Bitcoin Intelligence

Follow the money in the cryptocurrency world

RANSOMWARE

3 MILLION ATTACKS + 6000%

1 BILLION USD IN BITCOIN

DARKNET MARKETS

WEAPONS

DRUGS

PEDOPORNOGRAPHY

ILLEGAL SERVICES

REVENUES DOUBLED

MONEY LAUNDERING

TAX EVASION

TRANSFER ABROAD

ILLEGAL FUNDS

BITCOIN TX ARE FAST AND EASY

WTF ???

Dicono gli esperti (1)

…chiedendo la restituzione [dei dati] dietro il pagamento di una somma in “bit coin”.

...un riscatto esclusivamente in bitcoin, la valuta meno rintracciabile del mondo.

...pagamenti in bitcoin: la moneta virtuale gestita da personaggi misteriosi.

Dicono gli esperti (2)

...questa moneta può essere usata ovunque nel mondo ed a qualsiasi ora.

...siamo in grado di verificare quanti soldi sono stati raccolti da Wannacry grazie ad un tecnico di Google.

?

Follow the money!

ma con qualche piccola differenza…

Opportunità

La *blockchain* è un *public ledger* e chiunque può esaminare lo storico completo delle transazioni effettuate in bitcoin.

La rete P2P su cui si regge Bitcoin è aperta e chiunque vi può partecipare.

Limitazioni (1)

Bitcoin utilizza degli pseudonimi (*bitcoin address*) per inviare e ricevere denaro.

1EwNzYZPKupvYeZ4nYKGw36pH483Lgbx7L

Solo chi possiede la “chiave privata” relativa ad un certo indirizzo può spenderne il contenuto.

Limitazioni (2)

E’ possibile creare un nuovo indirizzo per ogni transazione.

Oltre 250 milioni di indirizzi ad oggi nella blockchain.

di cui 230 milioni usati una sola volta…

Non esiste una entità di controllo centrale.

Limitazioni (3)

A complicare le cose ci si aggiungono i bitcoin *mixer*.

Servizi che possono mascherare gli indirizzi di origine e/o destinazione di una transazione.

Sfruttiamo le opportunità!

e aggiriamo le limitazioni…

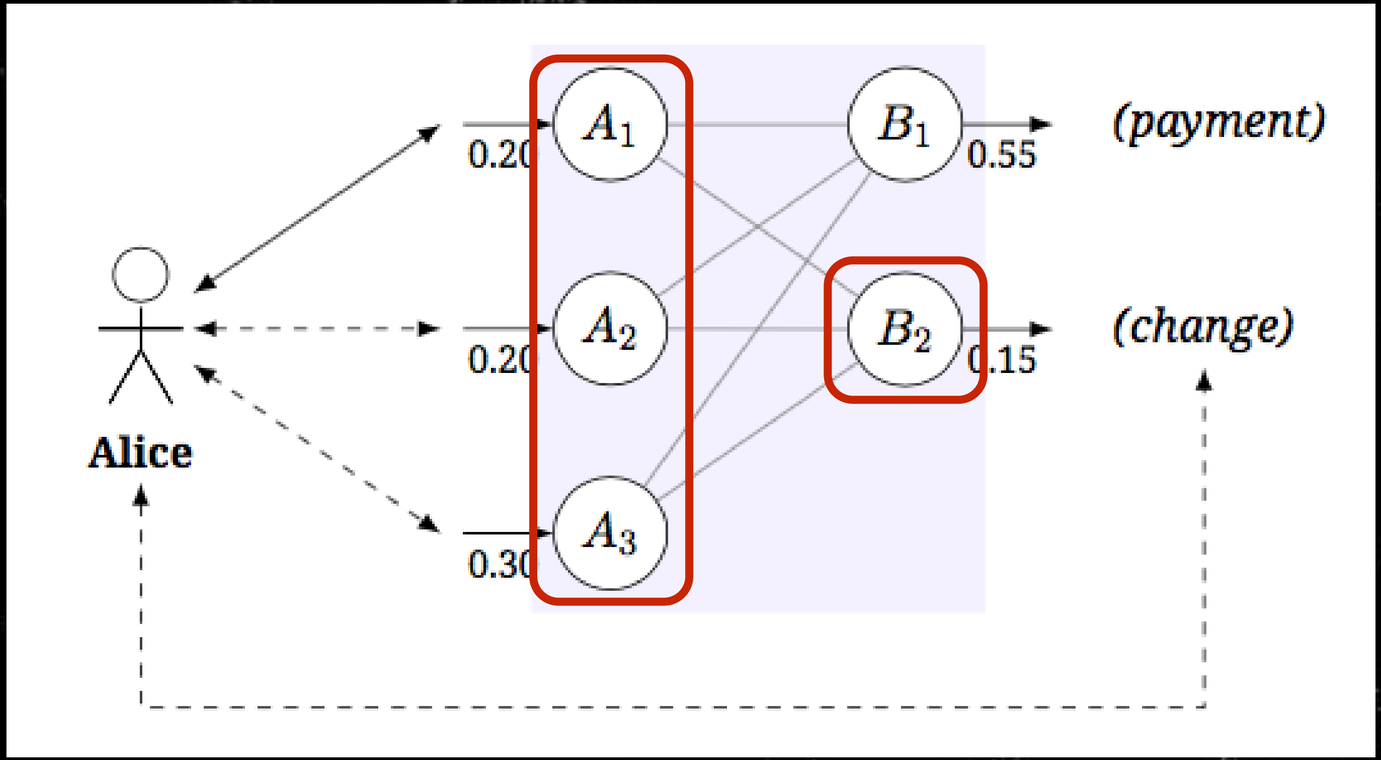
Tecniche di analisi

Address clustering

Address clustering

Permette di identificare il wallet di una data entità
cioè l’insieme di indirizzi controllati da essa.

Vengono utilizzati degli algoritmi euristici di *clustering* sui dati contenuti nella blockchain.



esempio di clustering

Servizi e software gratuiti

www.walletexplorer.com

bit-cluster.com

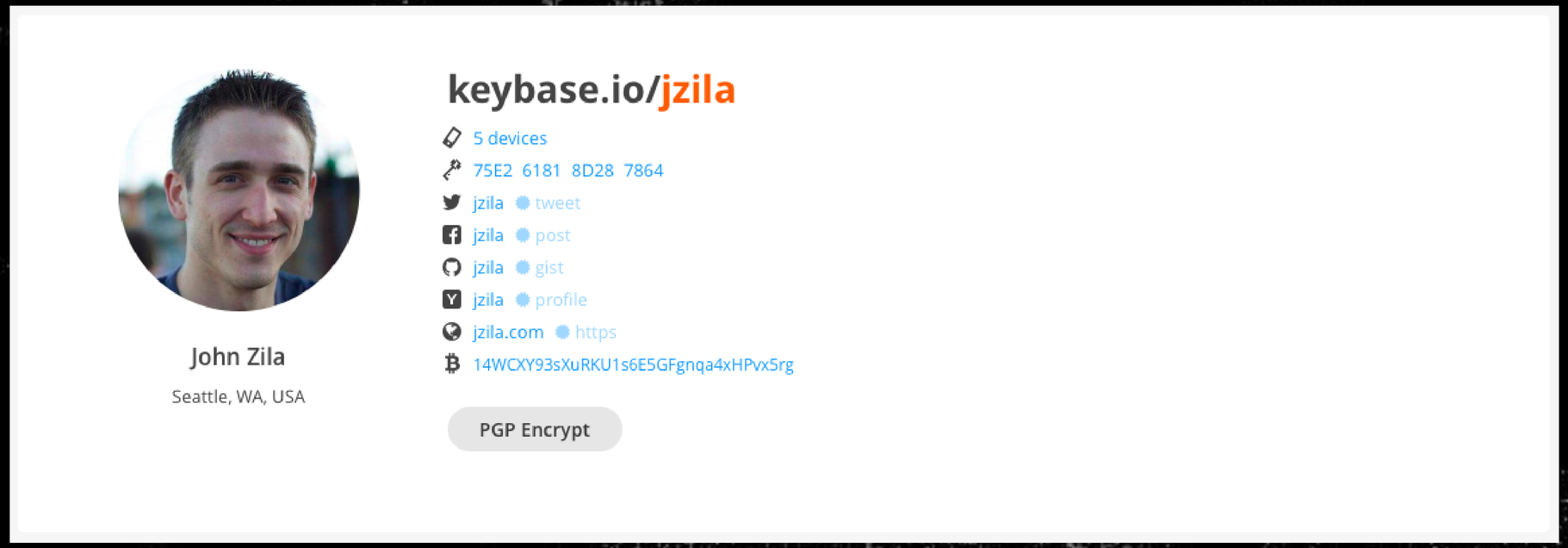
etc.

Tecniche di analisi

OpenSource Intelligence

OSINT (1)

Ci sono numerose fonti per ottenere informazioni in rete sugli indirizzi bitcoin.



Indirizzi bitcoin su keybase.io

OSINT (2)

Un semplice *crawler* permette di creare un buon database di informazioni.

E’ molto efficace anche sulla *darknet*.

OSINT (3)

Parsing delle pagine tramite *regular expression*.

/(?<![a-km-zA-HJ-NP-Z0-9])[13][a-km-zA-HJ-NP-Z0-9]{26,33}(?![a-km-zA-HJ-NP-Z0-9])/

Possibili target:

Forum - (BitcoinTalk, BitcoinForum, etc.)

Keybase

Pastebin

Il resto di internet...

Alcuni database on-line

www.walletexplorer.com

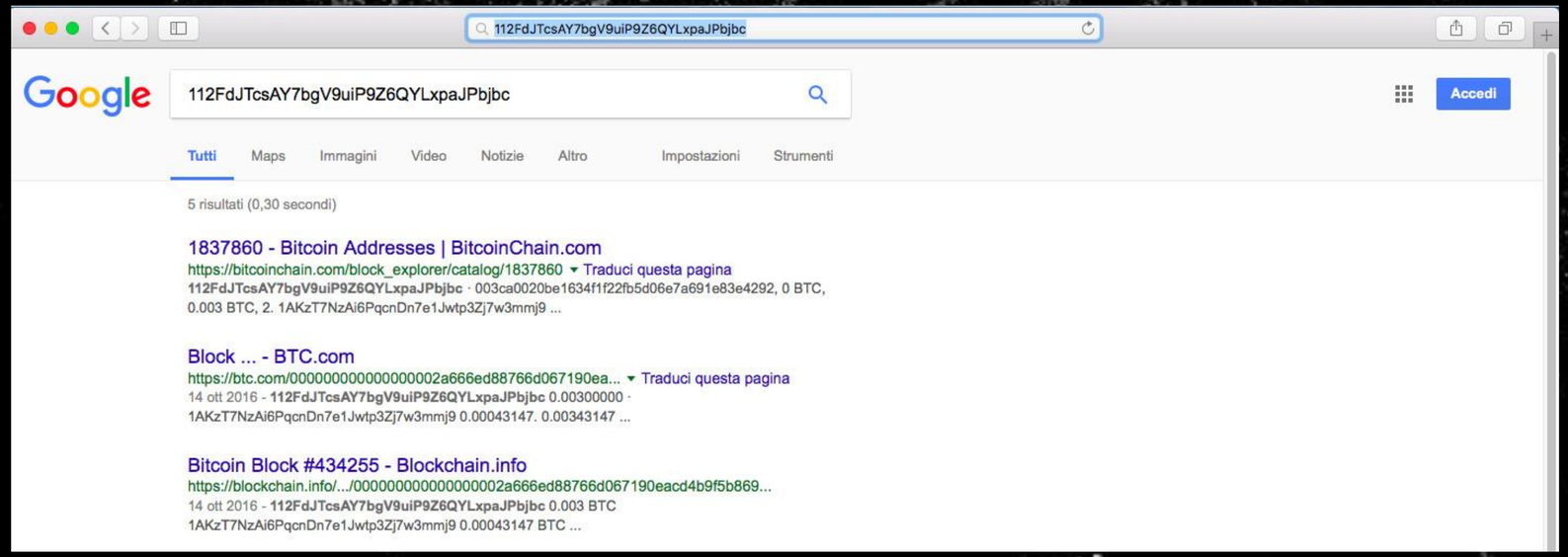
blockchain.info/tags

etc.

Google search per indirizzi

Non sempre efficace.

Si ottiene molto “rumore".



Categorizzazione manuale

Interazione manuale per identificare e categorizzare i maggiori servizi attivi nel mondo bitcoin.

L’efficacia è ovviamente maggiore se si combina con l’*address clustering*.

Per un’analisi più approfondita

"A Fistful of Bitcoins: Characterizing Payments Among Men with No Names"
(University of California, George Mason University).

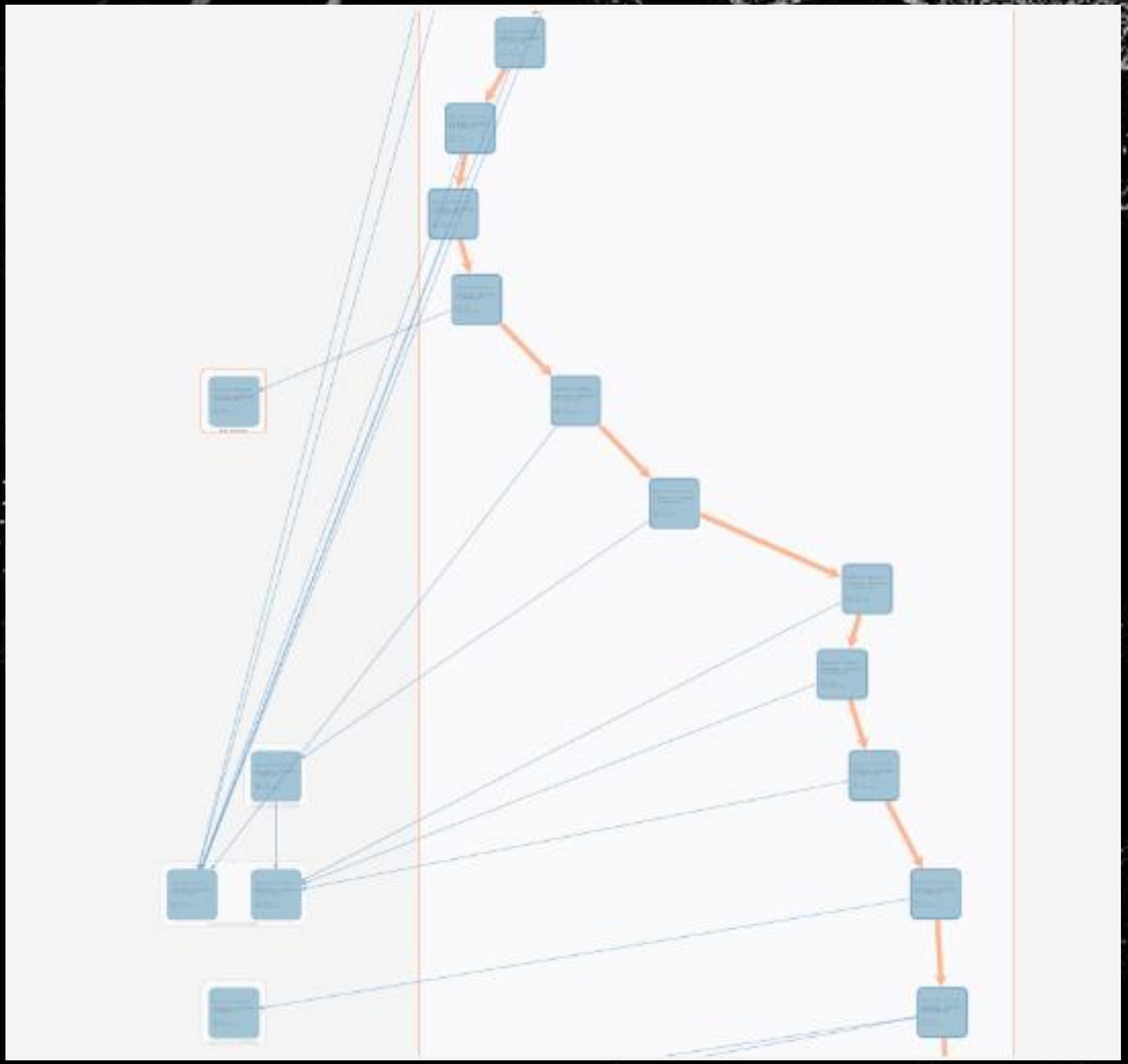
Tecniche di analisi

Pattern Analysis

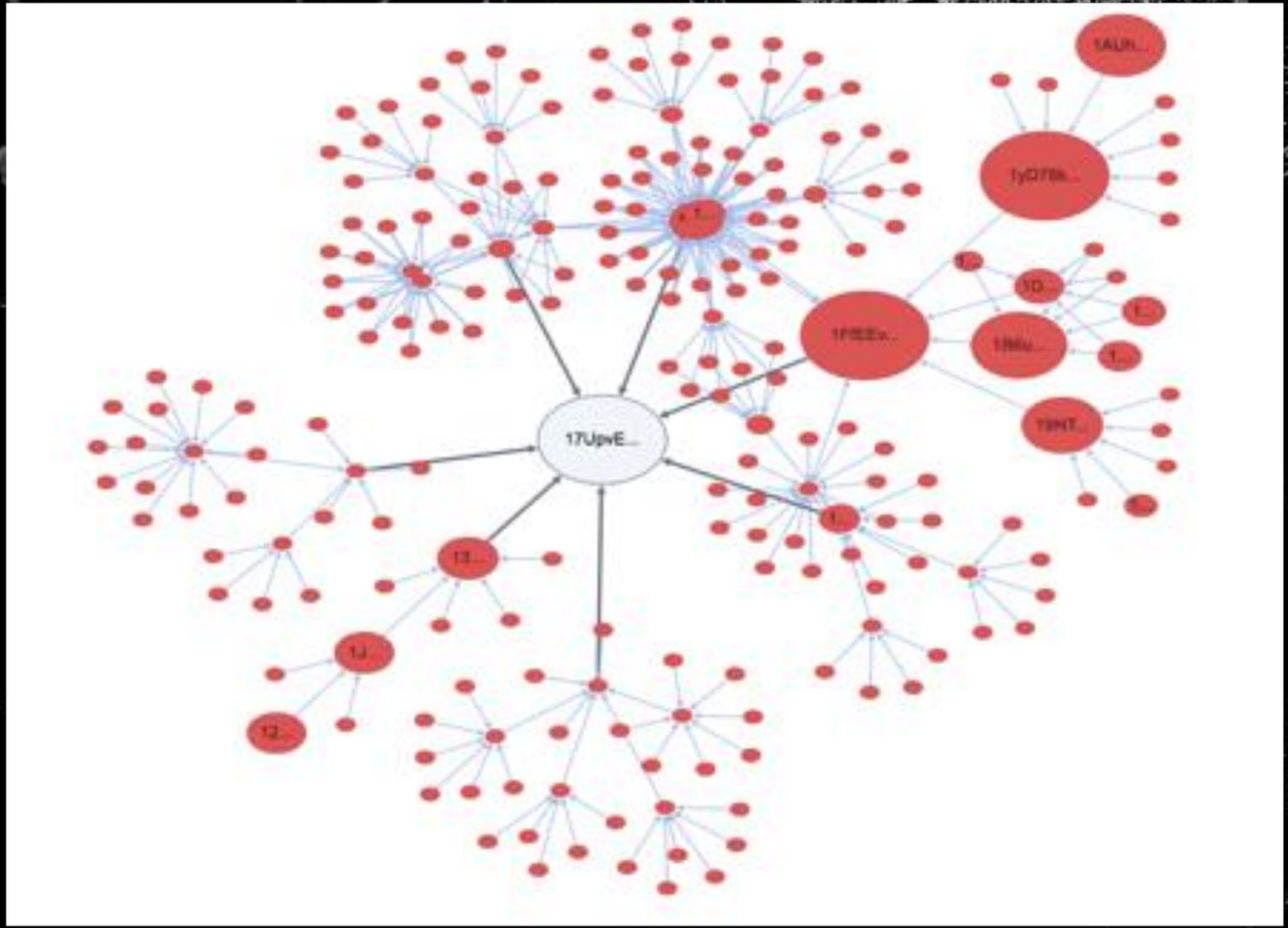
Pattern analysis

Algoritmi euristici e di *machine learning* applicati alla blockchain.

Permettono di identificare schemi di transazioni tipici di alcune attività illecite.



Ransomware payment scheme



Bitcoin mixing & money laundering

Tecniche di analisi
Geotracking

Geotracking

Chiunque può partecipare alla rete P2P di Bitcoin.

Utilizzando un numero di nodi arbitrario.

Monitorando come le informazioni si propagano sulla rete è possibile cercare di individuare il punto di origine di una transazione.

Indirizzo IP o servizio utilizzato.

Le basi teoriche

"*An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*" (P. Koshy, D. Koshy, P. McDaniel).

"*Deanonymisation of clients in Bitcoin P2P network*" (A.Biryukov, D. Khovratovich, I. Pustogarov).

"*On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients*" (A. Gervais, G. Karame, D. Gruber, S. Capkun).

Servizi e software gratuiti

blockchain.info implementa in maniera rudimentale una piccola parte di queste tecniche.

Geotracking di blockchain.info

Summary	
Size	225 (bytes)
Received Time	2016-10-21 06:20:15
Included In Blocks	435208 (2016-10-21 06:24:47 + 5 minutes)
Confirmations	29598 Confirmations
Relayed by IP	85.25.139.133 (whois)
Visualize	View Tree Chart

Network Propagation

…in realtà questa transazione era stata fatta da Roma

STRICTLY CONFIDENTIAL

Tecniche di analisi

Mixing & Demixing

Per incrementare l'anonimato nascono i **Bitcoin Mixer**.

Rendono più complesso il tracciamento dei flussi sulla blockchain.

Molti di questi sono attivi sulla darknet.

Non esistono stime esaustive dell'utilizzo di questi servizi.

Mixer centralizzati (1)

L'utente versa dei fondi su un indirizzo del mixer, specificando gli indirizzi di restituzione e le tempistiche.

Il mixer aggrega e mischia i fondi ricevuti da più utenti (*Anonymity Set*).

Vengono restituiti i fondi "puliti" agli indirizzi specificati in precedenza (il mixer trattiene una fee 1-3%).

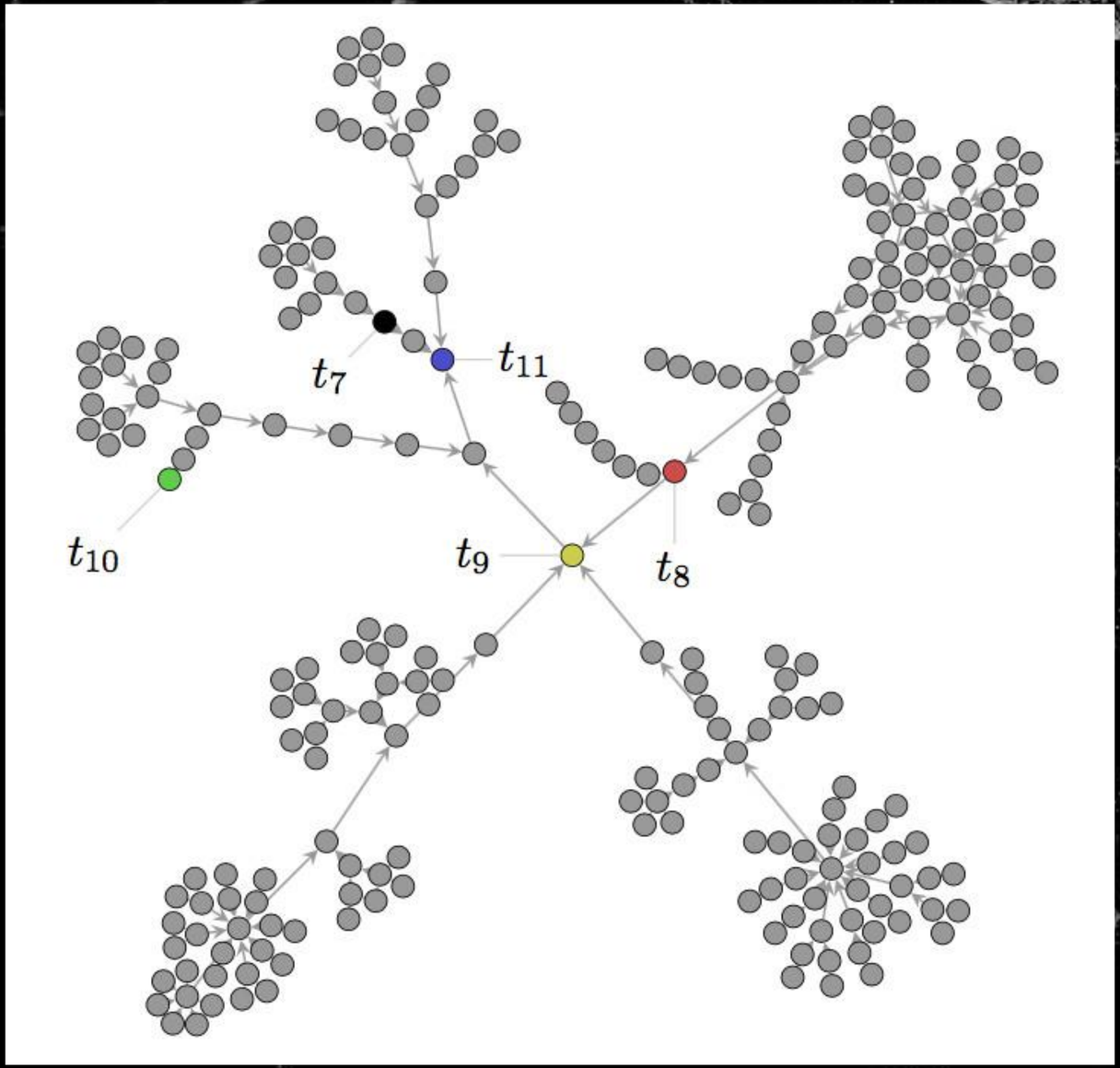
Mixer centralizzati (2)

BitcoinFog

BitLaundry

HelixMixer

etc.



Schema transazioni BitLaundry

Svantaggi dei Mixer centralizzati (1)

Se ci sono pochi fondi è possibile che all'utente torni indietro parte dei suoi stessi fondi.

Tool di analisi:
blokchain.info :: taint analysis

Svantaggi dei Mixer centralizzati (2)

Si deve avere totale fiducia nel gestore del servizio:

Conosce sorgente e destinazione di tutti i fondi che transitano.

Ha l'effettivo controllo dei soldi (potrebbe non restituirli).

Molti dei mixer sono in realtà *scam*!

btcmixers.com contiene "recensioni" di mixer con affidabilità, *taint* riscontrato, etc.

Per un’analisi più approfondita

"An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem" (M. Moser, R. Bohme, D. Breuker)

Per far fronte a queste problematiche nascono i sistemi di ***Mixing trustless & distributed***.

Nessuna entità centrale.

Struttura *peer-to-peer*.

Robustezza garantita dalla “matematica”.

…ma non esenti da vulnerabilità.

Per un’analisi più approfondita

http://www.coinjoinsudoku.com

http://www.neutrino.nu/single-post/2016/11/28/JoinMarket-a-distributed-and-trustless-mixing-system

Ambiti di utilizzo

Law Enforcement

Alcuni esempi (1)

Individuare gli utenti che effettuano acquisti sui *marketplace* della *darknet*.

Identificare il wallet di un marketplace (***clustering + OSINT***)

Identificare i wallet che inviano bitcoin al marketplace (***clustering***)

Ottenere informazioni sull'identità dei proprietari dei wallet identificati (***OSINT***)

Alcuni esempi (2)

Individuare gli autori di un *ransomware*.

Identificare le transazioni che rispecchiano lo schema di pagamento (***pattern analysis***)

Localizzare l’origine geografica delle transazioni spendenti (***geotracking***)

Ambiti di utilizzo

Normativo & Regolatorio

Risk scoring per AML e KYC

Ha inviato o ricevuto soldi da fonti ritenute sospette?

Ha utilizzato sistemi di anonimizzazione del traffico o di *bitcoin mixing*?

Ha effettuato transazioni da nazioni ritenute sospette?

E' collegato a dei pattern/flussi che possono essere assimilabili ad attività illecite?

Lo stato dell’arte

Ci sono piattaforme commerciali che mettono insieme le tecniche qui descritte (ed altre) per offrire servizi a 360°.

Q & A