funneling wallet

A funneling wallet main function is to funnel out funds it receives

Address ● `0xf37448a0d9c5d976edcdf4544f4601e6b163c3c9`

**Balance:** 0

**Transactions:** 19 txns

**Meta data**

**Name:** -

**Geo location:** -

**Ip address:** -

Transactions    Expansions    Reasons

Latest 19 txns

TxHash	Age	From		To	Value
<a href="#">0xc8df196cd15c6f...</a>	1 year ago	<span style="color: red;">●</span> <a href="#">0xf37448a0d9c5d9...</a>	OUT	<span style="color: green;">●</span> <a href="#">0x2b5634c4205580...</a>	1.093449
<a href="#">0xade60cbdd6f564...</a>	1 year ago	<span style="color: red;">●</span> <a href="#">0x4307e7d64a0f93...</a>	IN	<span style="color: red;">●</span> <a href="#">0xf37448a0d9c5d9...</a>	1.093659
<a href="#">0x20aa11de6cf3e8...</a>	1 year ago	<span style="color: red;">●</span> <a href="#">0xf37448a0d9c5d9...</a>	OUT	<span style="color: green;">●</span> <a href="#">0x2b5634c4205580...</a>	11.49829

The wallet is marked in red, meaning it is directly connected to illegal activity

The balance is zero since all funds recieved are funnled out



# Use Case - Going up the tree

Looking through the transactions we see the next wallet

TxHash	Age	From	To	Value
0xc8df196cd15c6f...	1 year ago	● 0xf37448a0d9c5d9...	OUT ● 0x2b5634c4205580...	1.093449
0xade60cbdd6f564...	1 year ago	● 0x4307e7d64a0f93...	IN ● 0xf37448a0d9c5d9...	1.093659
0x20aa11de6cf3e8...	1 year ago	● 0xf37448a0d9c5d9...	OUT ● 0x2b5634c4205580...	11.49829
0x271aabacfed06d...	1 year ago	● 0x28a6d6e41fcca5...	IN ● 0xf37448a0d9c5d9...	0.4995
0x6e7197eddb6c78...	1 year ago	● 0x909aac466640b0...	IN ● 0xf37448a0d9c5d9...	10.999
0x0dcee9b7c58dbe...	1 year ago	● 0xf37448a0d9c5d9...	OUT ● 0x2b5634c4205580...	16.11179
0x11106cab4449b4...	1 year ago	● 0x909aac466640b0...	IN ● 0xf37448a0d9c5d9...	7.082
0xf24dd136acdc25...	1 year ago	● 0xa970052e459bc8...	IN ● 0xf37448a0d9c5d9...	9.03
0x8c055bc9c48d01...	1 year ago	● 0xf37448a0d9c5d9...	OUT ● 0x2b5634c4205580...	8.54879
0x155a1054211215...	1 year ago	● 0xa6a7d616dbbb6b...	IN ● 0xf37448a0d9c5d9...	4.269
0x04db2088a75edc...	1 year ago	● 0xa970052e459bc8...	IN ● 0xf37448a0d9c5d9...	4.28





# Use Case - Root wallet

This is a KuCoin exchange pool, in here the ETH is exfiltrated to cash

Address `0x2b5634c42055806a59e9107ed44d43c426e58258` ●

**Balance:** 6421.713458965468536267

**Transactions:** 25 txns


**Meta data**

**Name:** KuCoin regulated exchange pool

**Geo location:** UK

**Ip address:** -

The wallet is marked in green, since it belongs to a regulated exchange



Transactions   Expansions   Reasons

Latest 25 txns

TxHash	Age	From	To	Value
<a href="#">0x2d2907c52f37ab...</a>	2 minutes ago	<span style="color: green;">●</span> <a href="#">0x2b5634c4205580...</a>	<span style="background-color: orange; color: white; padding: 2px;">OUT</span> <span style="color: green;">●</span> <a href="#">0x8276706d30b59b...</a>	3.92125226
<a href="#">0xd4de5177b9b734...</a>	2 minutes ago	<span style="color: green;">●</span> <a href="#">0x2b5634c4205580...</a>	<span style="background-color: orange; color: white; padding: 2px;">OUT</span> <span style="color: orange;">●</span> <a href="#">0xd4fa1460f537bb...</a>	0
<a href="#">0x0477584fa2e03c...</a>	3 minutes ago	<span style="color: green;">●</span> <a href="#">0x2b5634c4205580...</a>	<span style="background-color: orange; color: white; padding: 2px;">OUT</span> <span style="color: green;">●</span> <a href="#">0x1d462414fe14cf...</a>	0

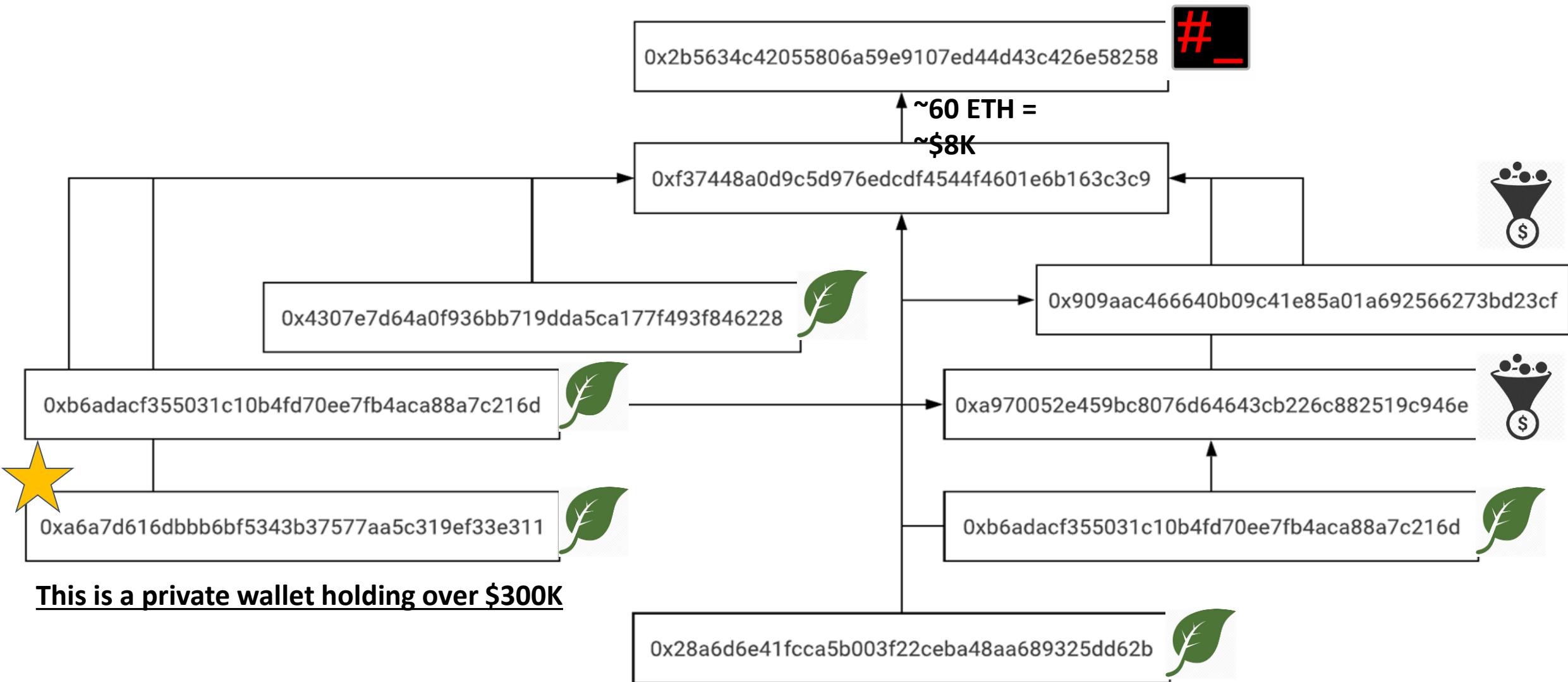


# What's next ?

- This campaign can be further mapped, to find additional funnels and leaves, for example:
  - 2<sup>nd</sup> Funneling wallet: 0x909aac466640b09c41e85a01a692566273bd23cf
  - 2<sup>nd</sup> Leaf wallet: 0x28a6d6e41fccca5b003f22ceba48aa689325dd62b
- After the complete mapping (see next slide) we can estimate the total funds laundered by the campaign, this specific example its ~\$8K.
- Law enforcement can contact KuCoin and ask for the KYC data of the person who owns the root wallet



# Mapping of the campaign



Questions so far ?

