2018-05-08

Digitala valutor, forensik och teknik

SECTRA

Knowledge and passion

Jonathan Jogenfors

- Forskningschef, Sectra Communications AB
- Teknologie Doktor, LiU 2017
- Postdoktortjänst vid LiU, forskar på informationssäkerhet och blockkedje-teknik samt undervisar i dessa ämnen
- Har i flera år assisterat Polisen, Tullen, EBM m.fl. med frågor om digitala valutor

Kryptografi och säkerhet

- Säkra mobiltelefoner upp till SECRET-nivån
- Krypto upp till TOP SECRET
- Övervakning av kritisk infrastruktur

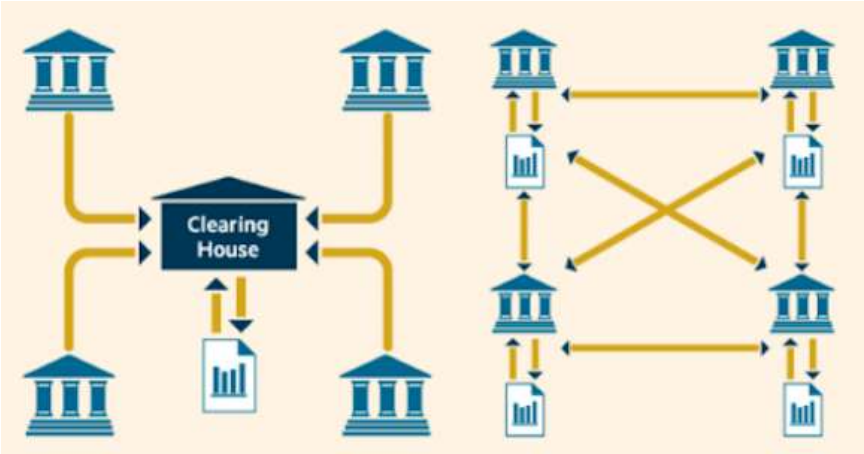
SECTRA
Knowledge and passion

Agenda

- Allmänt om Bitcoin och blockkedjan
- Metoder för att spåra transaktioner
- Ransomware
- Aktuella fall
- Nya kryptovalutor som förhindrar spårning
- Utblick

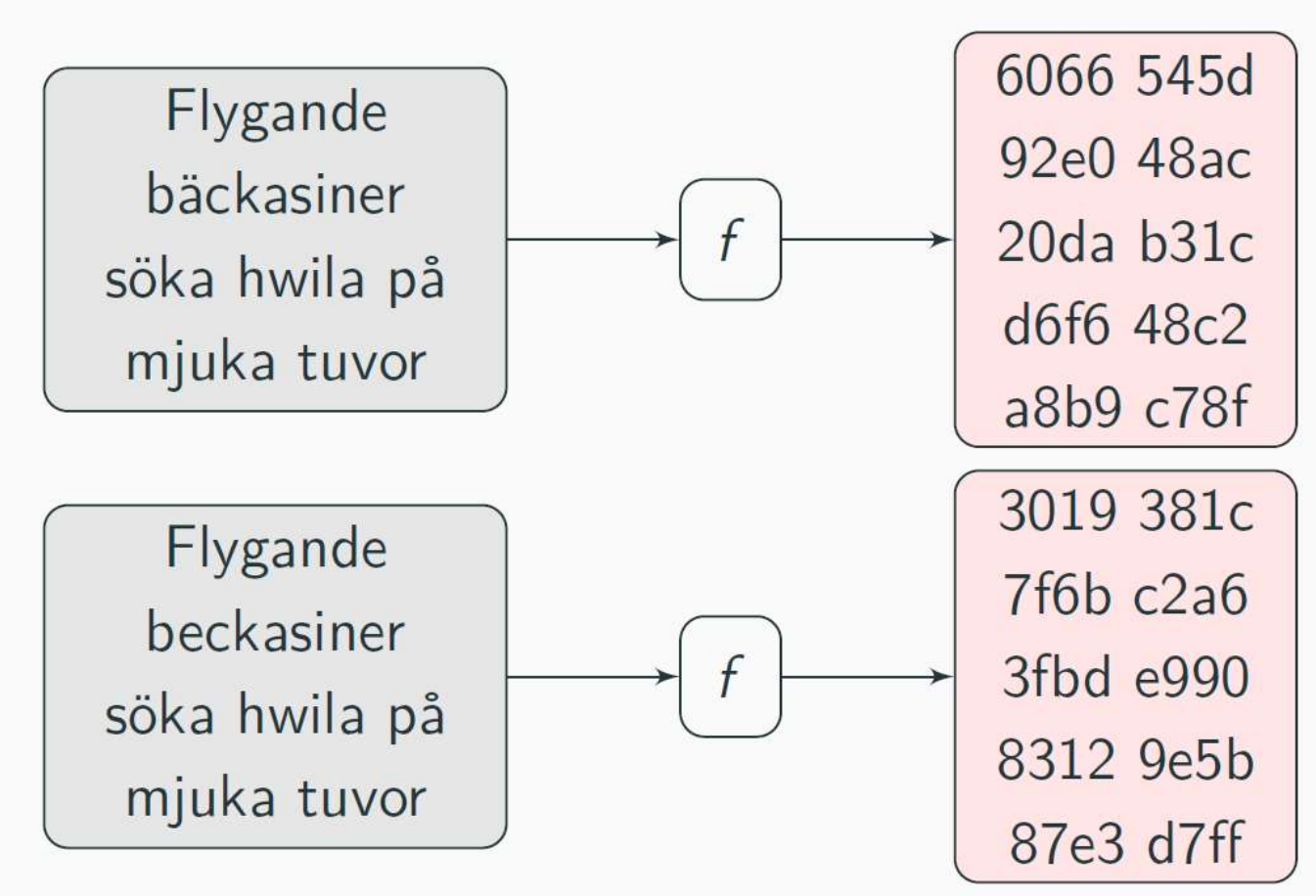
Hur fungerar Bitcoin?

- Transaktioner sparas i en lista
- Saldot bestäms av summan av transaktioner
- Nya transaktioner läggs till på slutet
- Listan växer hela tiden, ingenting tas bort

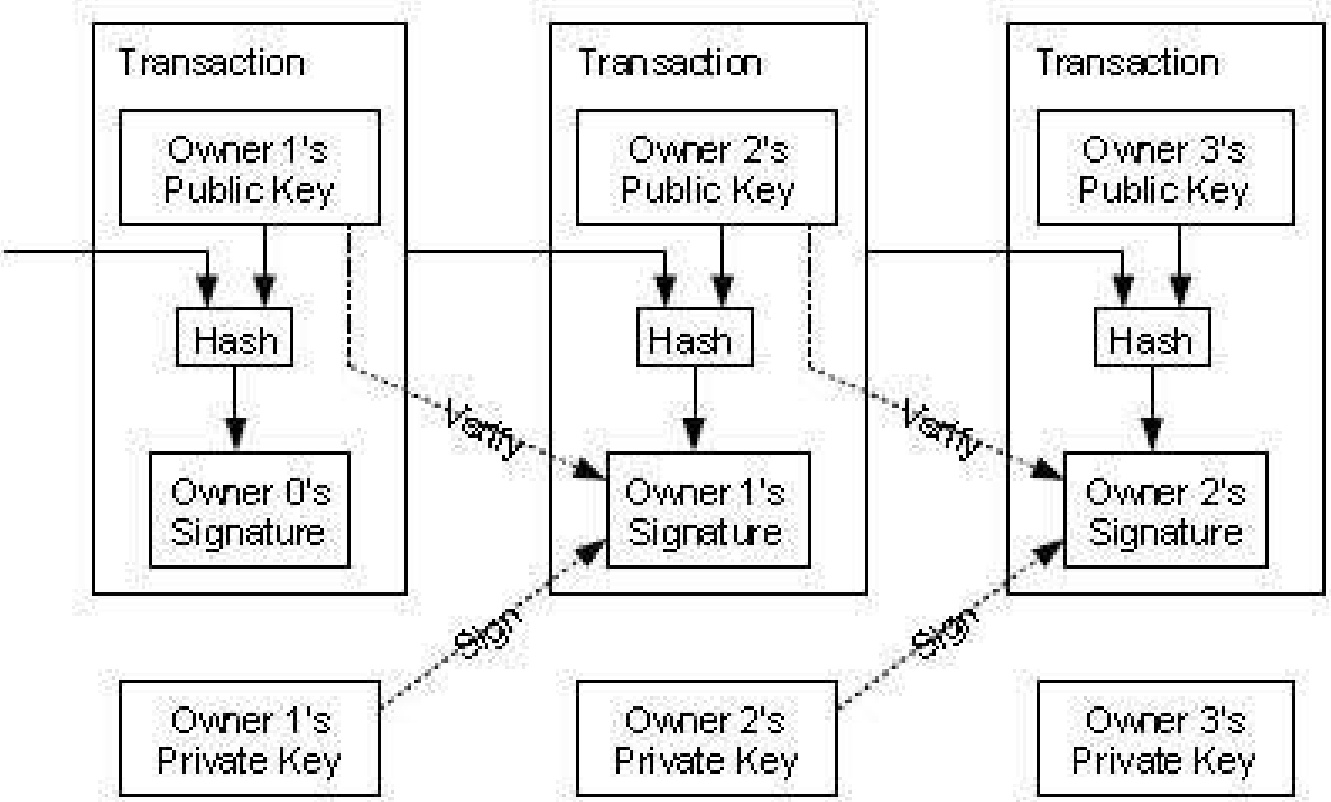


SECTRA
Knowledge and passion

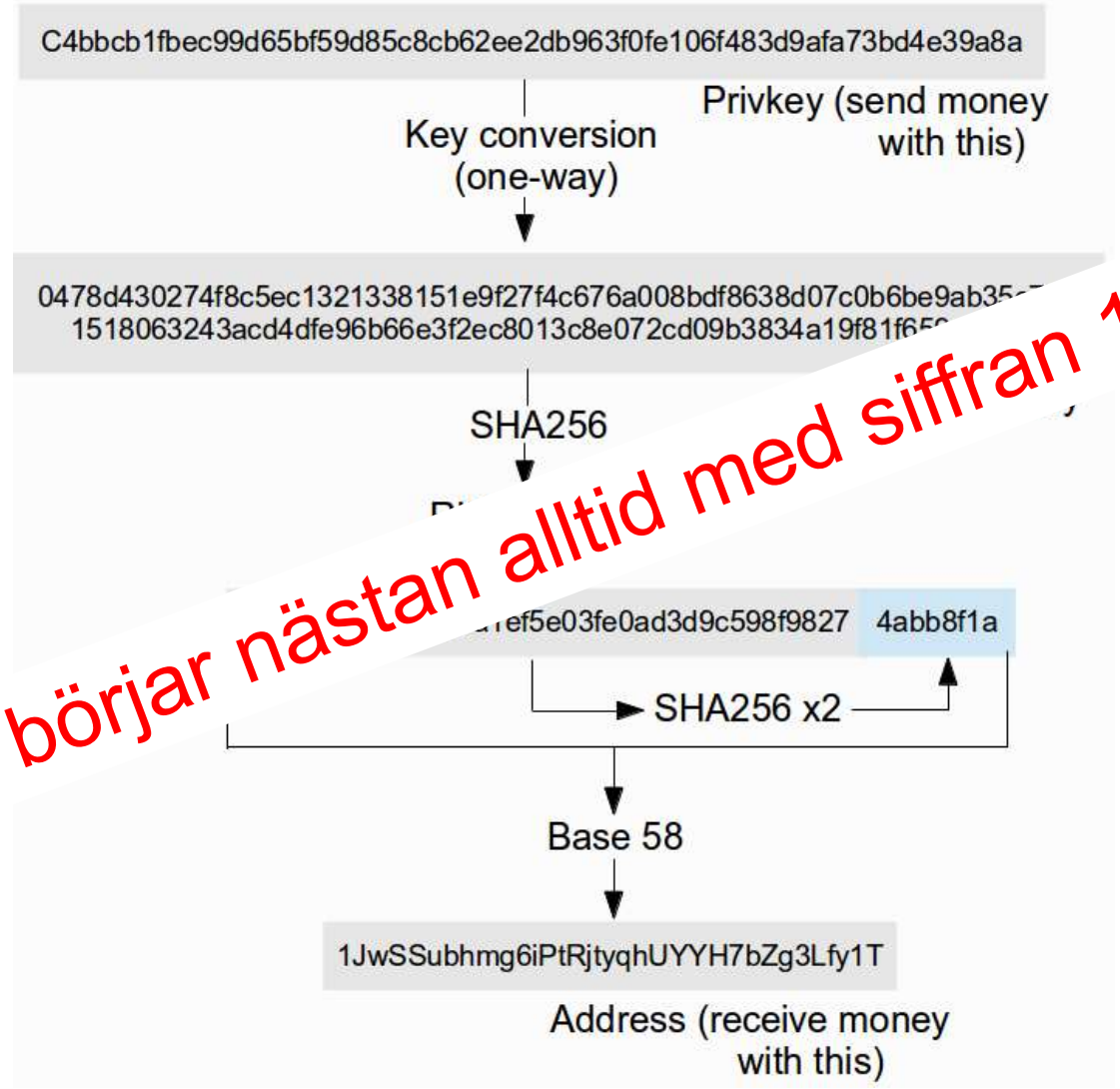
Hashfunktioner: Små ändringar syns fort



Bitcoin använder en blockkedja



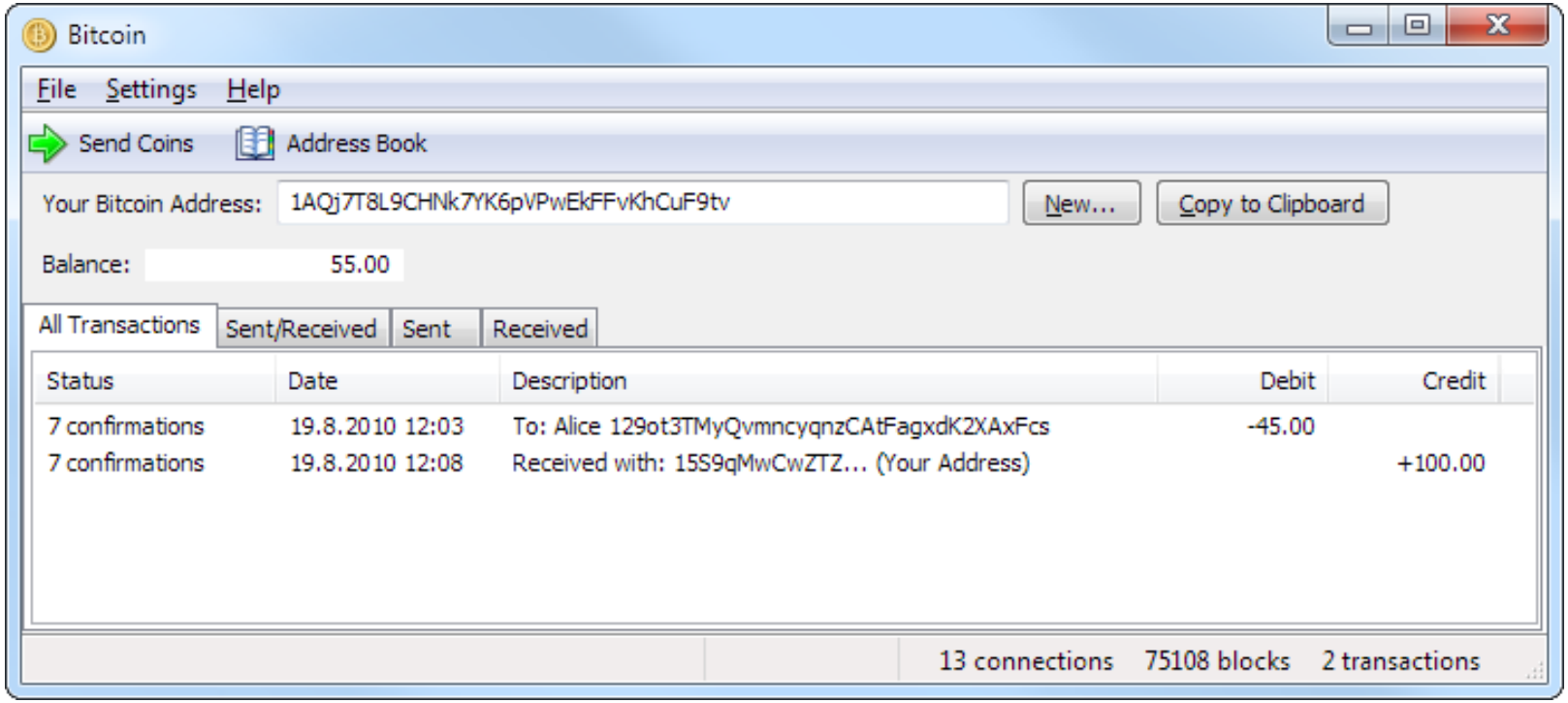
Bitcoin använder kryptografi



Adresser börjar nästan alltid med siffran 1 eller 3

SECTRA
Knowledge and passion

Kontot sköts av ett plånboksprogram



SECTRA
Knowledge and passion

2013: Bitcoin-skylt syntes på ESPN

Denna skylt gav 24000 USD

Mer om adresser

- Det finns 2^{160} möjliga adresser, det (minst sagt) räcker och blir över
- Nya adresser genereras lokalt i plånboken
- En plånbok har alltså många mottagar-adresser!

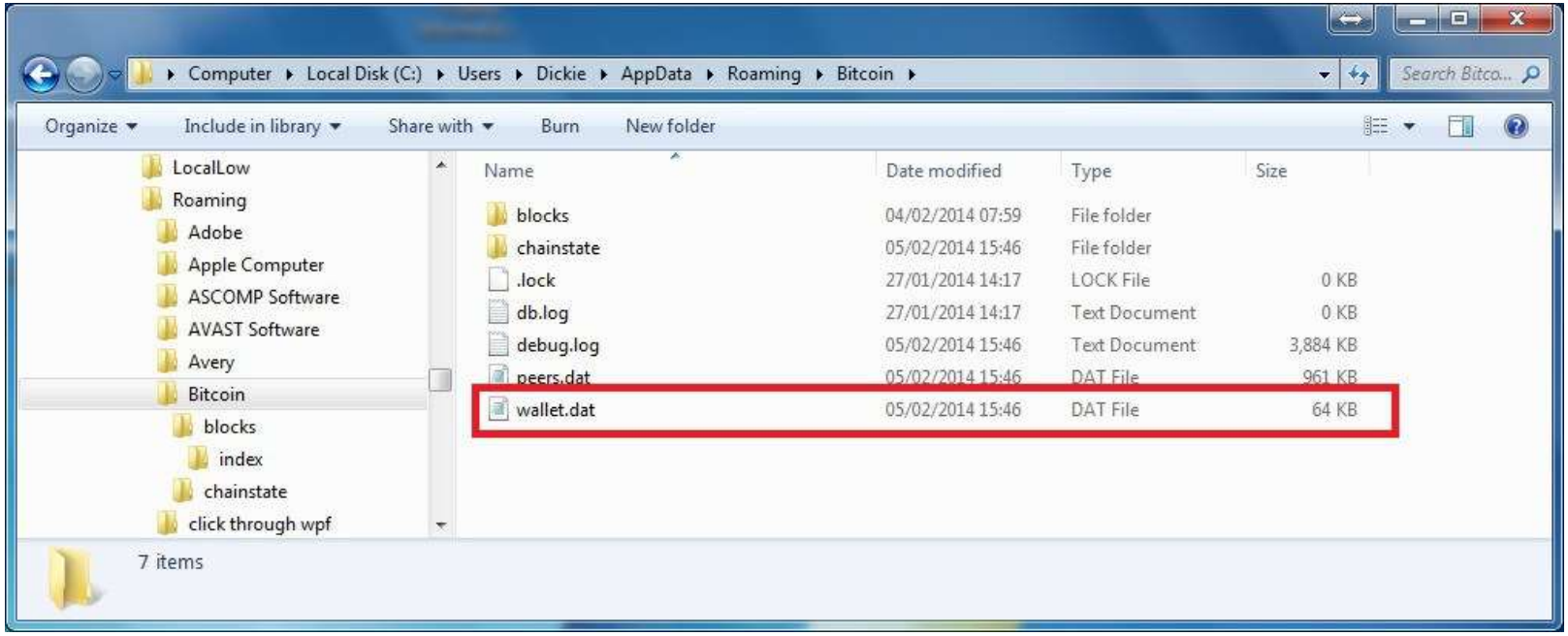
SECTRA
Knowledge and passion

Privata nyckeln styr allt

- Transaktioner initieras när plånboken signerar en transaktion med den privata nyckeln.
- Om nyckeln läcker blir man av med pengar
- Därför vanligt att nyckeln lagras offline, på papper eller i en betrodd hårdvaru-plånbok

SECTRA
Knowledge and passion

Plånboksfilen är #1 vid tillslag



SECTRA
Knowledge and passion

Växelkursen är mycket volatil

SECTRA
Knowledge and passion

Bitcoin-forensik

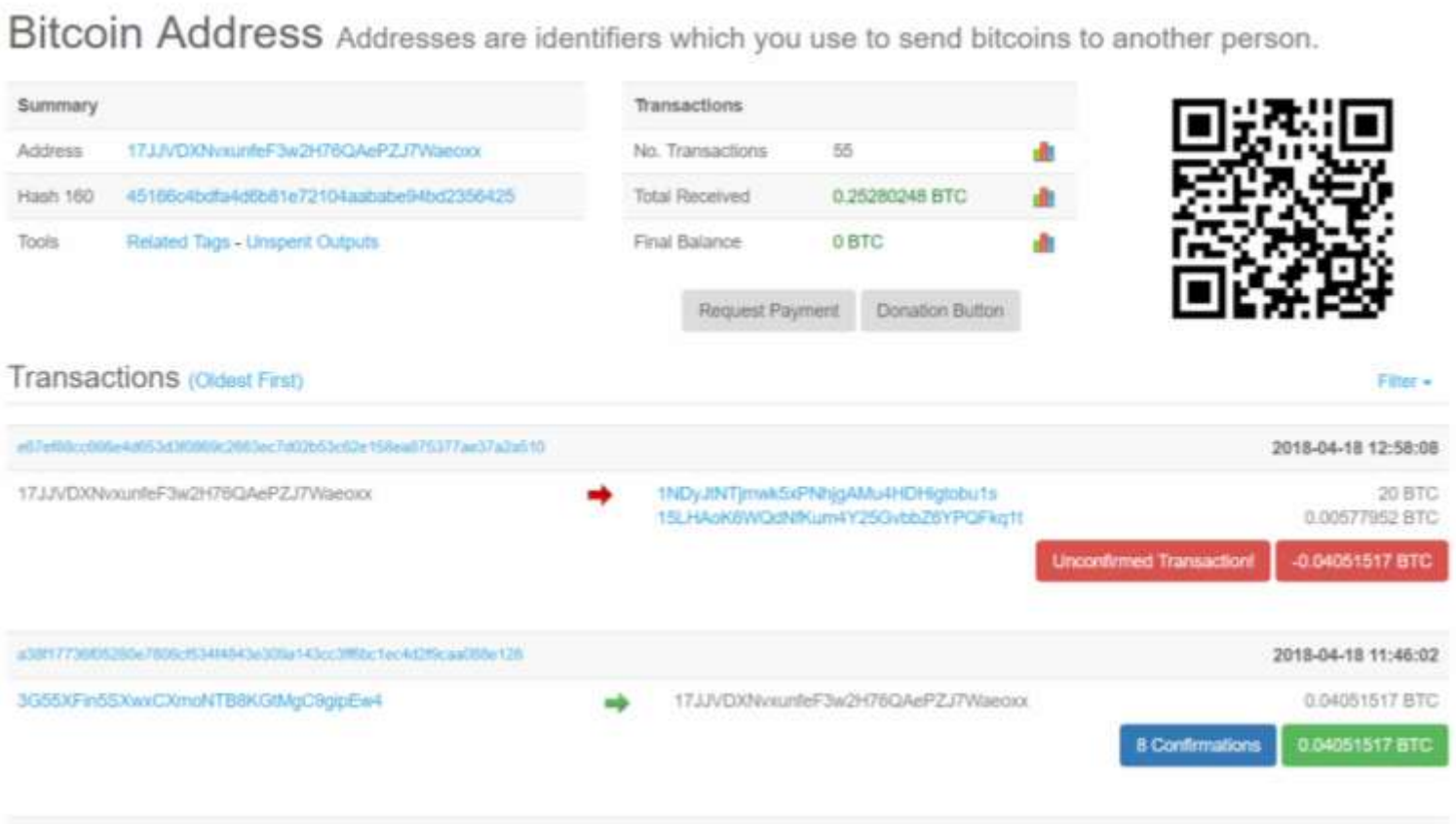
- Spåra och identifiera personer och organisationer från blockkedjan
- Spåra illegal handel till och från markadsplatser och verkliga personer
- Assistera och samla bevis för tillslag och förverkan
- Samla bevis för rättegångar

Hur spåras Bitcoin?

- Metoder
  - Gruppning/taggning/klustring
  - Växeladresser
  - Beteendemönster
  - Enter/Exit-punkter
  - Korrelering mot publik info
- Verktyg
  - blockchain.info
  - Wallet Explorer
  - Chainalysis
  - Excel, egna verktyg

blockchain.info

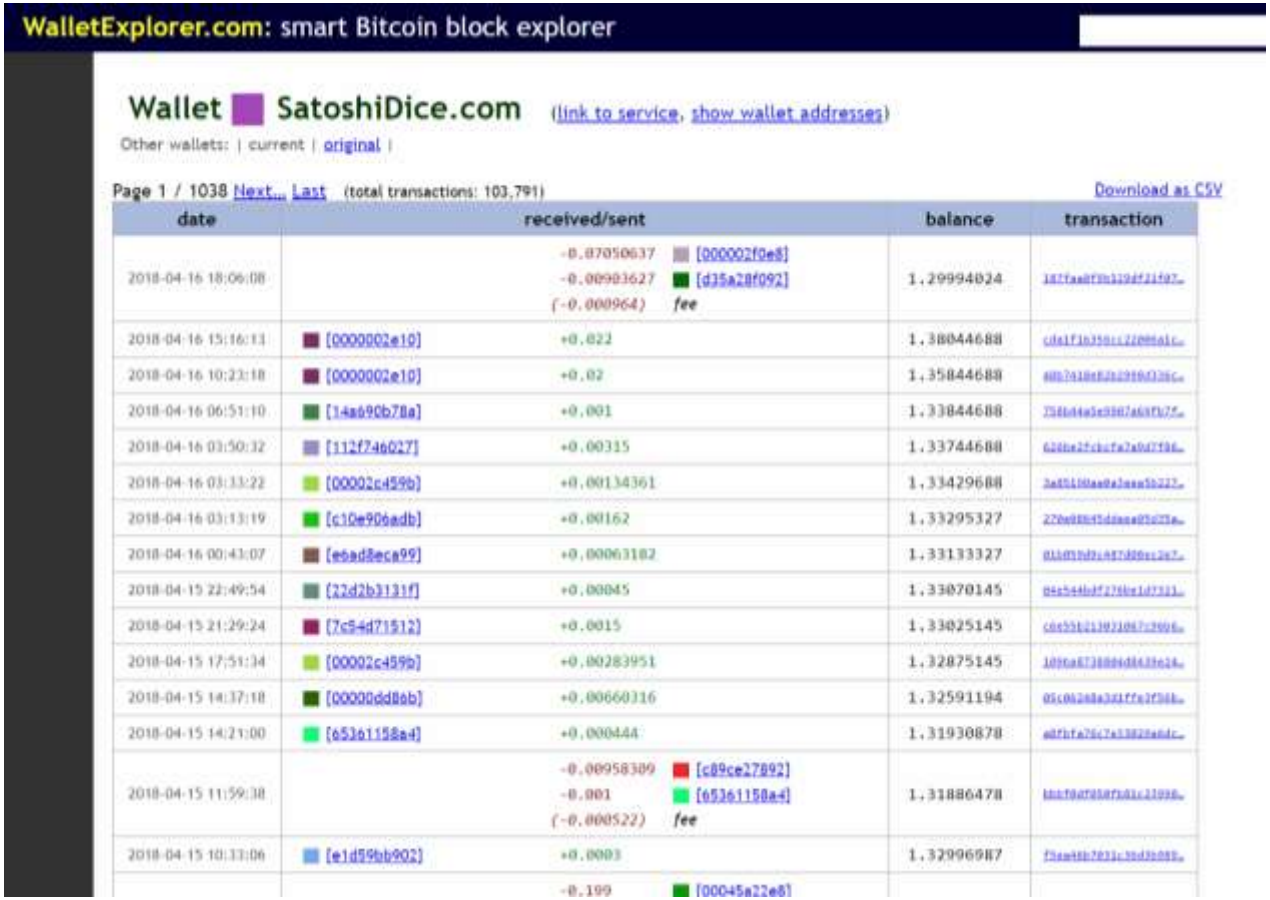
Se transaktioner, nästan i råformat



SECTRA
Knowledge and passion

Wallet Explorer

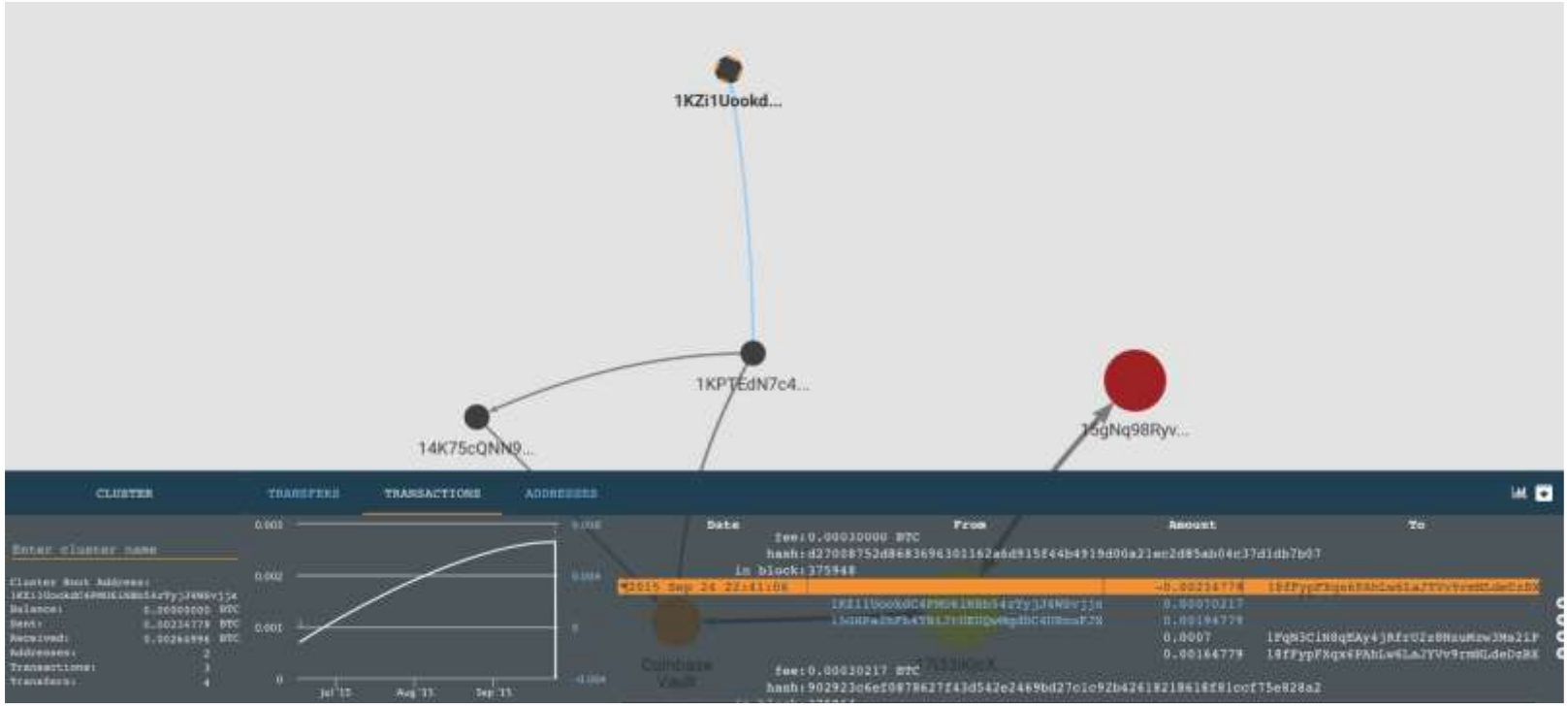
Klustring av plånböcker



SECTRA
Knowledge and passion

Chainalysis

Kommersiellt program för forensik

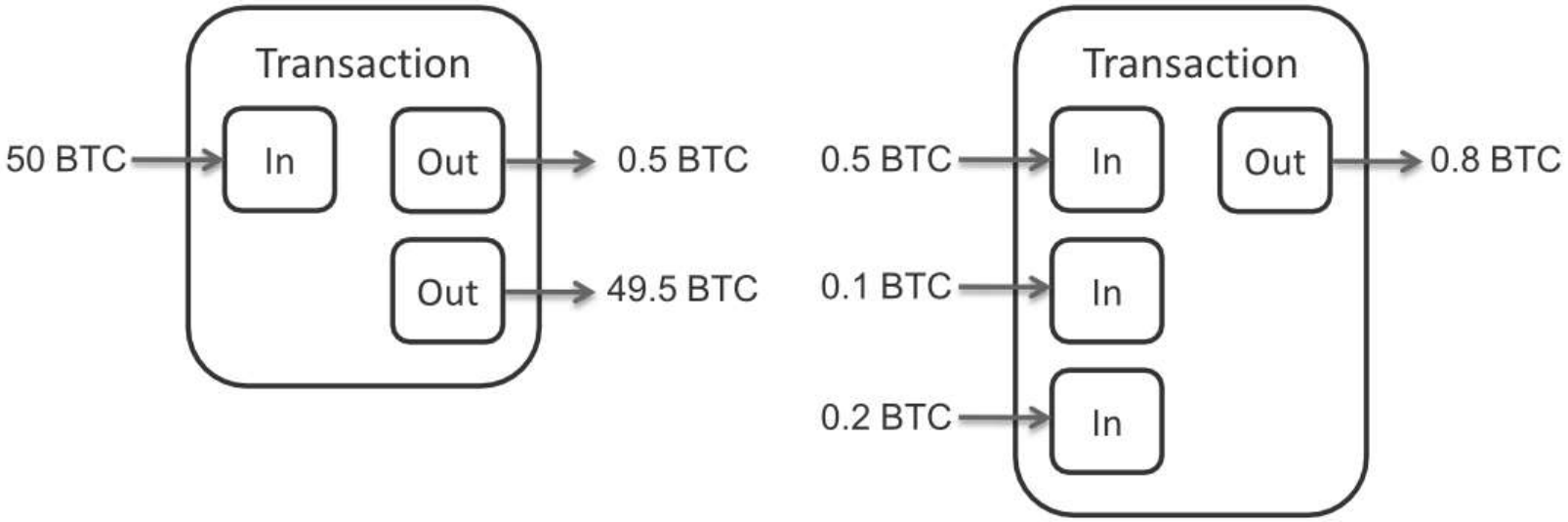


SECTRA
Knowledge and passion

Ett sätt att gruppera transaktioner

- Input-klustring
- Växel-klustring
- Datainsamling
- Aktiv spårning
- Exit-noder

Input- och outputadresser



Alla inputs måste förbrukas!

Input-klustring

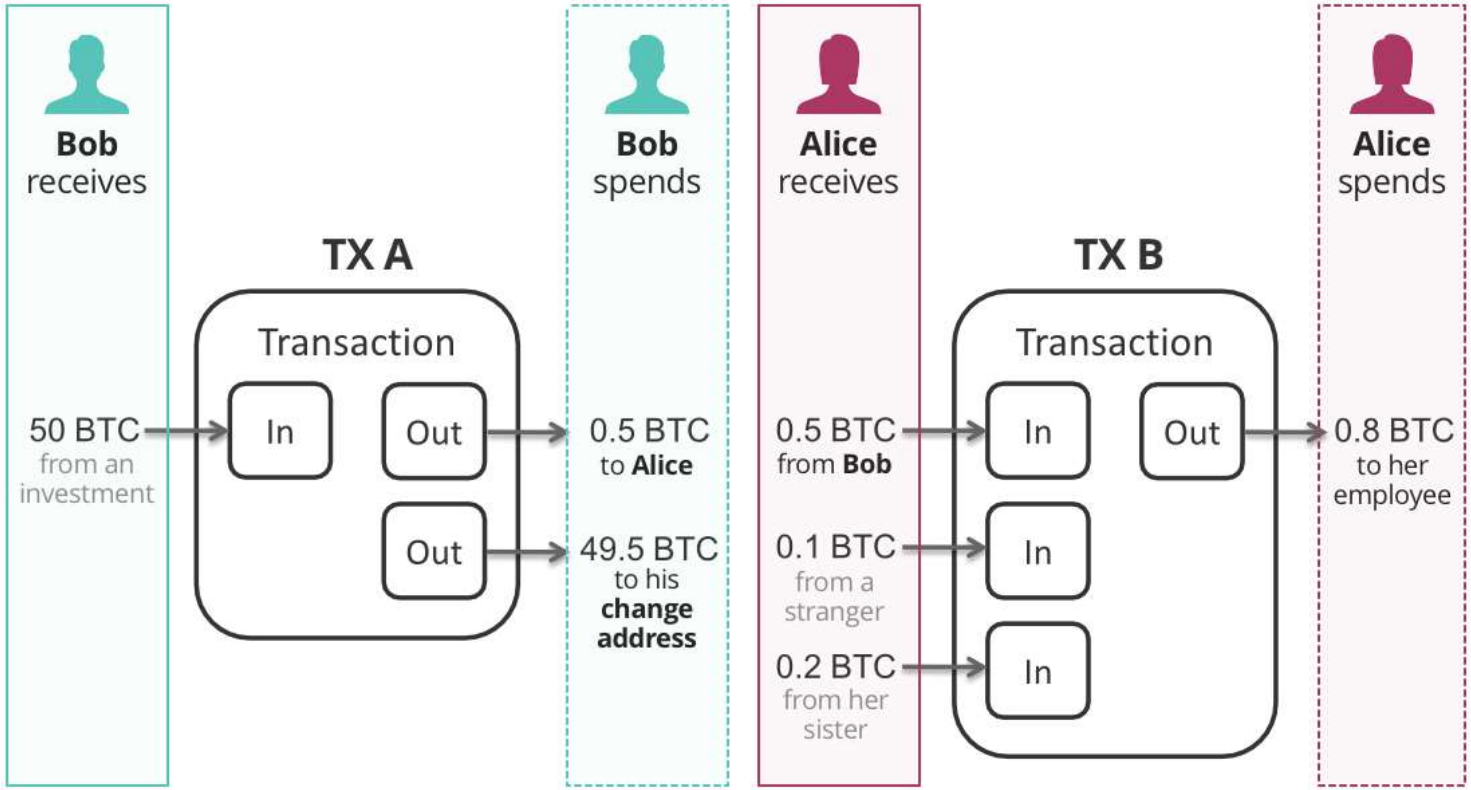
En användare styr dessa addresser!

SECTRA
Knowledge and passion

Input-klustring: Tillräckligt?

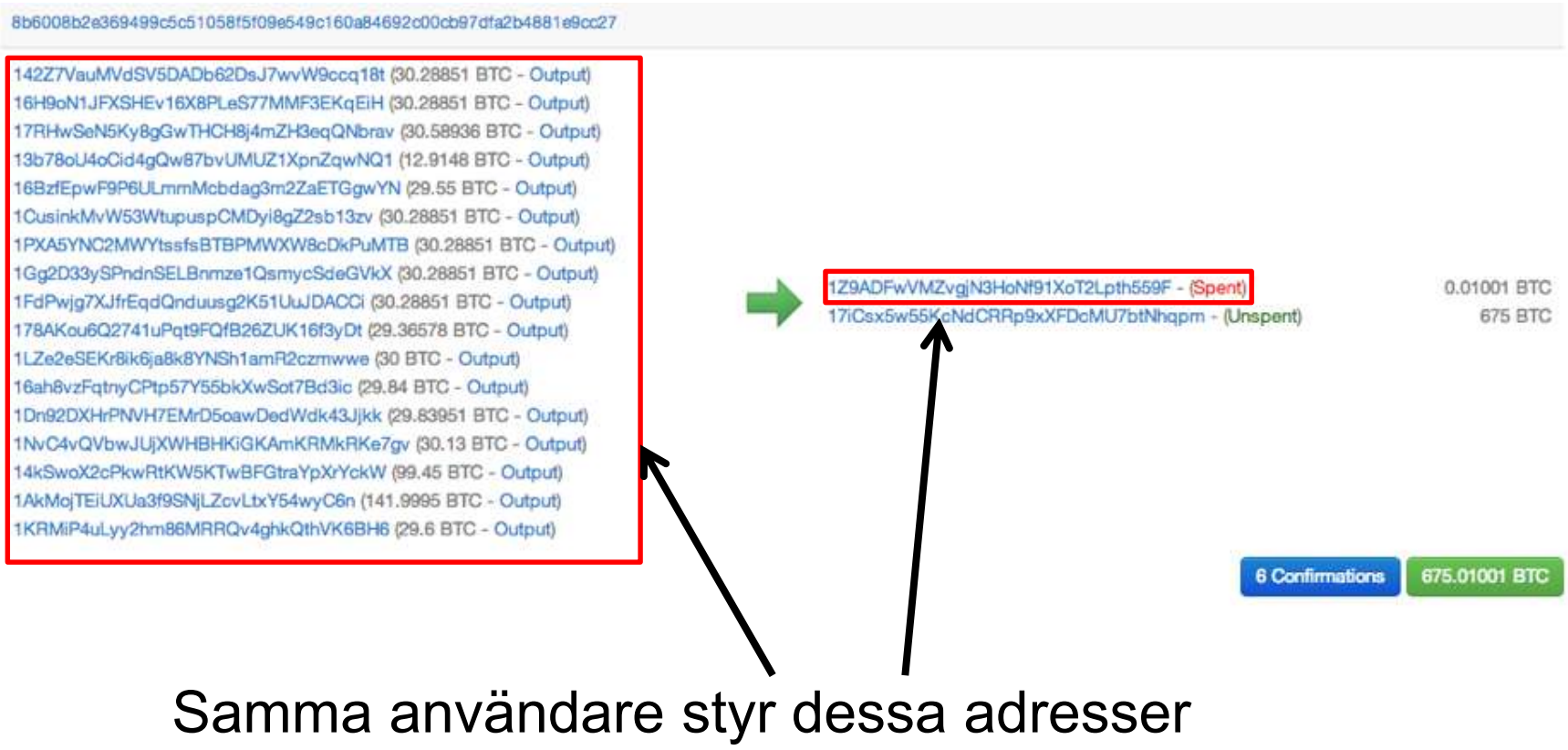
- Detta fungerar eftersom avsändaren måste kontrollera den privata nyckeln
- En etablerad metod som även bekräftats av Bitcoin-skaparen själv.
- Inga false positives!
- Men fångar inte allt

Växel måste hanteras



SECTRA
Knowledge and passion

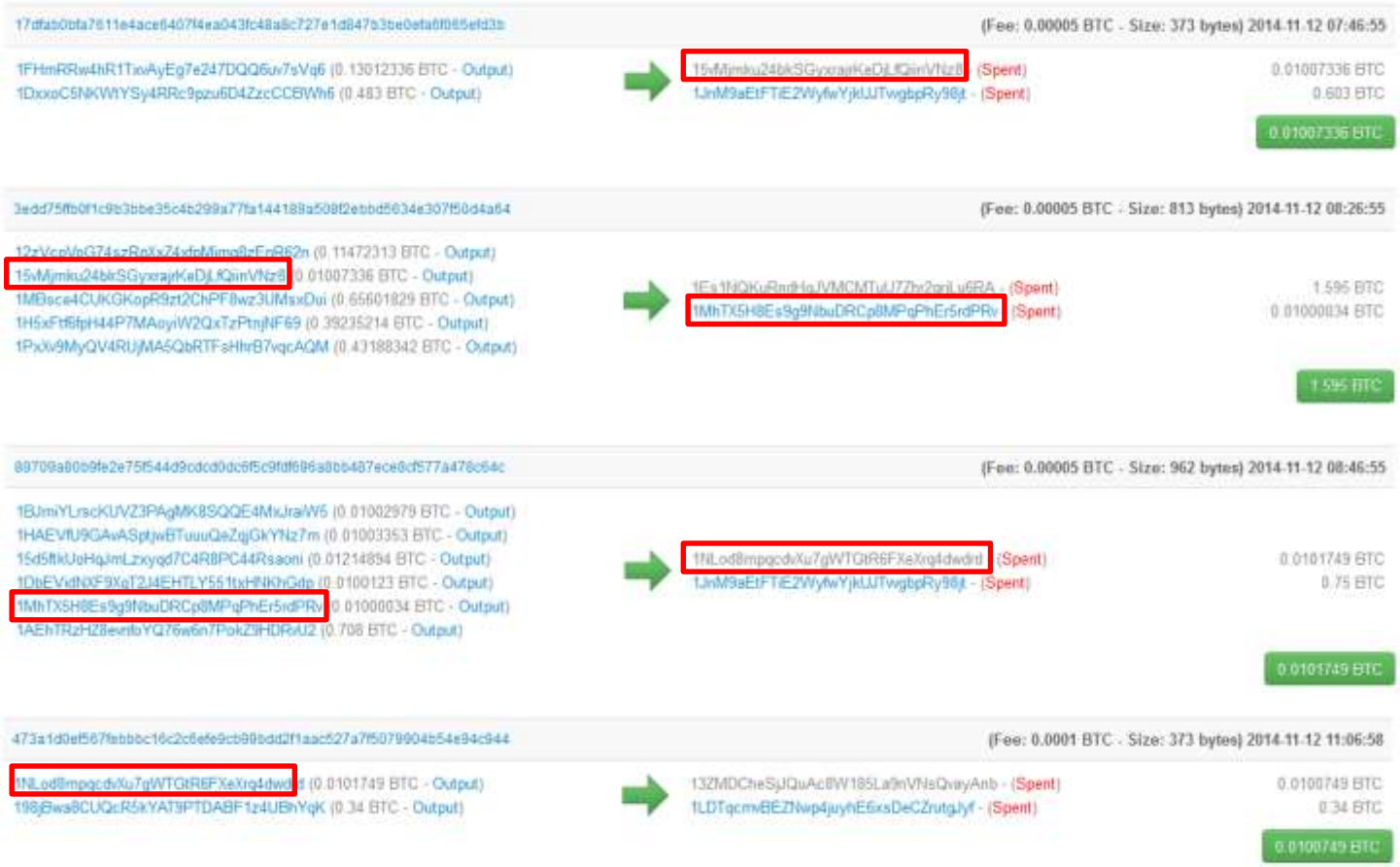
Växel-klustring



Samma användare styr dessa adresser

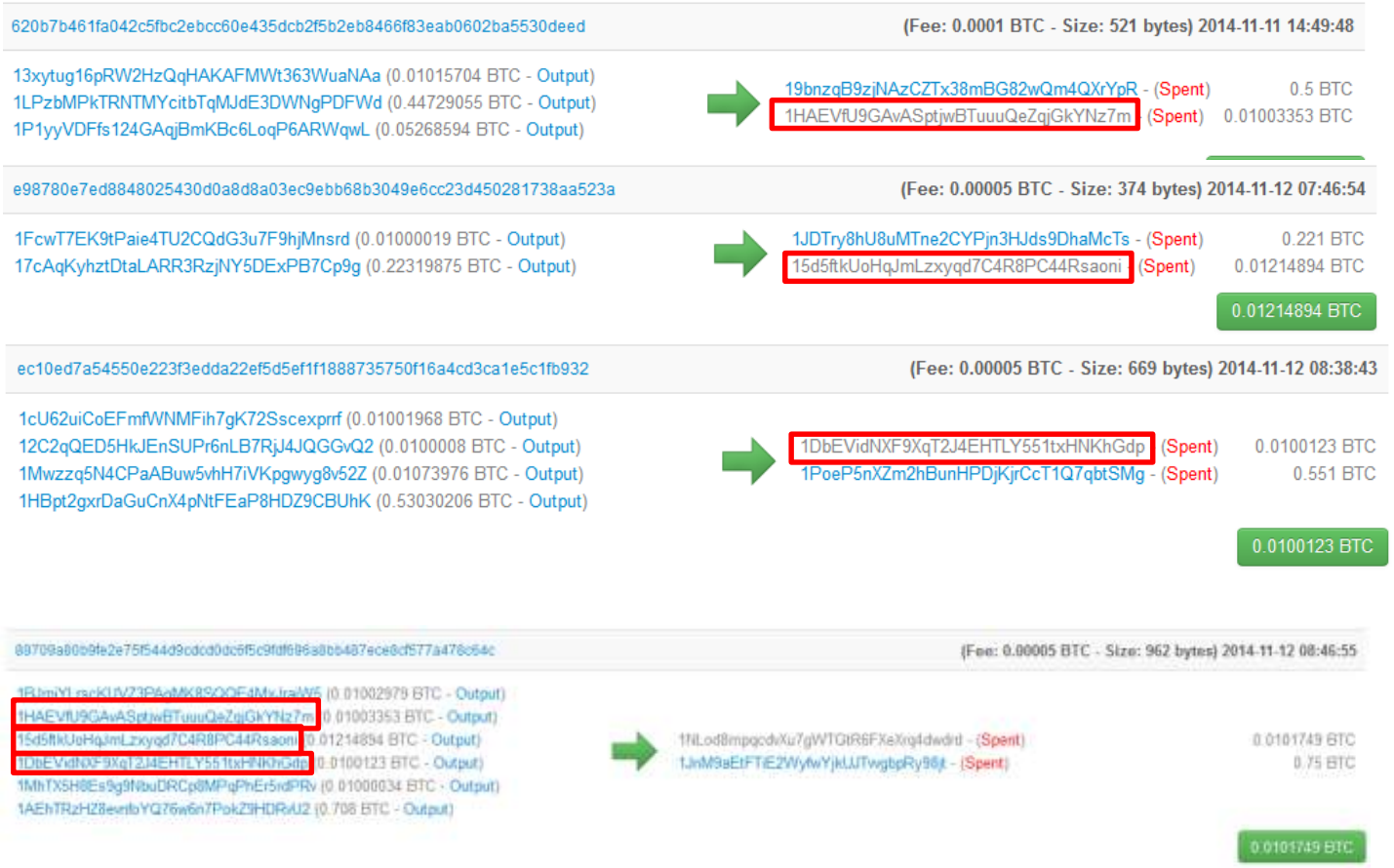
SECTRA
Knowledge and passion

Det går att följa växelpengar



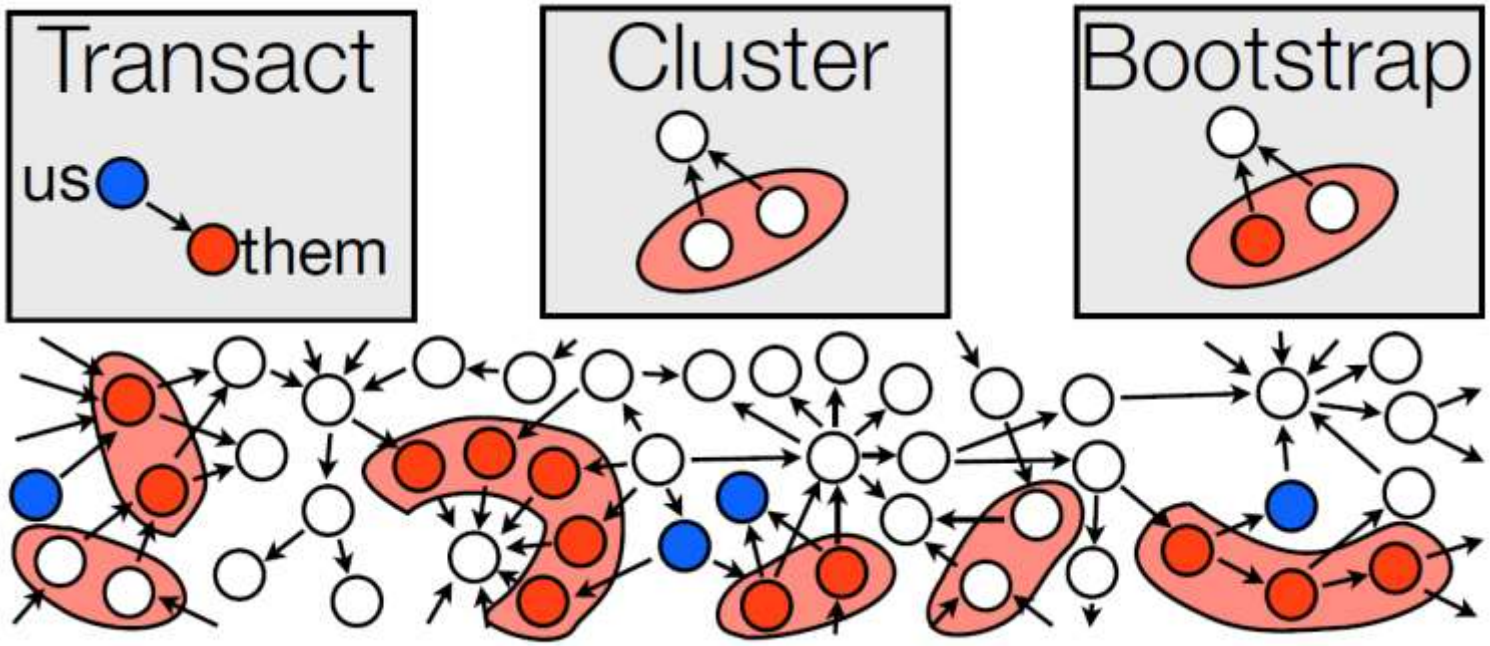
SECTRA
Knowledge and passion

Avancerad växel-klustring



SECTRA
Knowledge and passion

Klustring grupperar adresser



Meikelejohn et al. (2013) spårade 1.3M publika nycklar

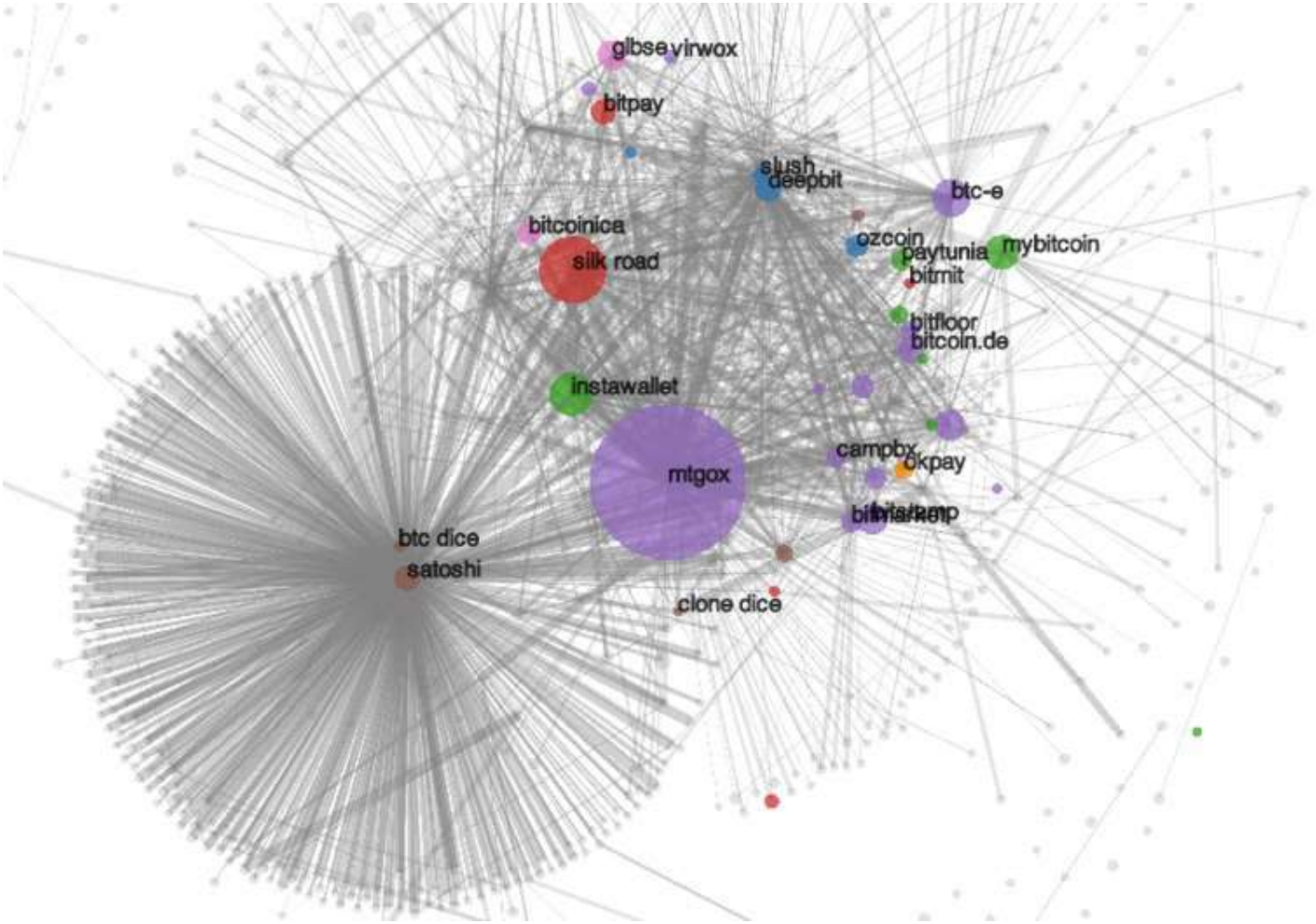
Kluster ska sedan namnges

- I nästa steg identifierar vi vem som äger kluster
- En lös tråd låter oss nysta upp hela garnet
- Adresser i forum-signaturer
- Donations-adresser m.m.
- Exit-noder

Aktiv spårning

Idé: Sätta in pengar på någons konto och se om de flyttas vidare

Identifierade kluster



SECTRA
Knowledge and passion

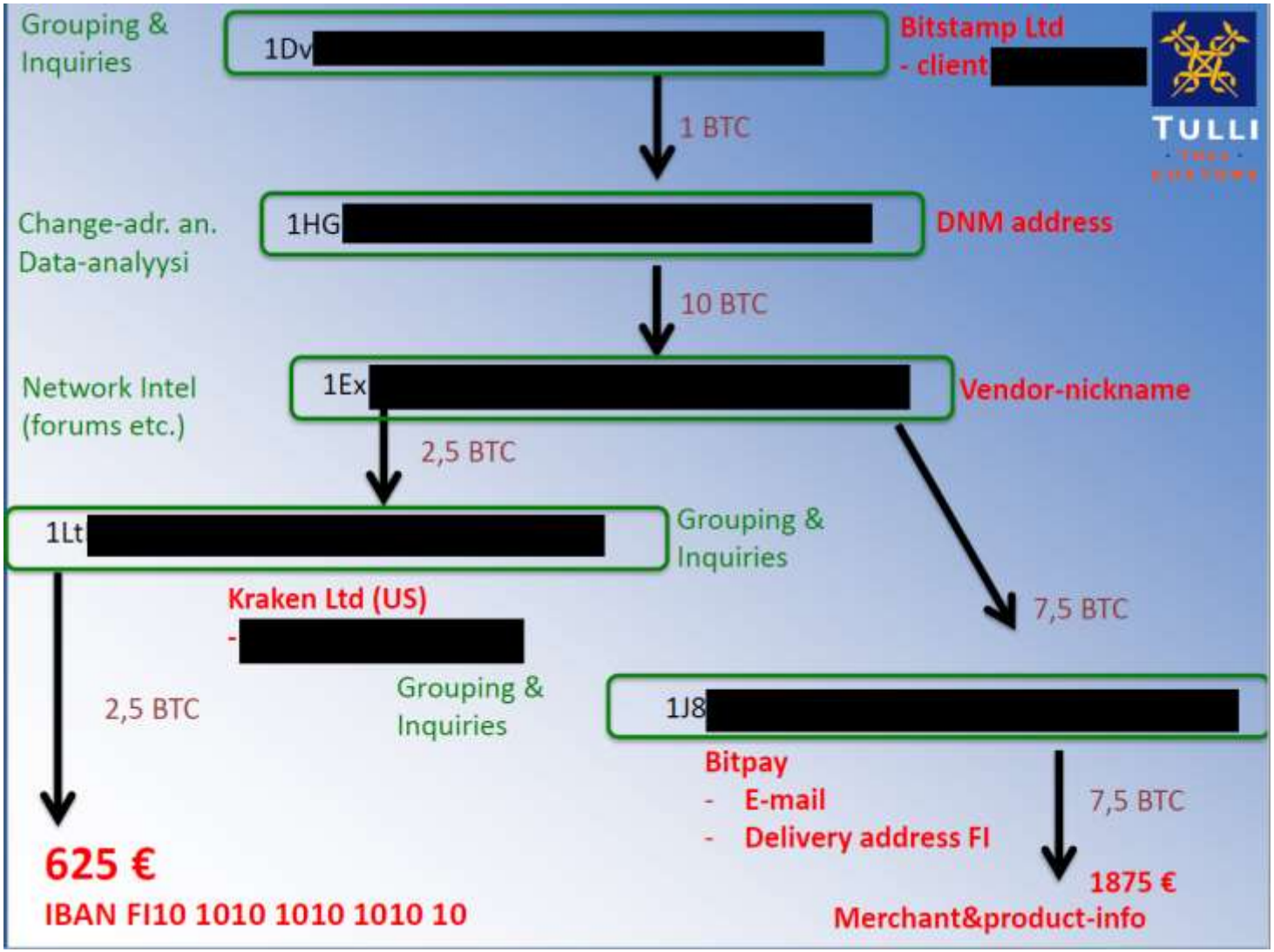
IP-adresser?

- Det hade varit bekvämt att ha IP-adresser från transaktionerna
- Detta sparas dock *inte* i blockkedjan
- Passiv analys kan därför inte se IP-nummer
- Om man däremot aktivt avlyssnar nätverket live är det möjligt
- Detta kräver dock stor arbetsinsats och går inte i efterhand

Enter/Exit-punkter

- En viktig attackpunkt är växlingen till/från fiat-valuta
- Idag är BTC inte användbart utanför Internet
- De flesta växlingskontor kräver att man identifierar sig för att kunna växla
- När ett växlingskontor identifierats i blockkedjan är det därför viktigt att efterfråga denna information
- Tyvärr befinner sig manga växlare i svåra länder

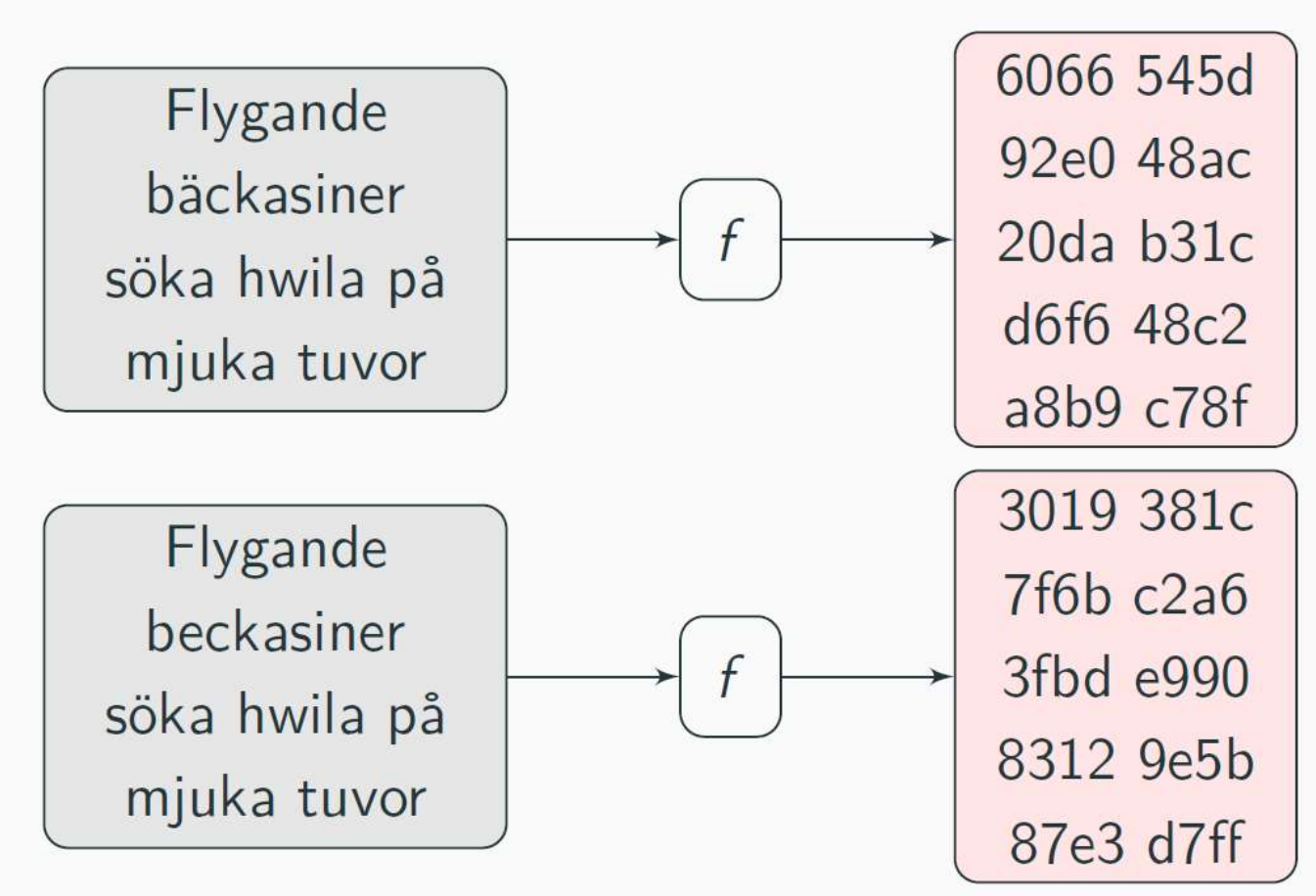
Fallstudie från finska tullen



SECTRA
Knowledge and passion

“Mining”: gräva pengar med datorkraft

Hashfunktioner: Små ändringar syns fort

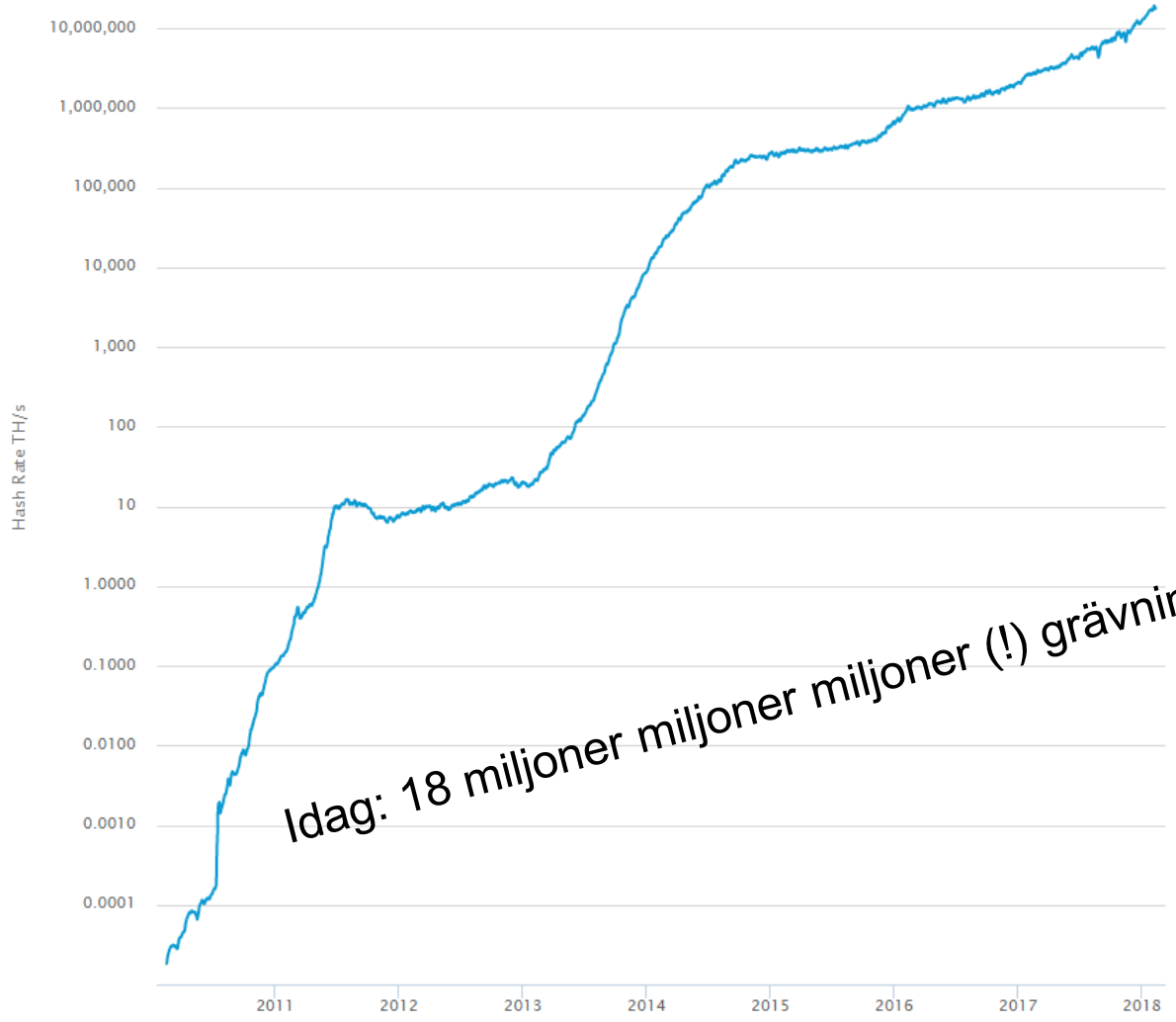


Proof of Work

Meddelande + siffra	Hashvärde
Skicka 100 BTC till Bob0	802dbe2e69…
Skicka 100 BTC till Bob1	Bbfce0d522…
Skicka 100 BTC till Bob2	7bb4db476f…
…	…
Skicka 100 BTC till Bob770239	00000921ac…

ASIC-grävare

Gräva Bitcoin är idag extremt svårt

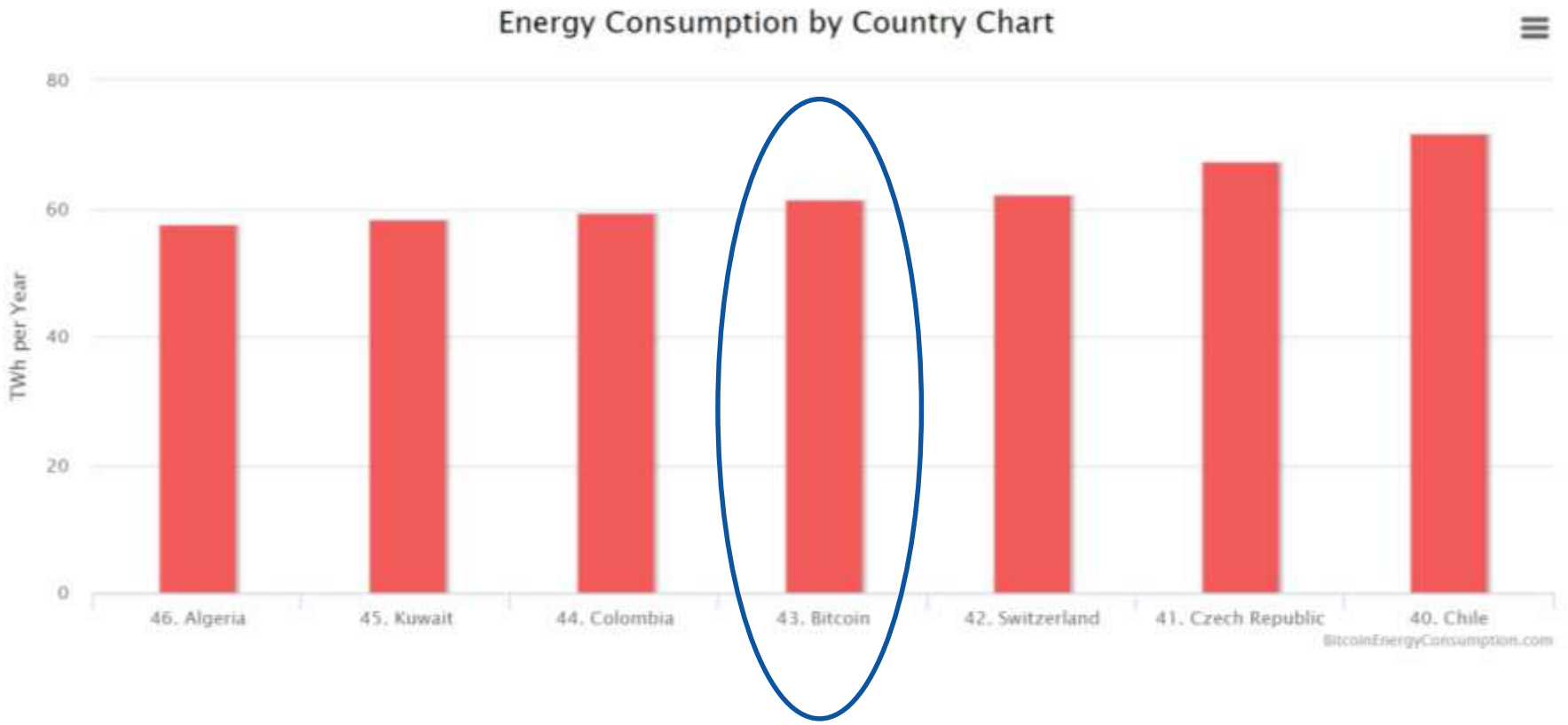


Idag: 18 miljoner miljoner miljoner (!) grävningar per sekund

SECTRA
Knowledge and passion

Inte direkt gröna pengar

Samma strömförbrukning som Schweiz!



SECTRA
Knowledge and passion

Uppgifter

1. Vilka 40 addresser är garanterat relaterade till 1JFaPoWMXz1mV535kEeiPRcdV4m7VaLSeG?
2. Hur många BTC har ”Hi Mom Send Bitcoin” idag? Ungefär hur många SEK är detta?
3. Hur många BTC omsattes i block 124530?
4. Beräkna väntevärdet på energiåtgången för att gräva ett Bitcoin-block idag, givet ett stort antal Antminer S9.

Konflikter inom Bitcoin-communityn

Blockkedjan kan och har delats

Nya kryptovalutor med ny funktionalitet

SECTRA
Knowledge and passion

Forensik i alternativa kryptovalutor

- Alternativa valutor bor i egna blockkedjor
- Forensik-verktyg är överlag fokuserade på Bitcoin
- De alternativa valutorna kräver alltså egna system
- Kan också ha
  - Eget format på adresser
  - Annan funktionalitet (t.ex. smarta kontrakt)
  - Skydd mot spårning (mer om detta senare)

Initial Coin Offering (ICO)

- Blev väldigt populärt under 2017
- En form av crowdfunding där man köper in sig tidigt i en ny kryptovaluta
- De flesta ICO:er är rena pyramidspel utan egentligt värde
- Enligt Cointelegraph drog ICO:er in 6 miljarder USD under 2017

Exit Scams

- Många[illegible]

1. Släng[illegible]
2. Få fo[illegible]värde
3. När [illegible]

- Senast i Apri[illegible]ed 50 miljoner USD

SECTRA
Knowledge and passion

Svårt att värdera små valutor

- Svensk 17-åring stal "Leocoin" mha datorvirus
- Dömdes i februari för bedrägeri av normalgraden
- Villkorlig dom
- Komplikation: Svårt att bestämma värdet av Leocoin
- Sundsvall TR B386-16

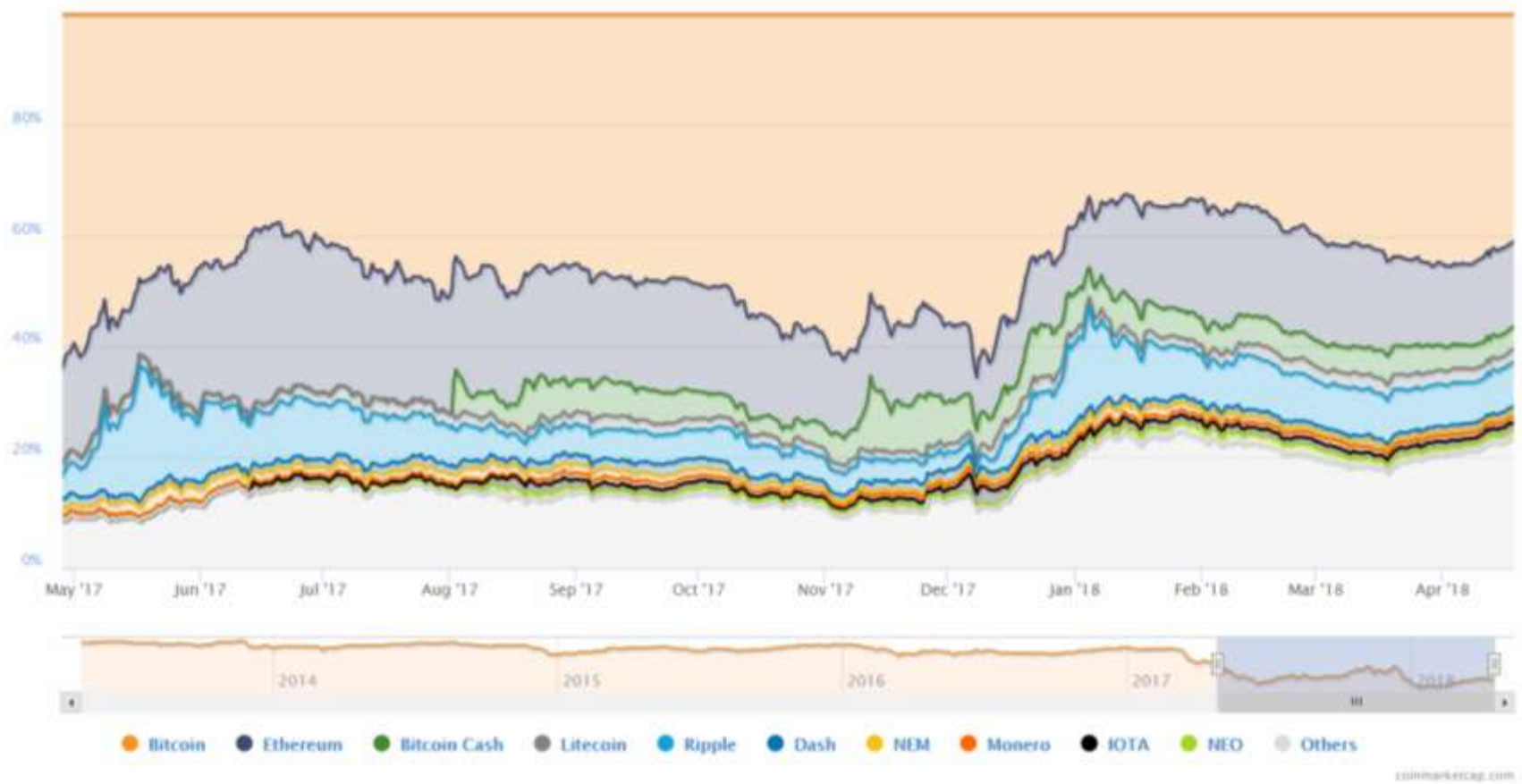
17-åring stal kryptovaluta – döms för bedrägeri

Ett mål gällande stöld av en så kallad kryptovaluta har nu avgjorts i Sundsvalls tingsrätt.

En 17-årig Sundsvallsbo skapade en så kallad "rat" (remote access trojan), ett program som möjliggör fjärrstyrning av andra datorer. Filen lades upp på en fildelningssajt och laddades ner av en annan man.

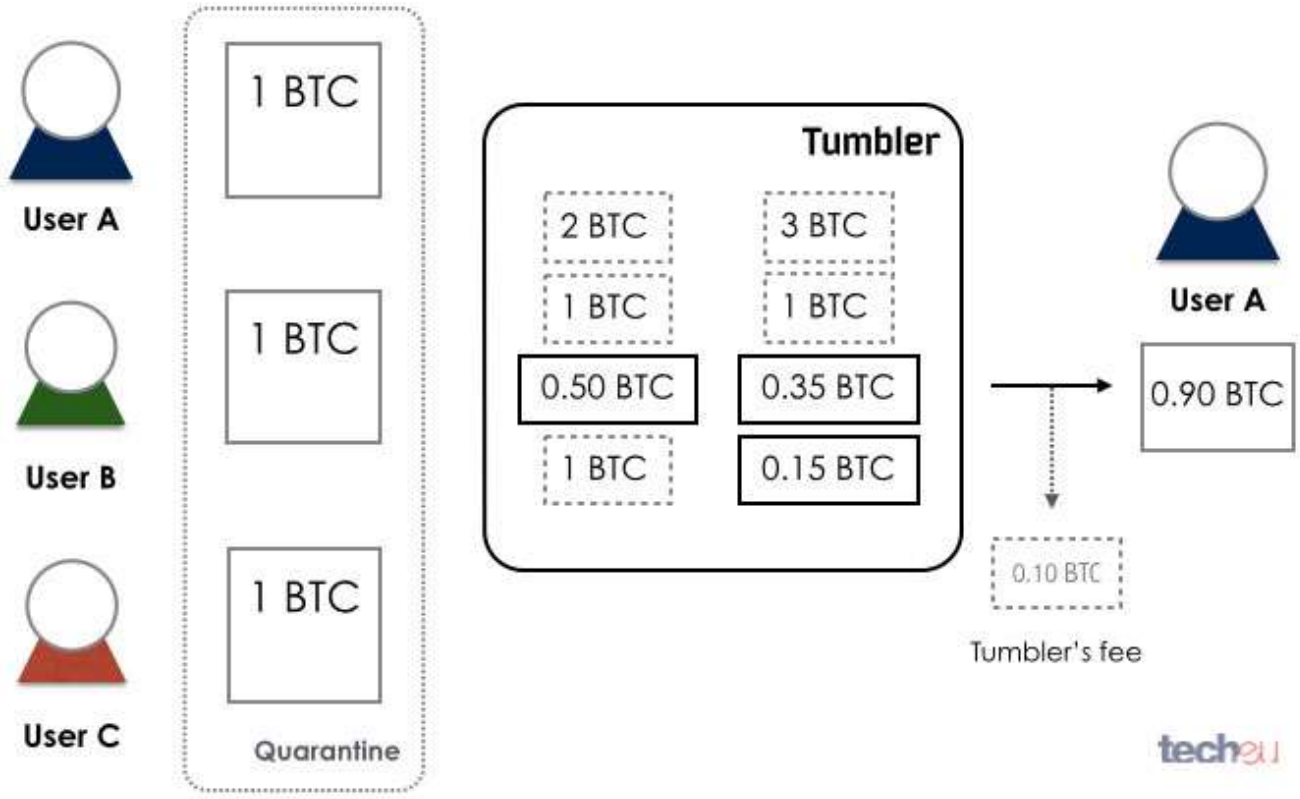
17-åringen kunde nu fjärrstyra mannens dator och använde den möjligheten till att föra över LEOcoins till sin egen dator. LEOcoins är, eller utger sig för att vara,

Bitcoin dominerar, men hur länge till?



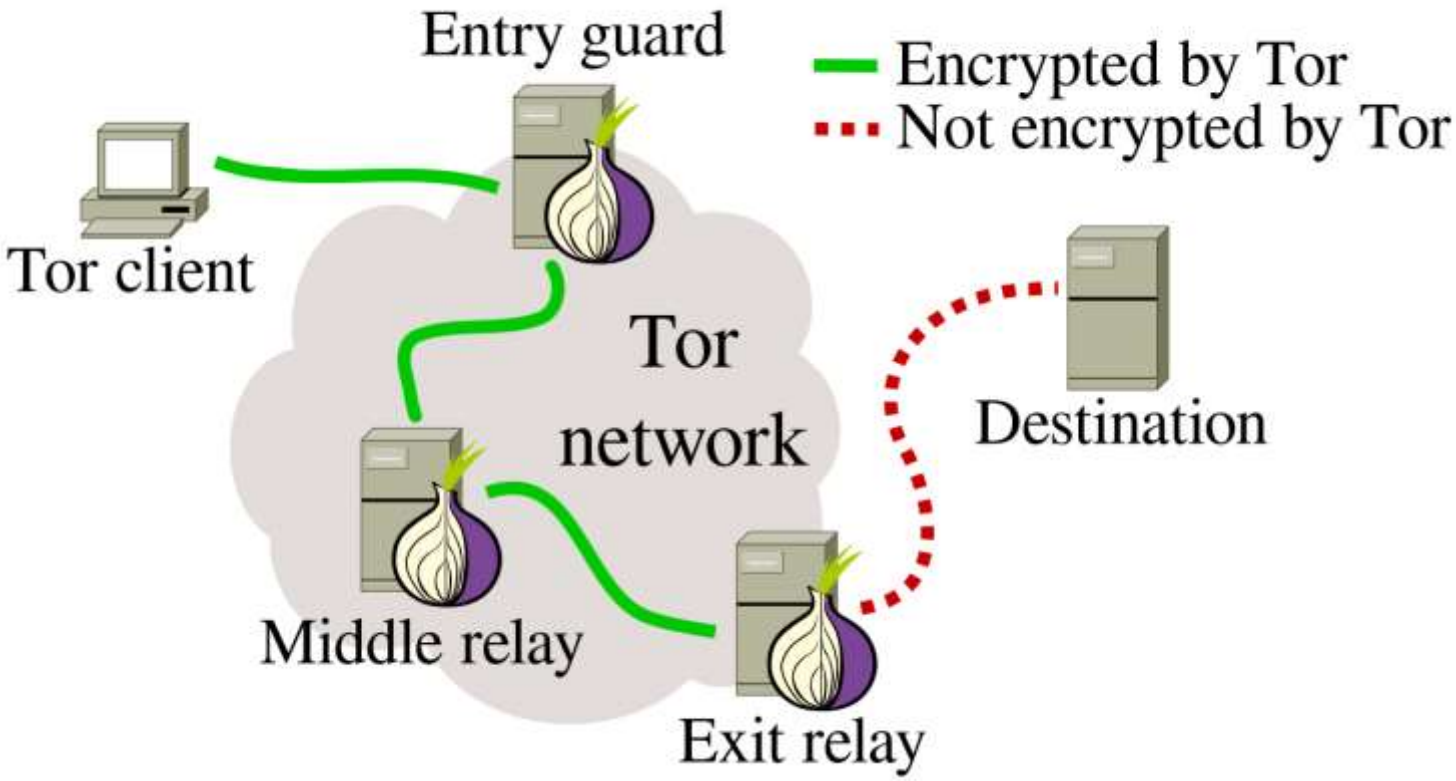
SECTRA
Knowledge and passion

Bitcoin-tumbler: Sopar igen spåren

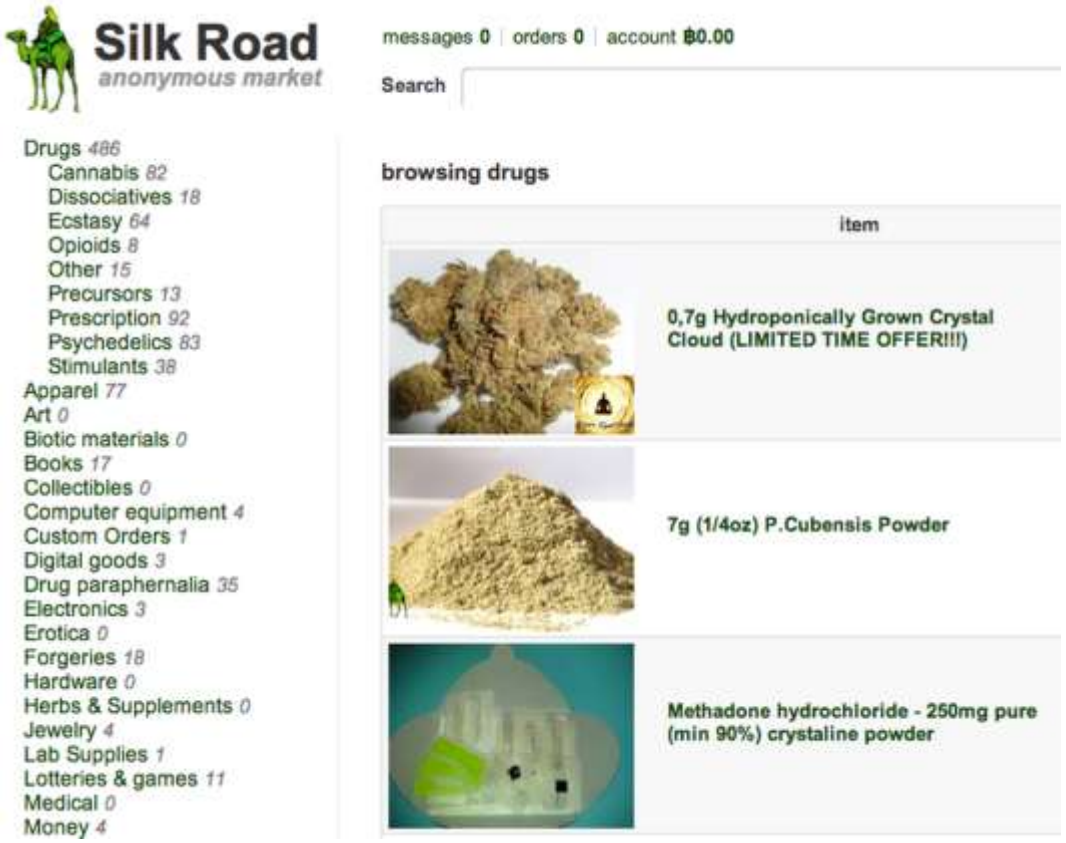


SECTRA
Knowledge and passion

Tor: anonym routing

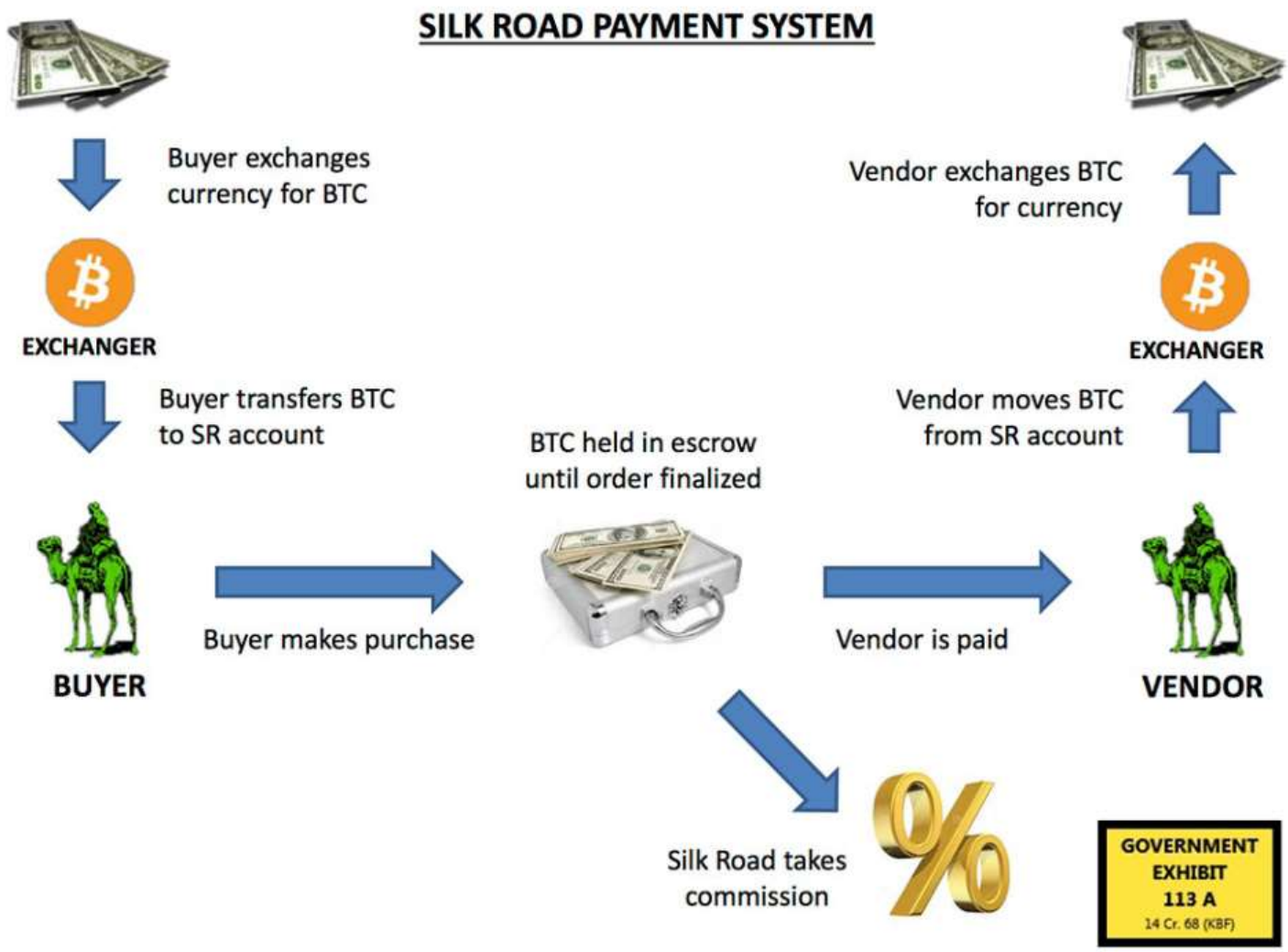


Darknet Market (DNM)



SECTRA
Knowledge and passion

Pengaflödet i DNM

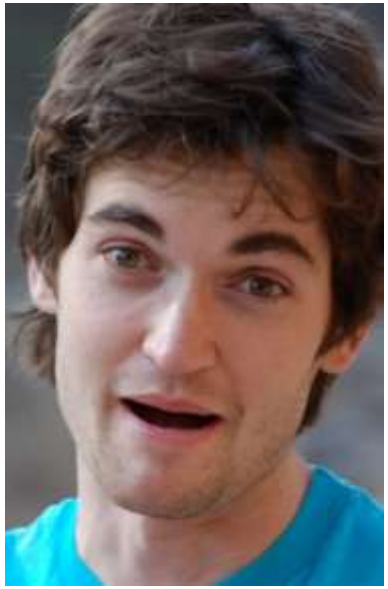


Silk Road: Den mest kända DNM

- Grundades i januari 2011
- Gick att hitta på tor-adressen silkroad6ownowfk.onion
- Uppskattad omsättning Q1+Q2 2012: 15 milj. USD
- Fungerar likt Ebay/Tradera: tar en avgift på försäljning, håller pengar, rankingsystem
- Drevs av pseudonymen “Dread Pirate Roberts”

Silk Road stängdes av FBI

- Ross William Ulbricht greps i oktober 2013, anklagad för att vara Dread Pirate Roberts
- FBI beslagtog 26000 bitcoin, då värt 3.6 miljoner USD
- Livstids fängelse för narkotikabrott, pengatvätt, m.m. utan möjlighet till villkorlig frigivning



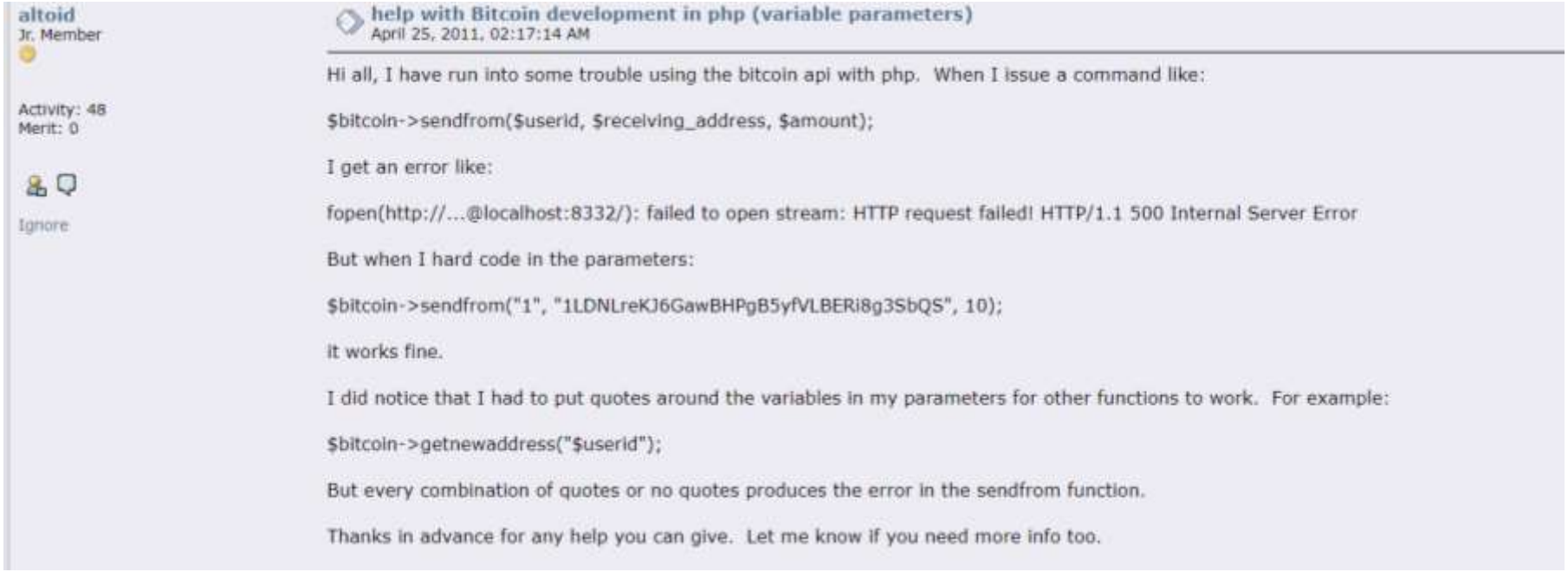
Komplikationer i utredningen

- Secret Service-agenten Shaun Bridges passade på när han stängde Silk Road
- Han sände 20000 bitcoin till sin egen plånbok, dåvarande värde 2.5 miljoner SEK

"This was a federal law enforcement agent . . . who decided to steal bitcoins that he later converted to cash, from the target of the investigation and later blamed on a cooperating witness."

- Bridges dömdes till sex års fängelse

Forensik kring Silk Road



altoid
Jr. Member

Activity: 46
Merit: 0

Ignore

help with Bitcoin development in php (variable parameters)
April 25, 2011, 02:17:14 AM

Hi all, I have run into some trouble using the bitcoin api with php. When I issue a command like:

$bitcoin->sendfrom($userid, $receiving_address, $amount);

I get an error like:

fopen(http://...@localhost:8332/): failed to open stream: HTTP request failed! HTTP/1.1 500 Internal Server Error

But when I hard code in the parameters:

$bitcoin->sendfrom("1", "1LDNLreKJ6GawBHPgB5yfVLBERi8g3SbQS", 10);

it works fine.

I did notice that I had to put quotes around the variables in my parameters for other functions to work. For example:

$bitcoin->getnewaddress("$userid");

But every combination of quotes or no quotes produces the error in the sendfrom function.

Thanks in advance for any help you can give. Let me know if you need more info too.

```
$bitcoin->sendfrom("1", "1LDNLreKJ6GawBHPgB5yfVLBERi8g3SbQS", 10);
```

Kända DNM

- Silk Road, sedan Silk Road 2.0 och 3.0
- Flugsvamp / Flugsvamp 2.0 (Sverige)
- Silkkitie (Finland)
- AgoraMarket
- AlphaBay
- ...

Alphabay och Hansa

Tillslag mot två DNM under 2017

- AlphaBay: >200k användare, >40k säljare
- Skattning: >1 miljard USD omsättning sedan 2014
- “The FBI and its partners used a combination of traditional investigative techniques along with sophisticated new tools to break the case and dismantle AlphaBay”
- Hansa Market stängdes samtidigt av polis från NL

Fallstudie: Swepuff

- Dom i Ystad TR mål B 1038-16, juli 2017
- Säljare på Flugsvamp 2.0 “Swepuff”/”Malvax”
- Amerikanska myndigheter hittade backup-kopior av Flugsvamp-sidan
- Fram till april 2016 skickades 4000 försändelser med narkotika, skattningsvis 3.8 miljoner SEK
- Två bröder dömdes till 10 års fängelse för grovt natkotikabrott

Katt-och-råtta-lek

U.S. Immigration and Customs Enforcement

THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

SECTRA
Knowledge and passion

Kryptovirus: Lukrativt för bedragarna

SECTRA
Knowledge and passion

Kryptovirus är en utvecklad industri

- “I en guldrusch, sälj spadar”
- Företagsamma programmerare erbjuder färdiga kryptovirus som andra kan använda
- Priser varierar mellan 474 kr till 5138 kr (källa: kryptera.se)
- RaaSberry är ett sådant exempel
- Europol: “Ransomware continues be one of the most prominent malware threats in terms of the variety and range of its victims and the damage done.”

Pengatvätt

SECTRA
Knowledge and passion

- April 2018: Europol genomför Operation Tulipan Blanca
- Finland, Spanien, USA: 11 arresteringar.
- Bitcoin användes för att tvätta > 8 miljoner EUR och föra över till Colombia.

SECTRA
Knowledge and passion

Kryptovalutor med anonymitet

- De senaste åren har nya kryptovalutor med mål att förhindra spårning
- Mimblewimble och Confidential Transactions: anonymitet i existerande blockkedjor.
- Dash, Zcash, Monero är helt nya valutor



De privata valutorna ökar kraftigt

"Cryptocurrencies continue to be exploited by cybercriminals, with Bitcoin being the currency of choice in criminal markets [...]

However, other cryptocurrencies such as Monero, Ethereum and Zcash are gaining popularity within the digital underground."

Monero (XMR)

- Grundades 2014
- Använder Cryptonote-protokollet för att dölja sina spår
- Unlinkability
  - Ska vara svårt att se att två eller fler transaktioner skickas till samma person
- Untraceability
  - Givet en input ska det vara svårt att se var motsvarade output hamnar

Monero (XMR) dyker upp överallt

- Cryptojacking: använder din webläsare för att gräva
- XMR accepteras numera av flera DNM
- 2017: Första ransomware med XMR
- Troligt att XMR kommer öka betydligt

Privata valutor är inte vattentäta

- Kumar et al. (2017): Kan identifiera 87% av XMR-outputs med säkerhet
- Möser et al. (2017): Metadata och timing läcker information.
- Mycket forskning sker idag på båda fronterna:
  - Hur kan man knäcka Moneros säkerhet?
  - Hur kan Monero skydda sig mot dessa attacker?
- Tekniskt svårt att göra blockkedjan privat då transaktioner måste kunna verifieras

Kronofogdemyndigheten

2017: exekutiv auktion av Bitcoin

- Utmätning av skuldsatt företag resulterade i beslagtagna Bitcoin.
- ”Kan vara världens första bitcoin-utmätning”
- 0.6 bitcoin, värt 27600 kr
- Slutbud: 43000 kr (!)
- Enormt stort intresse för budgivningen
- Troligtvis inte sista gången

Sammanfattning

- Bitcoin och digitala valutor är här för att stanna
- Många sidor av myntet, många nya aspekter att hantera
- Spåra kryptovalutor är snart lika viktigt som att spåra ip-adresser
- Krävs kunskap, rutiner

- Tack!
- jonathan.jogenfors@sectra.com

SECTRA

Knowledge and passion

Jonathan Jogenfors

Research Manager
jonathan.jogenfors@sectra.com