

2018-05-08

# Digitala valutor, forensik och teknik



# Jonathan Jogenfors

- Forskningschef, Sectra Communications AB
- Teknologie Doktor, LiU 2017
- Postdokortjänst 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



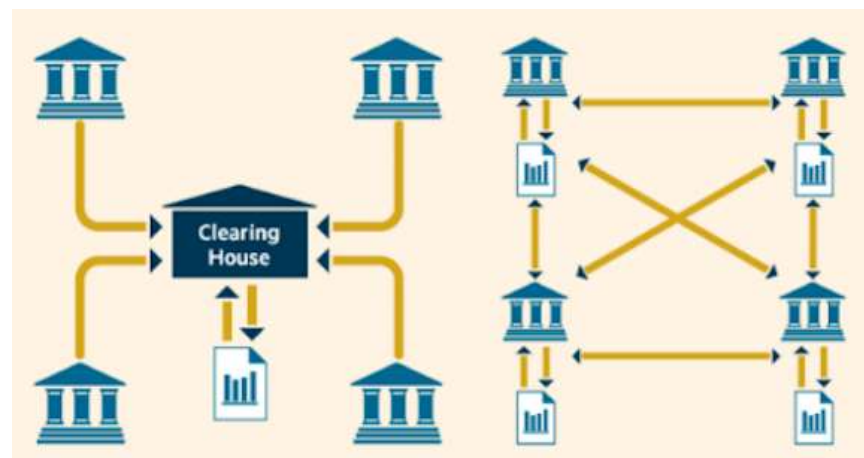
# Agenda

---

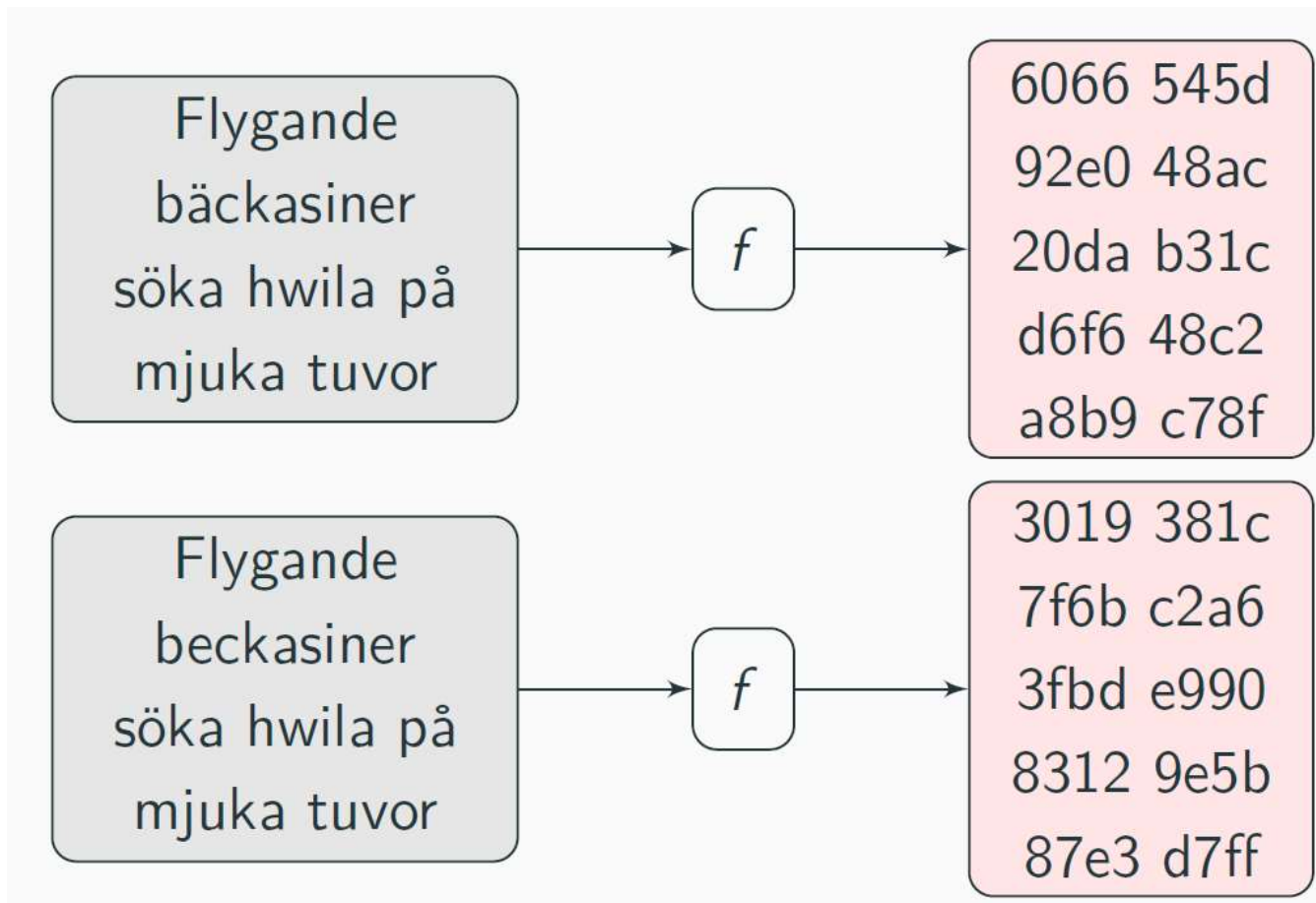
- Allmänt om Bitcoin och blockkedjan
- Metoder för att spåra transaktioner
- Ransomware
- Aktuella fall
- Nya kryptovalutor som förhindrar spårning
- Utblick

# Hur fungerar Bitcoin?

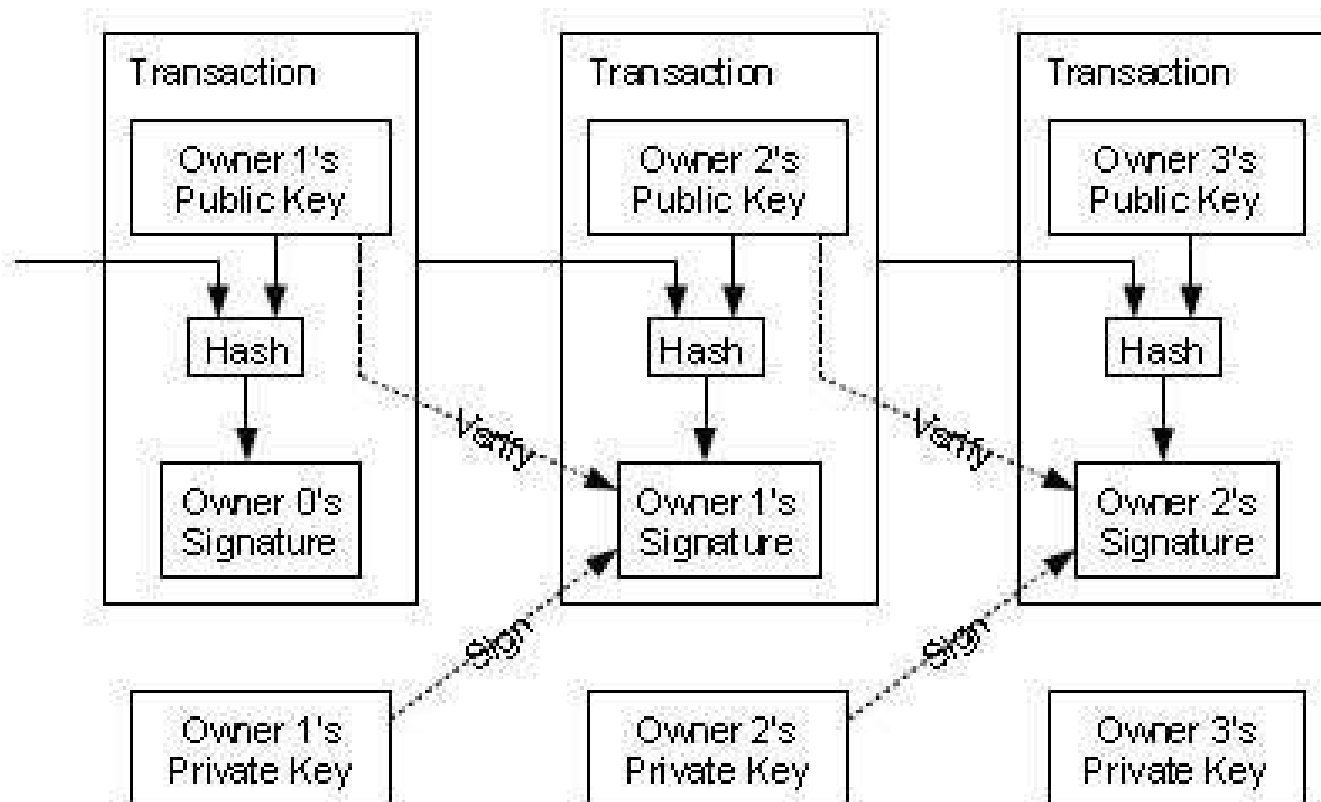
- Transaktioner sparas i en lista
- Saldot bestäms av summan av transaktioner
- Nya transaktioner läggs till på slutet
- Listan växer hela tiden, ingenting tas bort



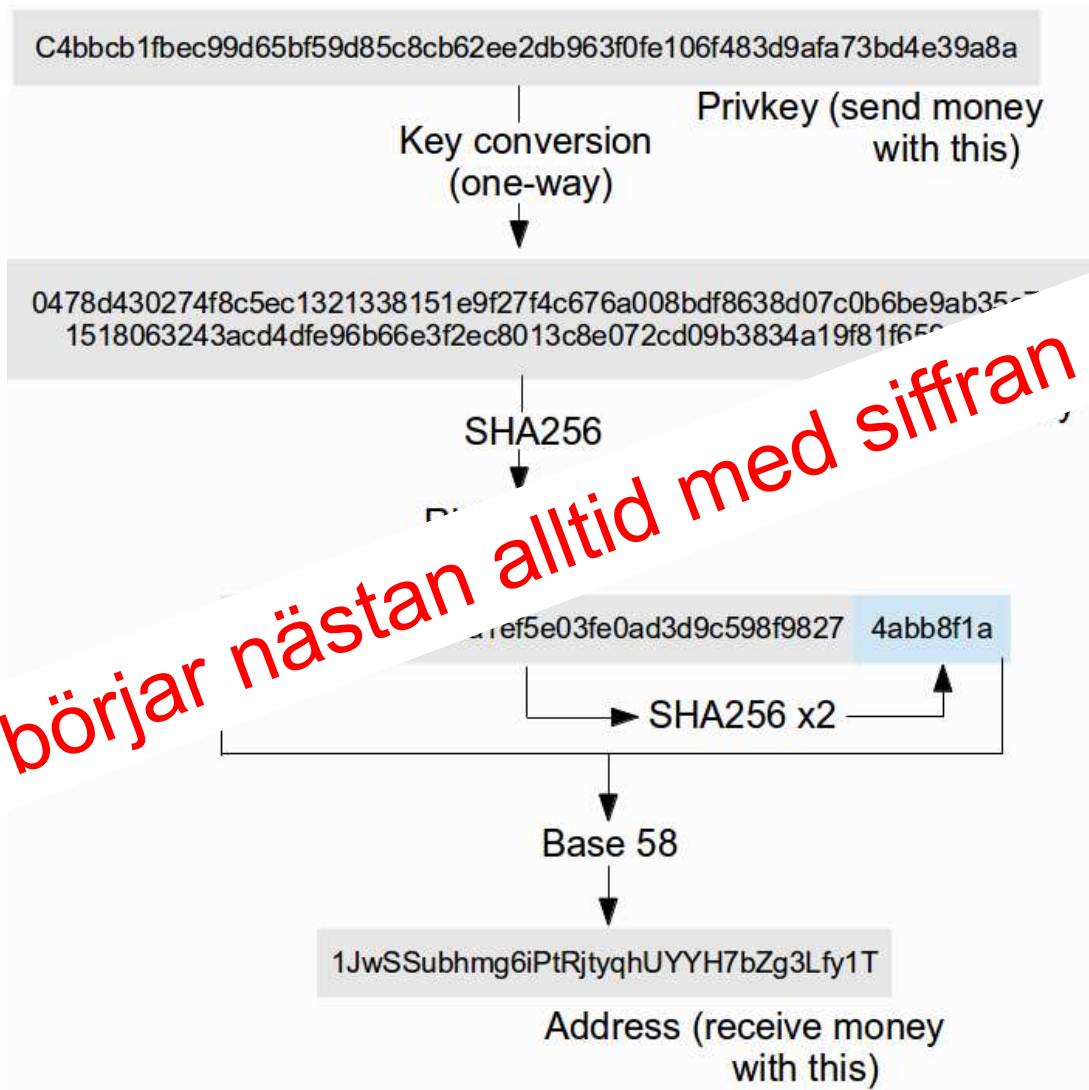
# Hashfunktioner: Små ändringar syns fort



# Bitcoin använder en blockkedja



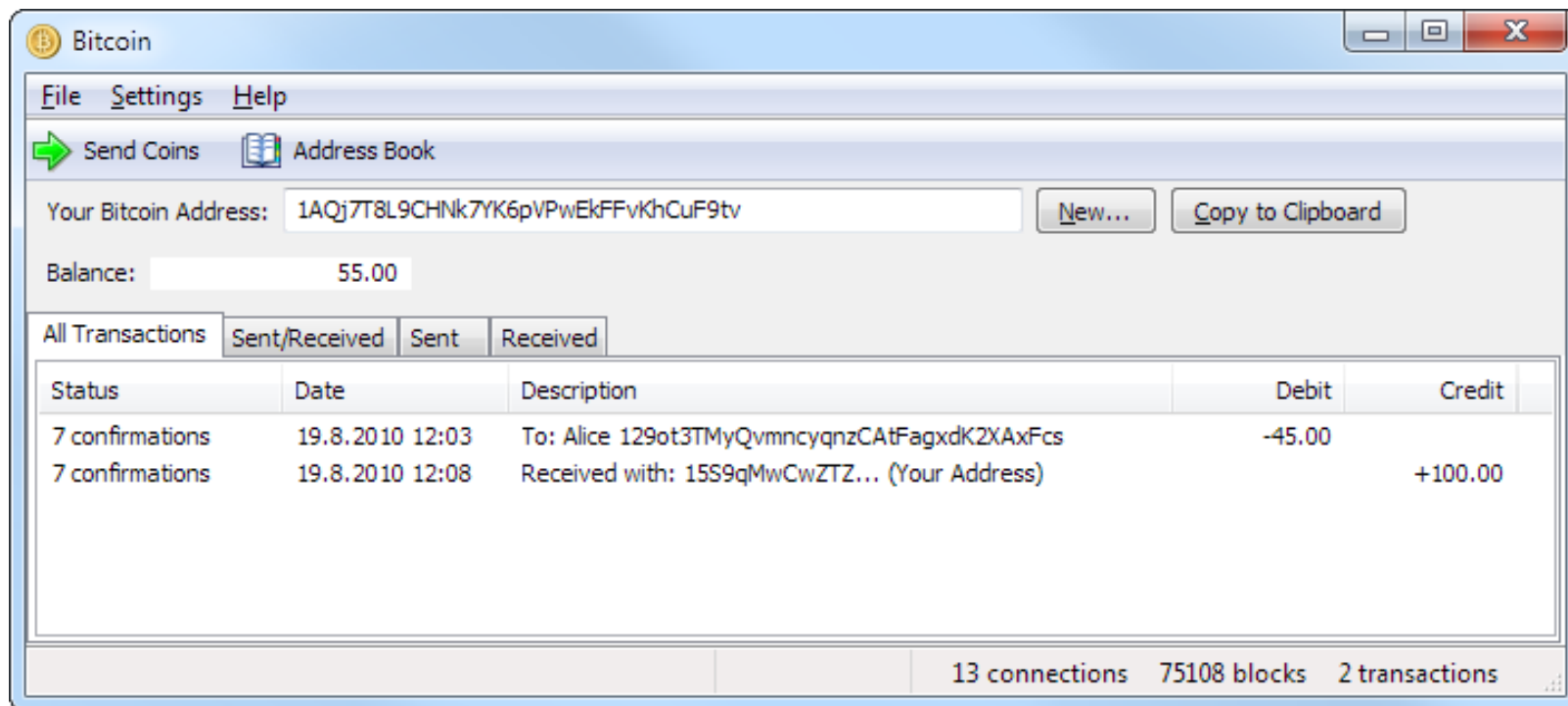
# Bitcoin använder kryptografi



Adresser börjar nästan alltid med siffran 1 eller 3



# Kontot sköts av ett plånboksprogram



# 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 mottagaradresser!

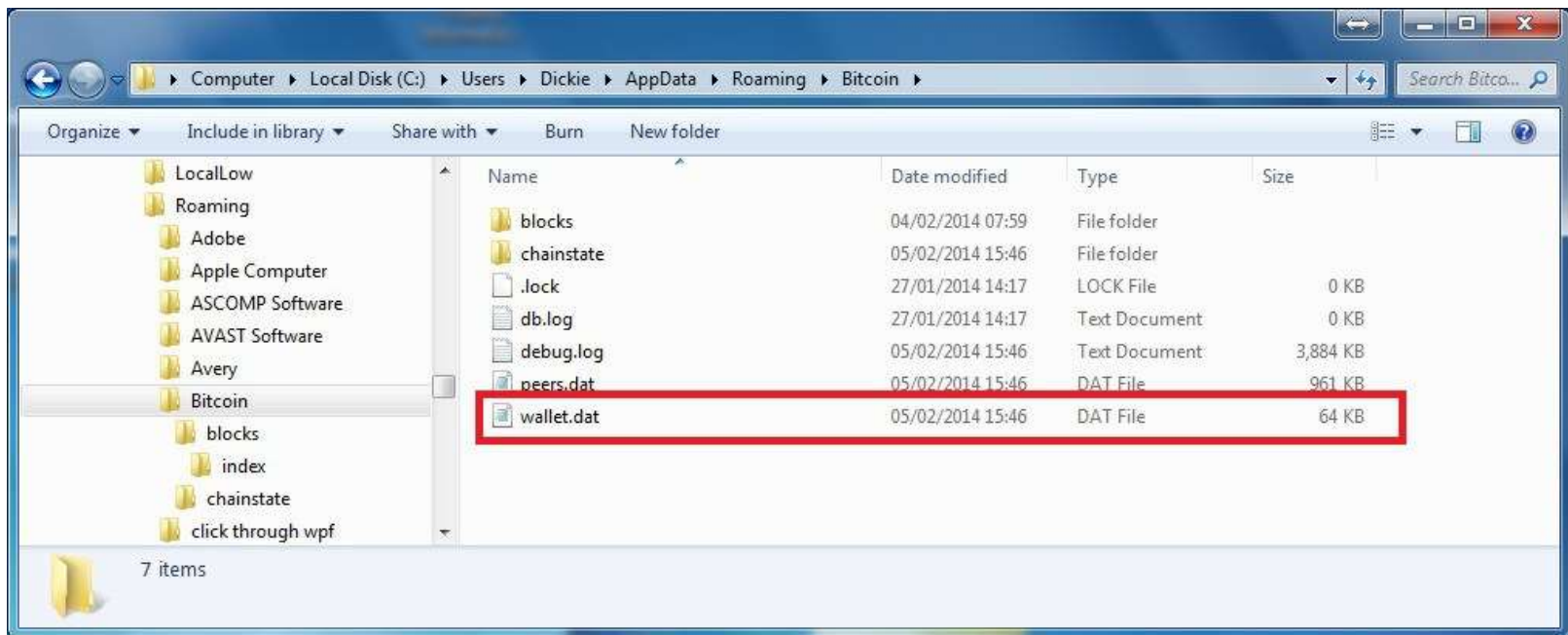


# Privata nyckeln styr allt

- 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



# Plånboksfilen är #1 vid tillslag



# Växelkursen är mycket volatil



# Bitcoin-forensik

---

- Spåra och identifiera personer och organisationer från blockkedjan
- Spåra illegal handel till och från marknadsplatser 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



# Se transaktioner, nästan i råformat

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	17JJVDXNvxunfeF3w2H76QAePZJ7Waeoxx
Hash 160	45166o4bdfa4d8b61e72104aababe94bd2356425
Tools	<a href="#">Related Tags</a> - <a href="#">Unspent Outputs</a>

Transactions	
No. Transactions	55
Total Received	0.25280248 BTC
Final Balance	0 BTC



[Request Payment](#) [Donation Button](#)

## Transactions (Oldest First)

[Filter](#)

Transaction Hash	Date
<a href="#">e67ef98cc096e4a853d30989c2663ec7a02b53cf2e158ea875377ac37a3a510</a>	2018-04-18 12:58:08
17JJVDXNvxunfeF3w2H76QAePZJ7Waeoxx	1NDyJNTjrwk5xPNhgAMu4HDHgtobu1s : 20 BTC 15LHAoK6WQdNKum4Y25OvbbZ6YPOFkq1t 0.00577952 BTC
	<b>Unconfirmed Transaction!</b> -0.04051517 BTC
<a href="#">a381773985286e7896c85344843e309a143cc398bc1ec4d29caa88e126</a>	2018-04-18 11:46:02
3G55XFin55XwiCXmoNTB8KtMgC9gipEw4	17JJVDXNvxunfeF3w2H76QAePZJ7Waeoxx 0.04051517 BTC
	<b>8 Confirmations</b> 0.04051517 BTC

# Wallet Explorer

## Klustering av plånböcker

WalletExplorer.com: smart Bitcoin block explorer

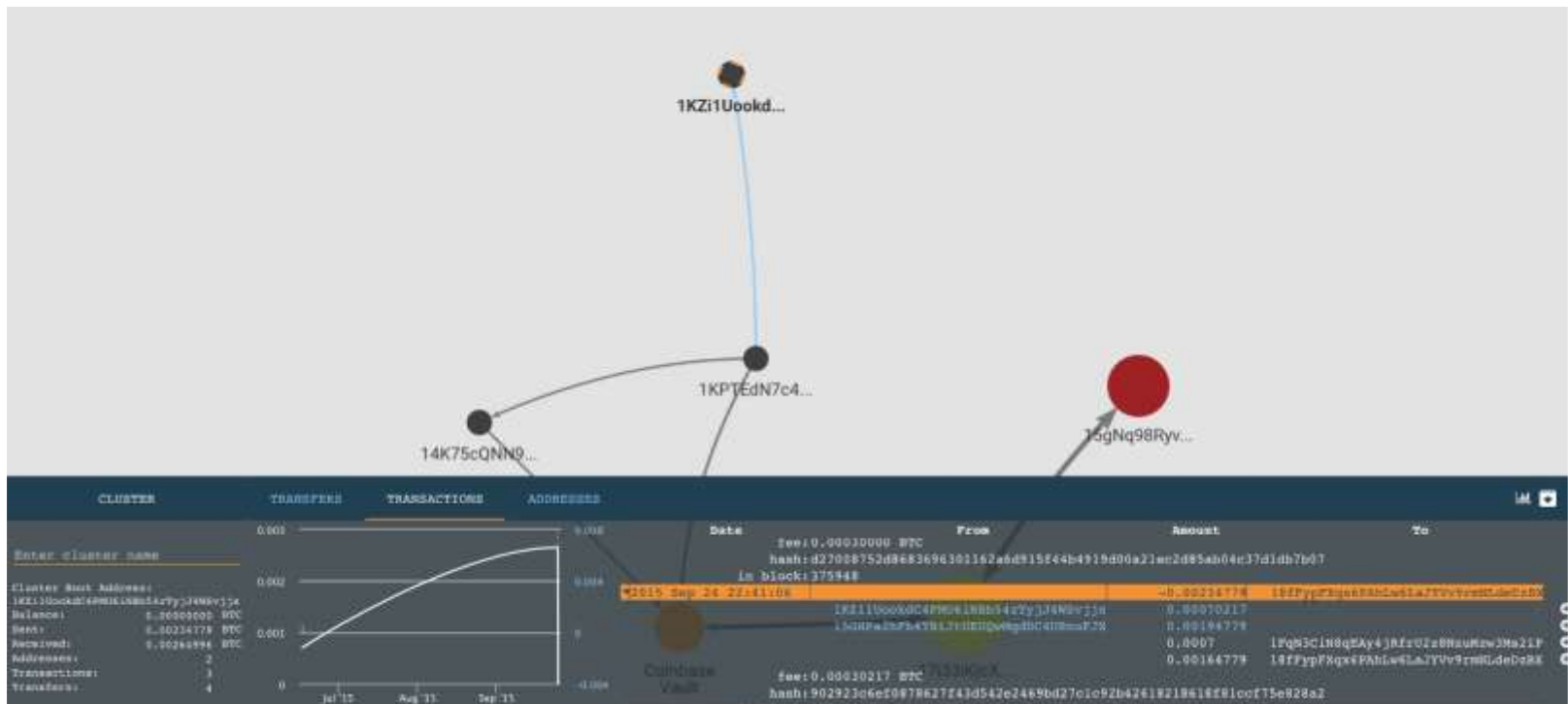
Wallet **SatoshiDice.com** ([link to service](#), [show wallet addresses](#))

Other wallets: | [current](#) | [original](#) |

Page 1 / 1038 [Next](#) [Last](#) (total transactions: 103,791) [Download as CSV](#)

date	received/sent	balance	transaction
2018-04-16 18:09:08	-0.07050637 [000002f0e8] -0.00993627 [d35a28f092] (-0.000964) fee	1.29994024	1d1fa07031194f11f92
2018-04-16 15:16:13	[0000002e10] +0.022	1.38044688	0fa1f1b350c1728801c
2018-04-16 10:23:18	[0000002e10] +0.02	1.35844688	80b7d18ef2a29f6d38c
2018-04-16 06:51:10	[14a690b78a] +0.001	1.33844688	738d44e3387a63f175
2018-04-16 03:50:32	[112f746027] +0.00315	1.33744688	628e2f3cfa2a0d7f8
2018-04-16 03:33:22	[00002c499b] +0.00134361	1.33429688	2a510aa0a3aa50222
2018-04-16 03:13:19	[c10e906adb] +0.00162	1.33295327	27be8204d3aa07c23
2018-04-16 00:43:07	[e6ad8eca99] +0.00063182	1.33133327	01d07d91a87d80e12e7
2018-04-15 22:49:54	[22d2b3131f] +0.00045	1.33070145	0a544b0f278b1d7311
2018-04-15 21:29:24	[7c94d71512] +0.0015	1.33025145	0cc551139710872006
2018-04-15 17:51:34	[00002c499b] +0.00283951	1.32875145	103ca873888d613e14
2018-04-15 14:37:18	[0000cd8ab] +0.00660316	1.32591194	05c0428a3dffa1704b
2018-04-15 14:21:00	[65361158a4] +0.000444	1.31930878	0d71fa767a138226dc
2018-04-15 11:59:38	-0.00958309 [c89ce27892] -0.001 [65361158a4] (-0.000522) fee	1.31886478	1aa707070701c1109b
2018-04-15 10:33:06	[e1d99bb902] +0.0003	1.32906987	f3a4017031c30d3089
	-0.199 [f00045a22e81]		

## Kommersiellt program för forensik

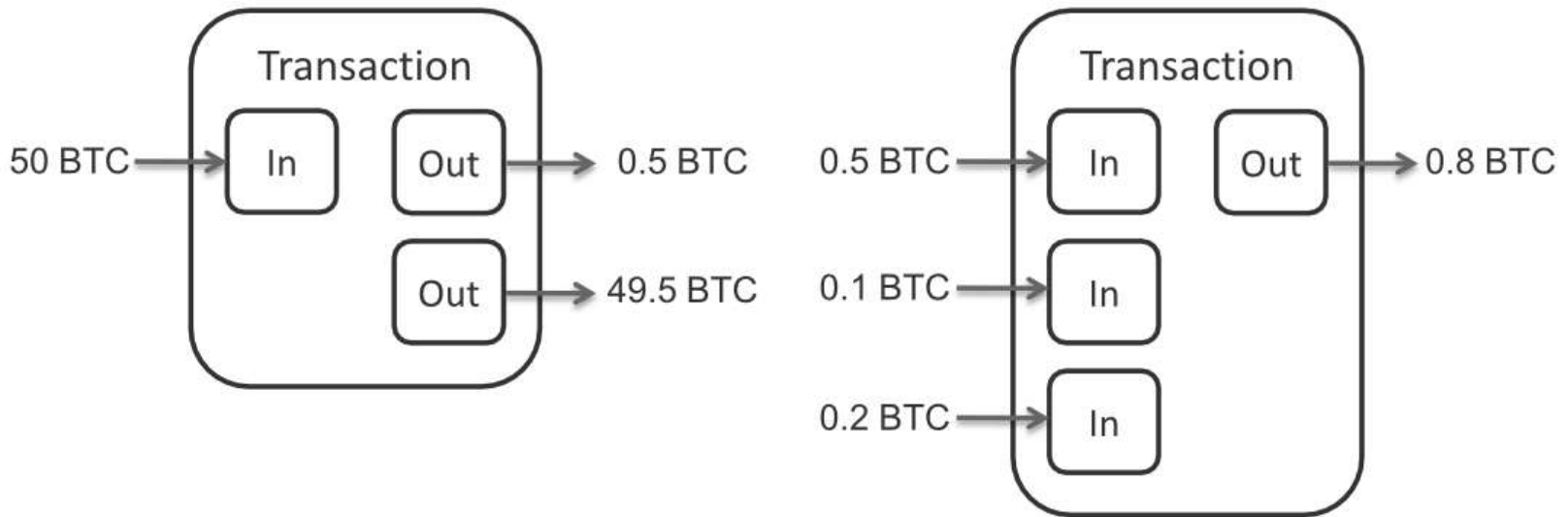


# Ett sätt att gruppera transaktioner

---

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

# Input- och outputadresser



Alla inputs måste förbrukas!

# Input-klustring

8b6008b2e369499c5c51058f5f09e549c160a84692c00cb97dfa2b4881e9cc27

142Z7VauMVdSV5DADb62DsJ7wvW9ccq18t (30.28851 BTC - Output)  
16H9oN1JFXSHEv16X8PLaS77MMF3EKqEiH (30.28851 BTC - Output)  
17RHwSeN5Ky8gGwTHCH8j4mZH3eqQNbrav (30.58936 BTC - Output)  
13b78oU4oCid4gQw87bvUMUZ1XpnZqwNQ1 (12.9148 BTC - Output)  
16BzfEpwF9P6ULmmMcbdag3m2ZaETGgwYN (29.55 BTC - Output)  
1CusinkMvW53WtupuspCMDyI8gZ2sb13zv (30.28851 BTC - Output)  
1PXA5YNC2MWYtssfsBTBPMWXW8cDkPuMTB (30.28851 BTC - Output)  
1Gg2D33ySPndnSELBnmze1QsmycSdeGVkX (30.28851 BTC - Output)  
1FdPwjg7XJfrEqdQnduusg2K51UuJDACci (30.28851 BTC - Output)  
178AKou6Q2741uPqt9FQfB26ZUK16f3yDt (29.36578 BTC - Output)  
1LZe2eSEKr8ik6ja8k8YNSH1amR2czmwwe (30 BTC - Output)  
16ah8vzFqtrnyCPtp57Y55bkXwSot7Bd3ic (29.84 BTC - Output)  
1Dn92DXHrPNVH7EMrD5oawDedWdk43Jjkk (29.83951 BTC - Output)  
1NvC4vQVbwJUjXWHBHKIGKAmKRMkRKe7gv (30.13 BTC - Output)  
14kSwoX2cPkwRtKW5KTWBFGtraYpXrYckW (99.45 BTC - Output)  
1AkMajTEiLXUa3f9SNjLZcvLtxY54wyC6n (141.9995 BTC - Output)  
1KRMiP4uLyy2hm86MRRQv4ghkQthVK6BH6 (29.6 BTC - Output)



1Z9ADFwVMZvgjN3HoNf91XoT2Lpth559F - (Spent)  
17iCsx5w55KcNdCRRp9xXFDcMU7btNhqpm - (Unspent)

0.01001 BTC  
675 BTC

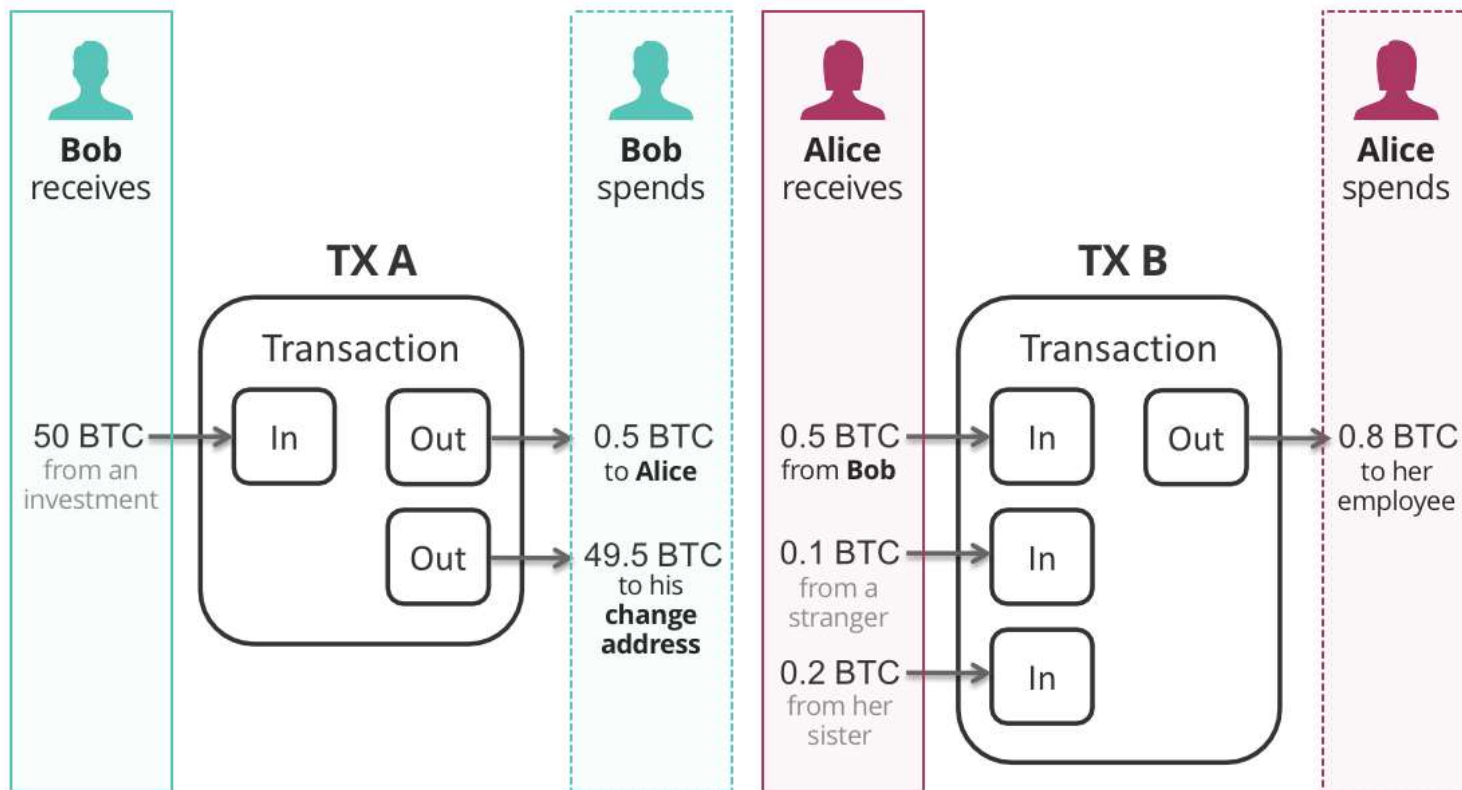
6 Confirmations 675.01001 BTC

En användare styr dessa adresser!

# 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





# Växel-klustring

8b5008b2e369499c5c51058f5f09e549c160a84692c00cb97dfa2b4881e9cc27

142Z7VauMVdSV5DADb62DsJ7wvW9ccq18t (30.28851 BTC - Output)  
16H9oN1JFXSHEv16X8PLeS77MMF3EKqEiH (30.28851 BTC - Output)  
17RHwSeN5Ky8gGwTHCH8j4mZH3eqQNbrav (30.58936 BTC - Output)  
13b78oU4cCid4gQw87bvUMUZ1XpnZqwNQ1 (12.9148 BTC - Output)  
16BzfEpwF9P6ULmmMcbdag3m2ZaETGgwYN (29.55 BTC - Output)  
1CusinkMvW53WtupuspCMDyi8gZ2sb13zv (30.28851 BTC - Output)  
1PXA5YNC2MWYtssfsBTBPMWXW8cDkPuMTB (30.28851 BTC - Output)  
1Gg2D33ySPndnSELBnmze1QsmycSdeGVkX (30.28851 BTC - Output)  
1FdPwjg7XJfrEqdQnduusg2K51UuJDACci (30.28851 BTC - Output)  
178AKou6Q2741uPqt9FQfB26ZUK16f3yDt (29.36578 BTC - Output)  
1LZe2eSEKr8ik6ja8k8YNSH1amR2czmww (30 BTC - Output)  
16ah8vzFqtryCPtp57Y55bkXwSot7Bd3ic (29.84 BTC - Output)  
1Dn92DXHrPNVH7EMrD5oawDedWdk43Jkk (29.83951 BTC - Output)  
1NvC4vQVbwJUjXWHBHKiGKAmKRMkRKe7gv (30.13 BTC - Output)  
14kSwoX2cPkwRtKW5KTWBFgtraYpXrYckW (99.45 BTC - Output)  
1AkMojTEiUXUa3f9SNjLZcvLtxY54wyC6n (141.9995 BTC - Output)  
1KRMiP4uLyy2hm86MRRQv4ghkQthVK6BH6 (29.6 BTC - Output)



1Z9ADFwVMZvgjN3HoN91XoT2Lpth559F - (Spent)

17iCsx5w55KcNdCRRp9xXFDcMU7btNhqpm - (Unspent)

0.01001 BTC  
675 BTC

6 Confirmations 675.01001 BTC

Samma användare styr dessa adresser

# Det går att följa växelpengar

17dfab0bfa7611e4ace646714ea043fc48a8c727e1d847b3be0eaf0085efd35	(Fee: 0.00005 BTC - Size: 373 bytes) 2014-11-12 07:46:55
1FHmRRw4hR1TixAyEg7e247DQQ6uv7sVq6 (0.13012336 BTC - Output) 1DxxeC5NkKWYSy4RRc9pzu6D4ZzcCCBWh6 (0.483 BTC - Output)	→ 15vMjmkU24bkSGyxrjKKeDjLQmVNg8 (Spent) 0.01007336 BTC 1jnM9aEtFTIEZWyfwYjklJTWgtpRy96t (Spent) 0.603 BTC
	0.01007336 BTC
3e0d75fb0f1c9b3bbe35c4b299a77fa144189a508f2e5bd5034e30750d4a64	(Fee: 0.00005 BTC - Size: 813 bytes) 2014-11-12 08:26:55
12vVc0mG74ezRnXsZ4xf0fims0eFrR62n (0.11472313 BTC - Output) 15vMjmkU24bkSGyxrjKKeDjLQmVNg8 (0.01007336 BTC - Output) 1ME0ce4CUKkKopR9zt2CHPF0wz3UfmsxDui (0.65601829 BTC - Output) 1H5xFt6pH44P7MAyyW2QxTzPtnjNF69 (0.39235214 BTC - Output) 1Pxx9MyQV4RUjMA5QbRTFsHlrB7vqcAQM (0.43188342 BTC - Output)	→ 1Fs1NDKwRrd4uVMCMUu177hv2wcl_u6RA (Spent) 1.595 BTC 1MhTX5H8Es9g9f9buDRCp8MPqPhEr5rdPRV (Spent) 0.01000034 BTC
	1.595 BTC
89709a80b9fe2e75f544d9cdcd0dc5f9fd0f6968b5487ece6df577a478c54c	(Fee: 0.00005 BTC - Size: 962 bytes) 2014-11-12 08:46:55
1BjmiYLrscKUVZ3PAgMK89QQE4MxJraW5 (0.01002979 BTC - Output) 1HAEVU9GAvaASptjwBTuuuQeZijGkYnZ7m (0.01003353 BTC - Output) 15d5f8kUeHq3mLzxyqd7C4R8PC44R8aoni (0.01214894 BTC - Output) 1DteEVdtdXF9XaT24EHTLY551wHNk0Gdp (0.0100123 BTC - Output) 1MhTX5H8Es9g9f9buDRCp8MPqPhEr5rdPRV (0.01000034 BTC - Output) 1AEn7RzH28eembYQ76w6n7PokZ9HDr0U2 (0.708 BTC - Output)	→ 1NLoD8mpqcdXU7gWTGR6FXeXrgdwdnt (Spent) 0.0101749 BTC 1jnM9aEtFTIEZWyfwYjklJTWgtpRy96t (Spent) 0.75 BTC
	0.0101749 BTC
473a1d0e567fbbbc16c2c6efe9cb98dd2f1aac527a7f5079904b54e94c944	(Fee: 0.0001 BTC - Size: 373 bytes) 2014-11-12 11:06:58
1NLoD8mpqcdXU7gWTGR6FXeXrgdwdnt (0.0101749 BTC - Output) 198j6wa8CUQzR5kYAT9PTDABF1z4UBhYqk (0.34 BTC - Output)	→ 13ZMDChesJQuAc8WY185La7nVNsQvayAnb (Spent) 0.0100749 BTC 1LDTqcmvBEZnwp4juyhE6xsDeCZrutgJyf (Spent) 0.34 BTC
	0.0100749 BTC

# Avancerad växel-klustring

620b7b461fa042c5fbc2ebcc60e435dcb2f5b2eb8466f83eab0602ba5530deed

(Fee: 0.0001 BTC - Size: 521 bytes) 2014-11-11 14:49:48

13xytug16pRW2HzQqHAKAFMwt363WuaNAa (0.01015704 BTC - Output)  
1LPzbMPkTRNTMYcitbTqMJdE3DWNngPDFWd (0.44729055 BTC - Output)  
1P1yyVDFs124GAqjBmKBc6LoqP6ARWqW (0.05268594 BTC - Output)



19bnzqB9ziNAzCZTx38mBG82wQm4QXrYpR - (Spent) 0.5 BTC  
1HAEVUJ9GAvASptjwBTuuuQeZqGkYnZ7m - (Spent) 0.01003353 BTC

e98780e7ed8848025430d0a8d8a03ec9ebb68b3049e6cc23d450281738aa523a

(Fee: 0.00005 BTC - Size: 374 bytes) 2014-11-12 07:46:54

1FcwT7EK9tPaie4TU2CQdG3u7F9hjMnsrd (0.01000019 BTC - Output)  
17cAqKyhtDtaLARR3RzjNY5DEXPB7Cp9g (0.22319875 BTC - Output)



1JDtry8hU8uMTne2CYPjn3HJds9DhaMcTs - (Spent) 0.221 BTC  
15d5ftkUoHqJmLzxyqd7C4R8PC44Rsaoni - (Spent) 0.01214894 BTC

0.01214894 BTC

ec10ed7a54550e223f3edda22ef5def1f1888735750f16a4cd3ca1e5c1fb932

(Fee: 0.00005 BTC - Size: 669 bytes) 2014-11-12 08:38:43

1cU62uiCoEFmWNMFih7gK72Sscexprf (0.01001968 BTC - Output)  
12C2qQED5HkJEnSUPr6nLB7RjJ4JQGvQ2 (0.01000008 BTC - Output)  
1Mwzzq5N4CPaABuw5vhH7iVKpgwyg8v5Z2 (0.01073976 BTC - Output)  
1HBpt2gxrDaGuCnX4pNtFEaP8HDZ9CBuHK (0.53030206 BTC - Output)



1DbEvidNXF9XqT2J4EHTLY551txHNKhGdp - (Spent) 0.0100123 BTC  
1PoeP5nXZm2hBunHPDjKjrCcT1Q7qbtSMg - (Spent) 0.551 BTC

0.0100123 BTC

00700a000b9e2e75f544d3dcd0dc6f5c9fd6f86s0b5487ece0d577a478c54c

(Fee: 0.00005 BTC - Size: 962 bytes) 2014-11-12 08:46:55

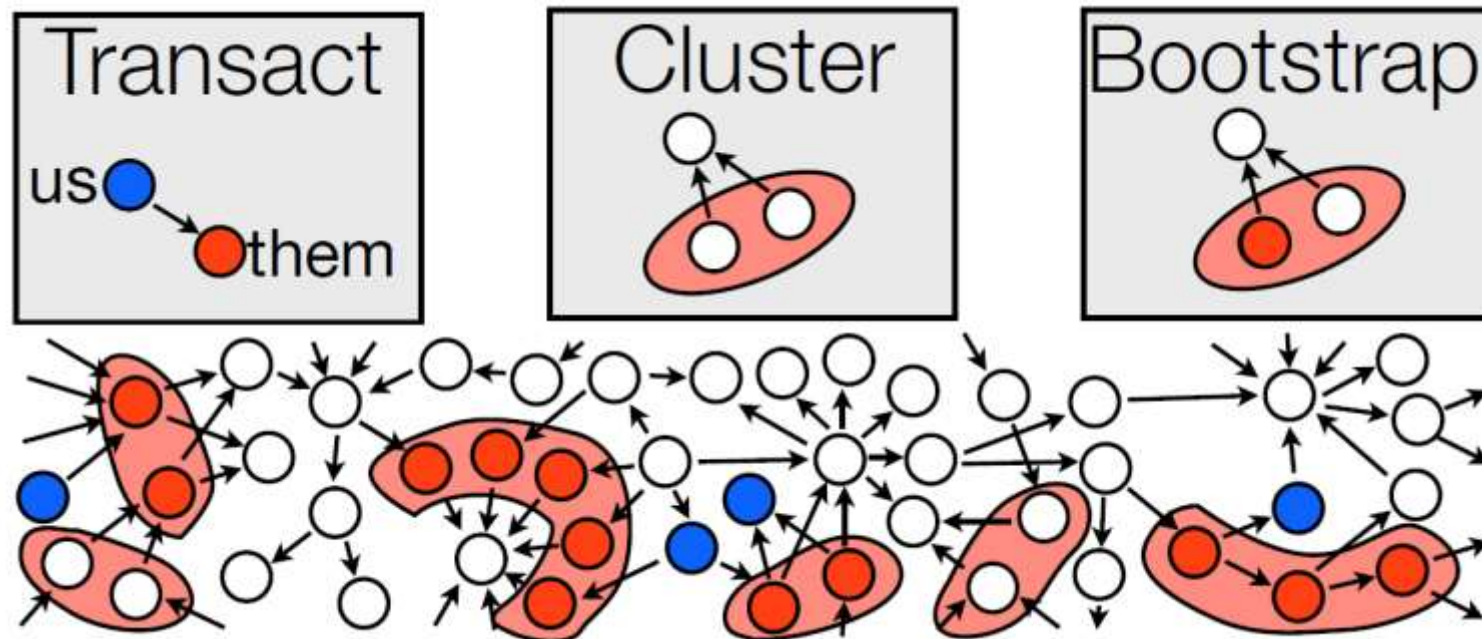
1BtmY1cckK1VZ3P6vMK89QOF4MvtraW5 (0.01002979 BTC - Output)  
1HAEVUJ9GAvASptjwBTuuuQeZqGkYnZ7m (0.01003353 BTC - Output)  
15d5ftkUoHqJmLzxyqd7C4R8PC44Rsaoni (0.01214894 BTC - Output)  
1DbEvidNXF9XqT2J4EHTLY551txHNKhGdp (0.0100123 BTC - Output)  
1MhTXSH8Es9g9NouDRcp8MPqPhE5rdPRv (0.01000034 BTC - Output)  
1AEhTrzH28eenbYQ76w6n7PokZ9HDrAU2 (0.708 BTC - Output)



1fLod8mpgcdXu7gWTGR6FxeXqgdwdtd - (Spent) 0.0101749 BTC  
1Jm9aEiFTE2WYwYjklW7wgbRy96t - (Spent) 0.75 BTC

0.0101749 BTC

# Klustering grupperar adresser



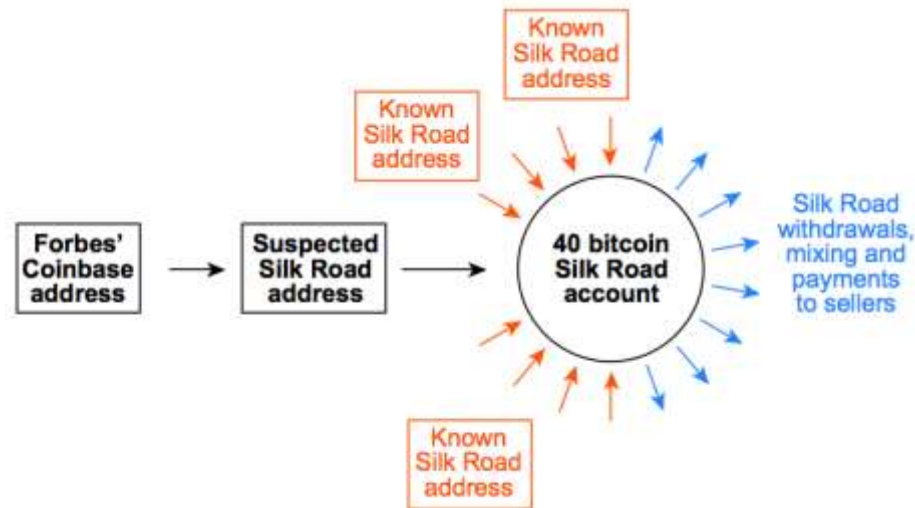
Meikelejohn et al. (2013) spårade 1.3M publika nycklar

# Kluster ska sedan namnges

---

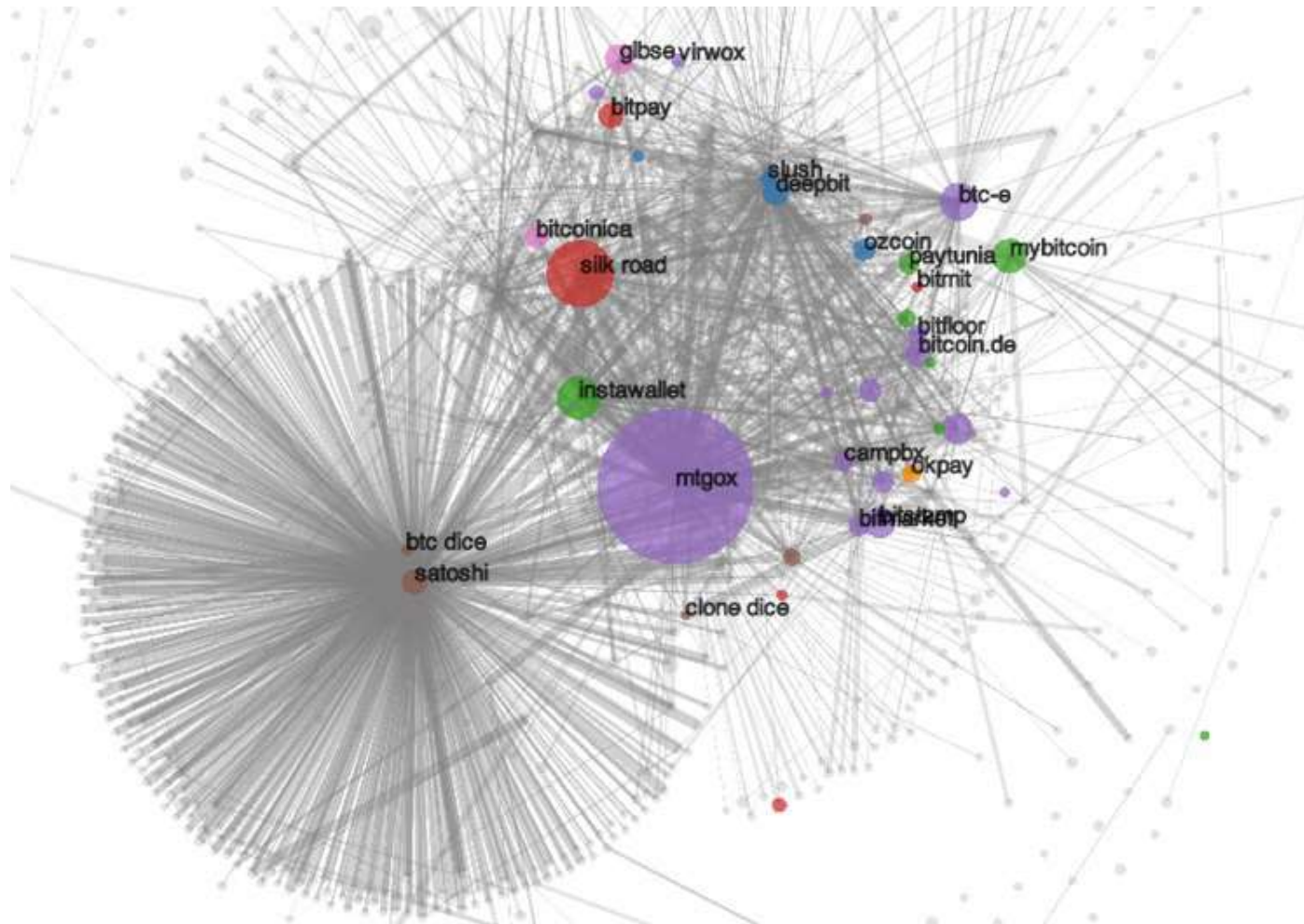
- I nästa steg identifierar vi vem som äger kluster
- En lös tråd låter oss nysta upp hela garnet
- Adresser i forum-signaturer
- Donations-adresser m.m.
- Exit-noder

# Aktiv spårning



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

# Identifizierte kluster



# IP-adresser?

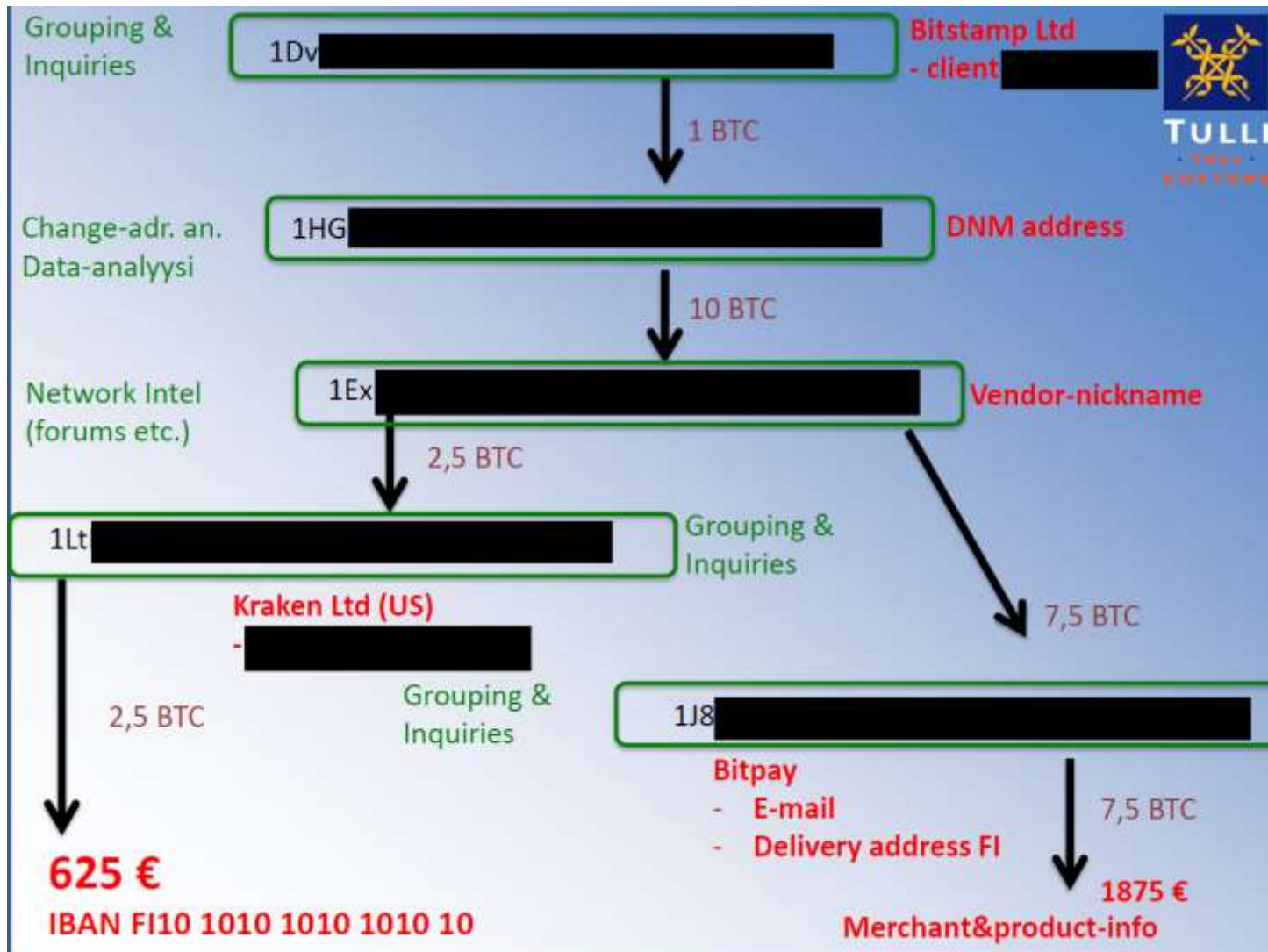
- Det hade varit bekvämt att ha IP-adresser från transaktionerna
- Detta sparas dock *inte* i blockkedjan
- Passiv analys kan därför inte se IP-nummer
- Om man däremot aktivt avlyssnar nätverket live är det möjligt
- Detta kräver dock stor arbetsinsats och går inte i efterhand



# 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 många växlare i svåra länder

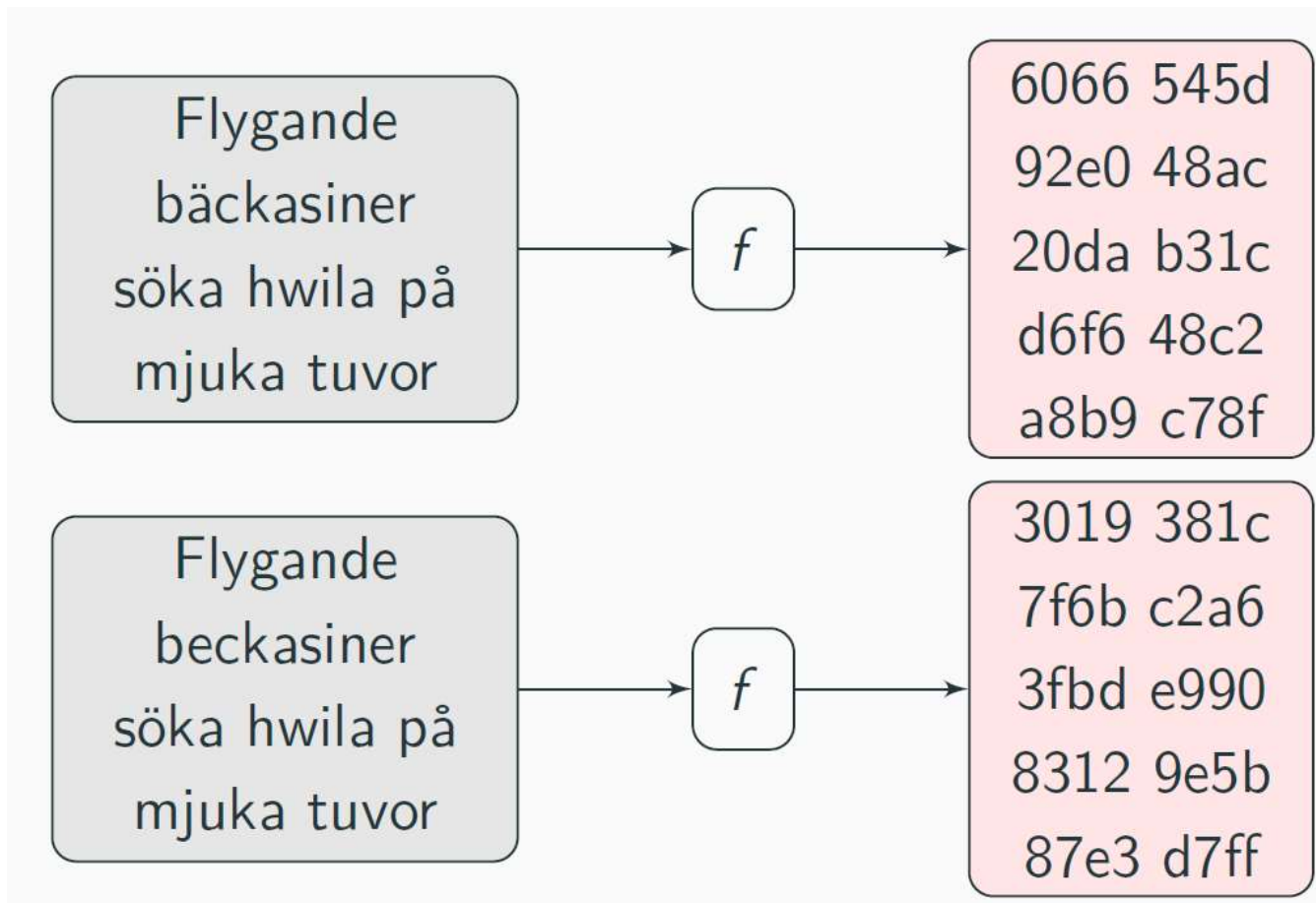
# Fallstudie från finska tullen



# “Mining”: gräva pengar med datorkraft



# Hashfunktioner: Små ändringar syns fort



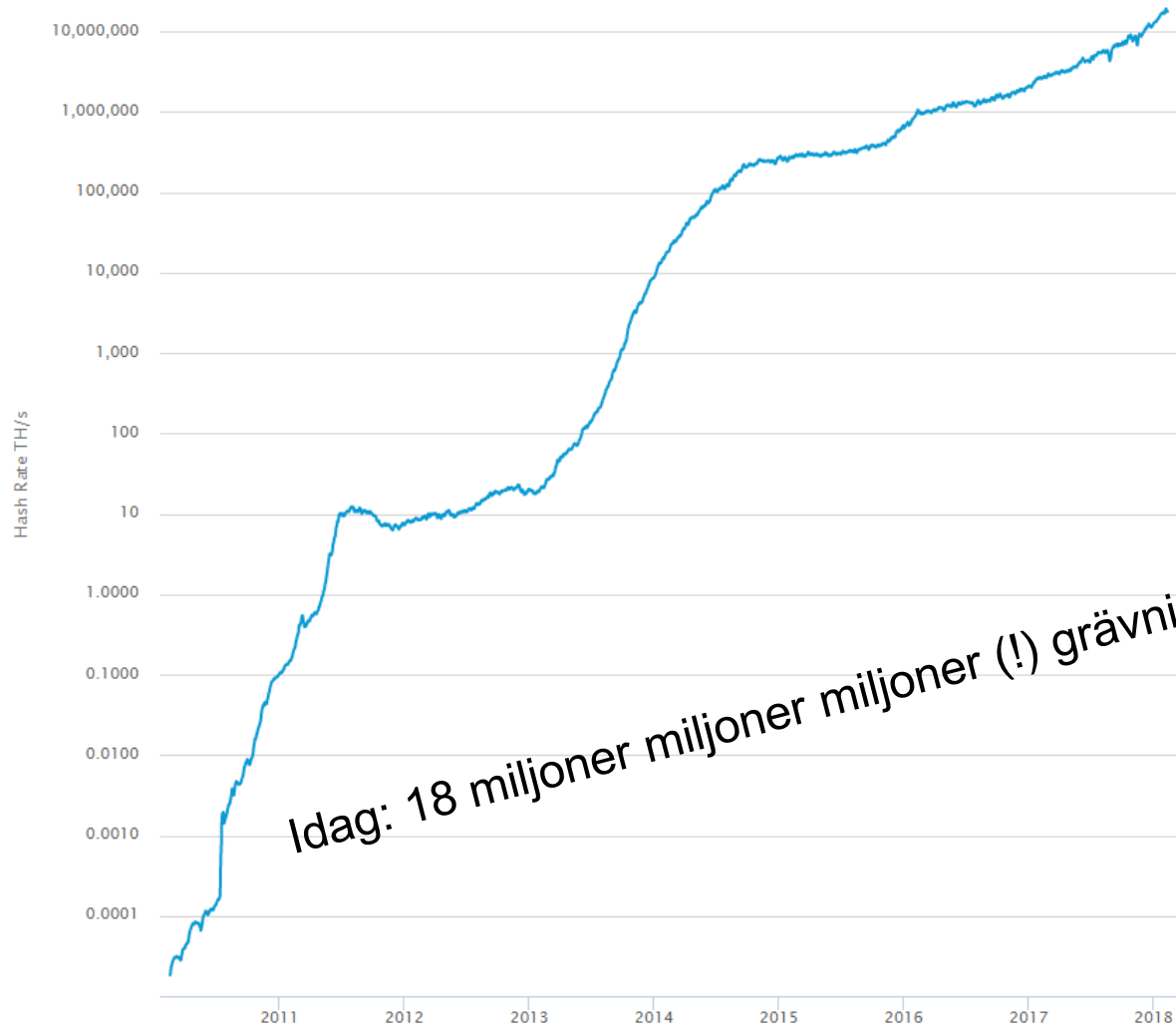
# Proof of Work

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

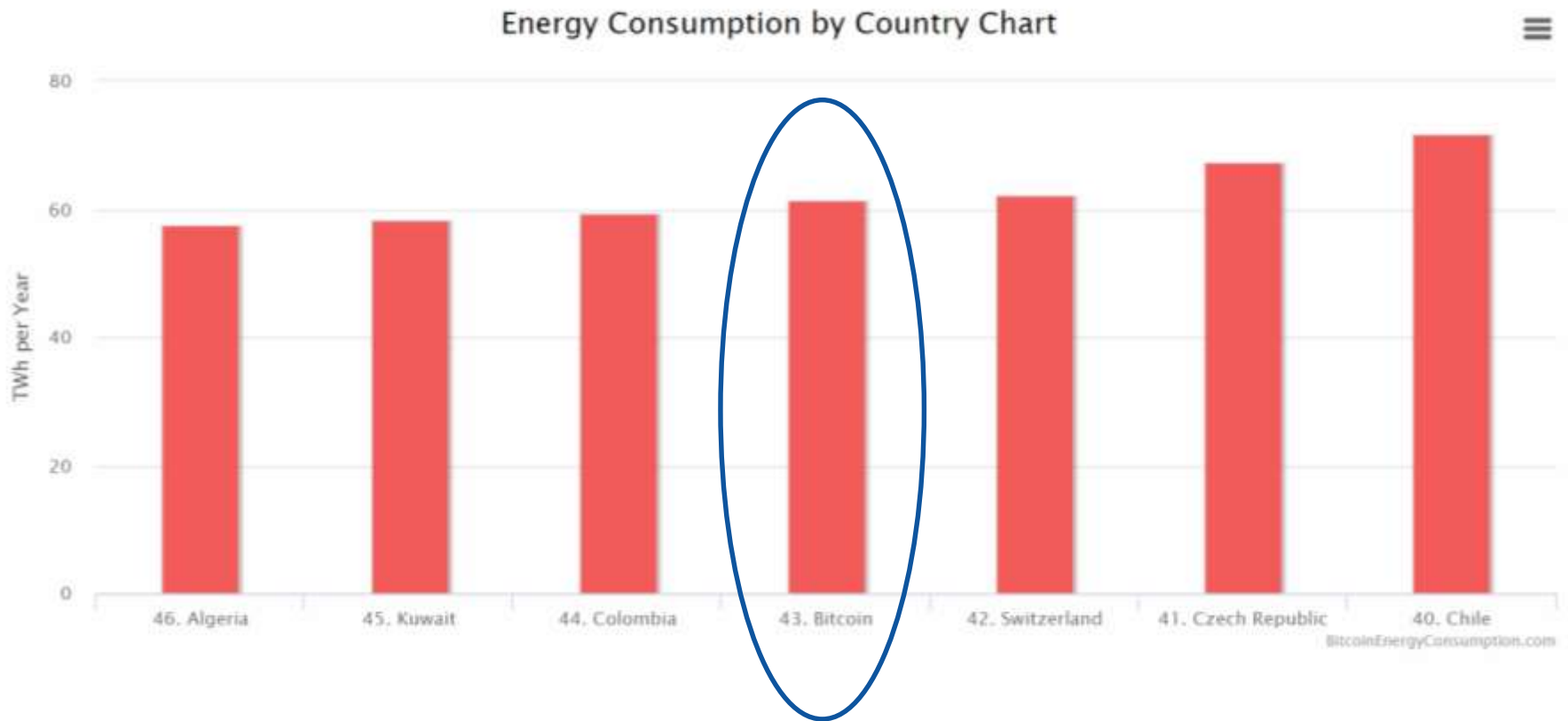


# Gräva Bitcoin är idag extremt svårt



Inte direkt gröna pengar

# Samma strömförbrukning som Schweiz!





# Uppgifter

1. Vilka 40 adresser 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



# 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

1. Släng

2. Få fo

3. När

- Senast i April  
miljoner USD



värde

ed 50

# 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



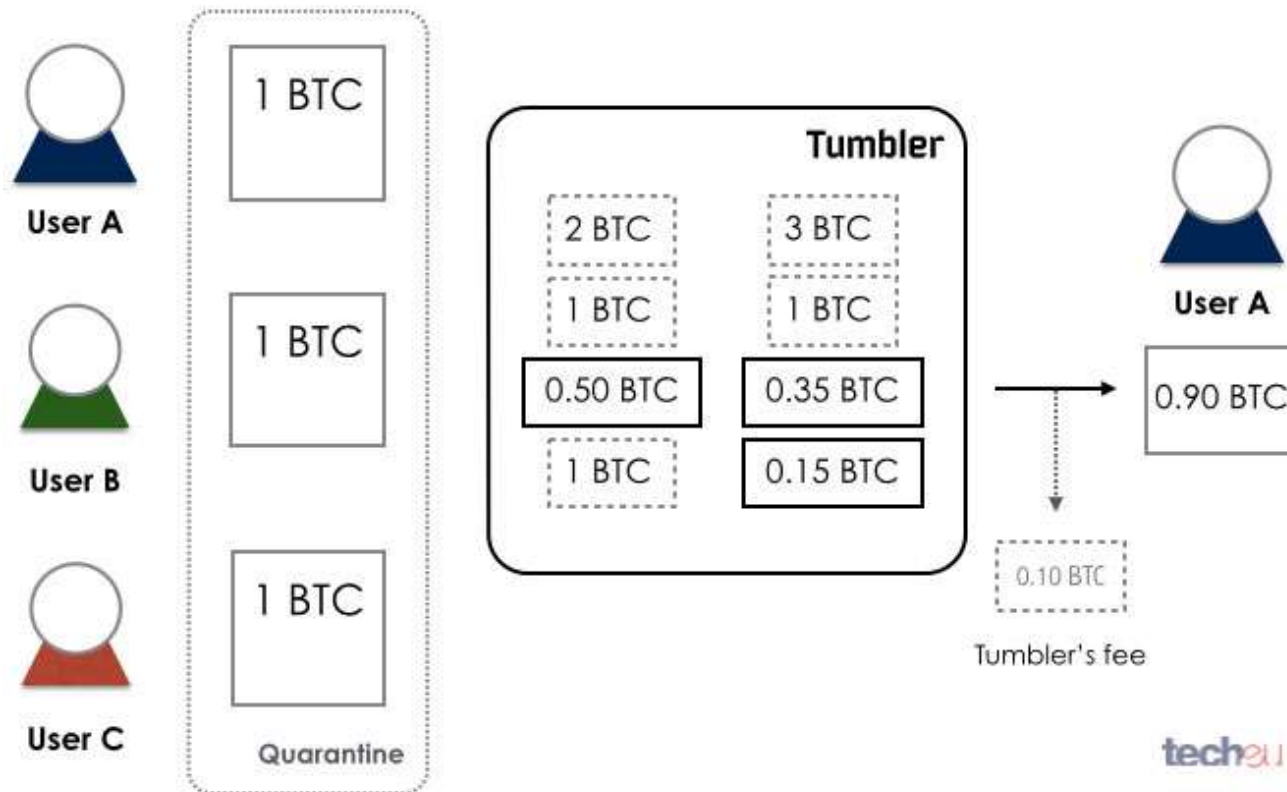
# Bitcoin dominerar, men hur länge till?



coinmarketcap.com

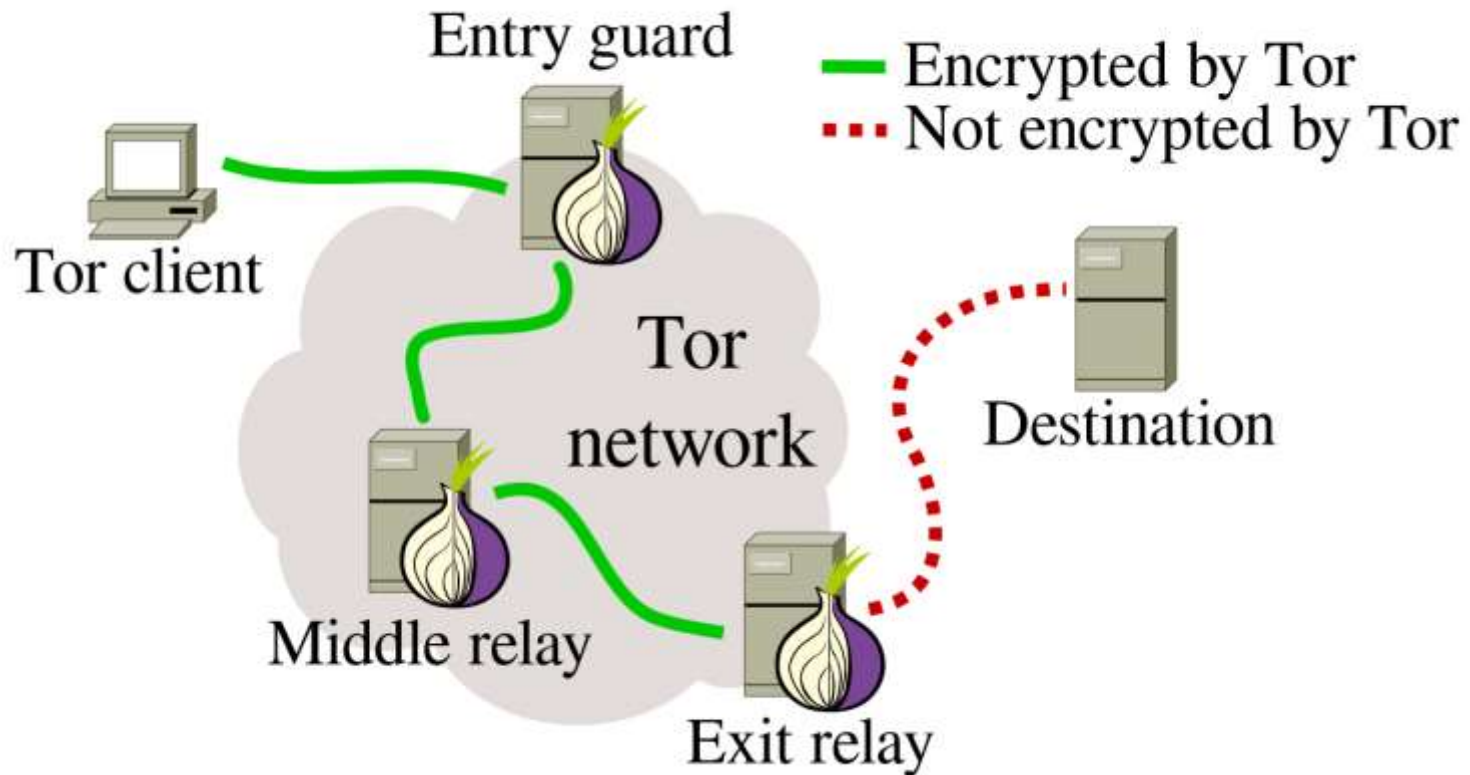


# Bitcoin-tumbler: Sopar igen spåren



tech2U

# Tor: anonym routing



# Darknet Market (DNM)



messages 0 | orders 0 | account \$0.00

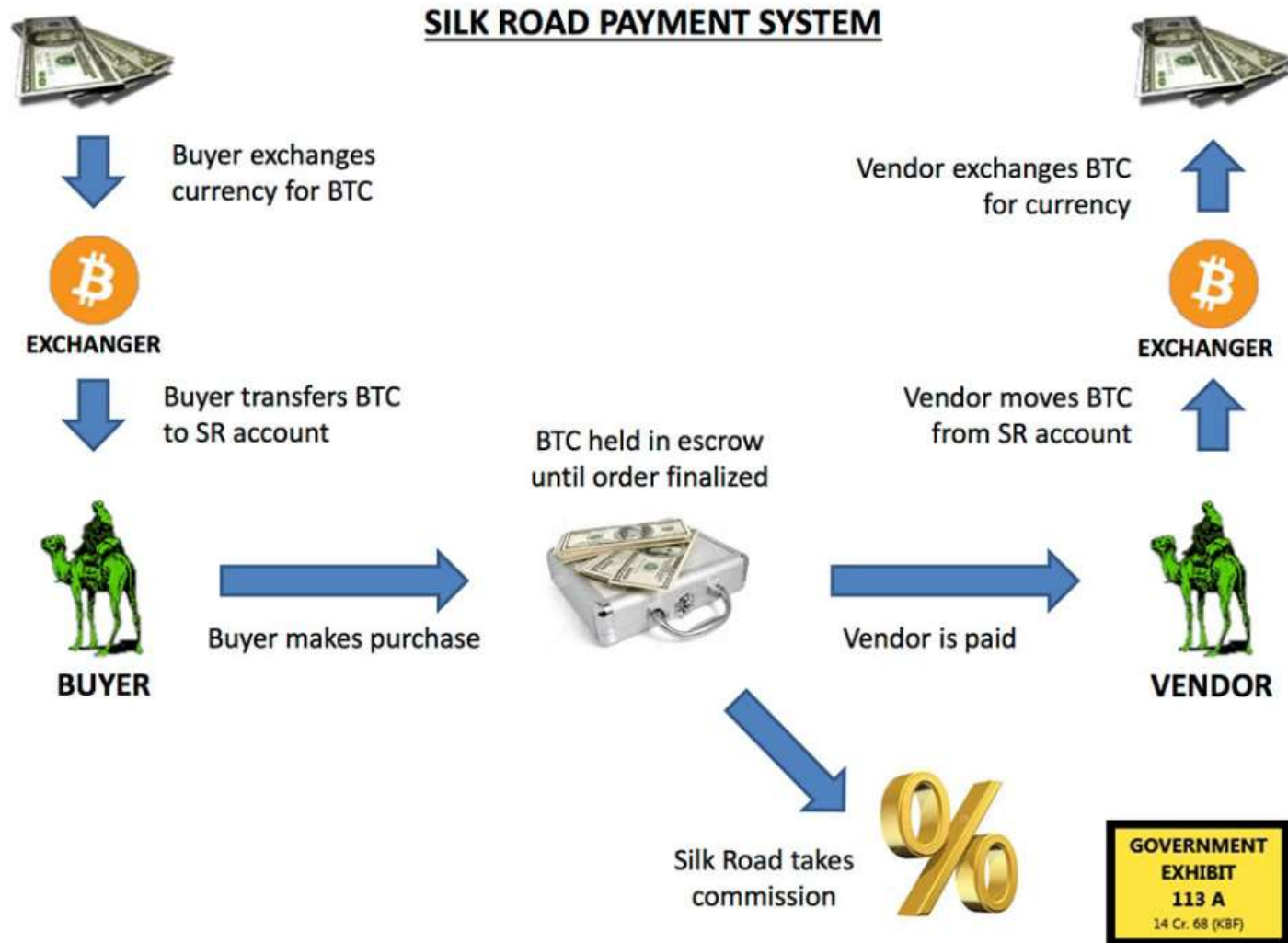
Search

- Drugs 486
  - Cannabis 82
  - Dissociatives 18
  - Ecstasy 64
  - Opioids 8
  - Other 15
  - Precursors 13
  - Prescription 92
  - Psychedelics 83
  - Stimulants 38
- Apparel 77
- Art 0
- Biotic materials 0
- Books 17
- Collectibles 0
- Computer equipment 4
- Custom Orders 1
- Digital goods 3
- Drug paraphernalia 35
- Electronics 3
- Erotica 0
- Forgeries 18
- Hardware 0
- Herbs & Supplements 0
- Jewelry 4
- Lab Supplies 1
- Lotteries & games 11
- Medical 0
- Money 4

## browsing drugs

item	
	0,7g Hydroponically Grown Crystal Cloud (LIMITED TIME OFFER!!)
	7g (1/4oz) P.Cubensis Powder
	Methadone hydrochloride - 250mg pure (min 90%) crystalline powder

# Pengafloödet i DNM



# Silk Road: Den mest kända DNM

- Grundades i januari 2011
- Gick att hitta på tor-adressen [silkroad6ownowfk.onion](http://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 beslagtogs 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: 48  
Merit: 0

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
- ...

# 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 narkotikabrott

# Katt-och-rätta-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



# Kryptovirus: Lukrativt för bedragarna



**Ooops, your files have been encrypted!** English

**What Happened to My Computer?**  
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

**Payment will be raised on**  
5/16/2017 00:47:55  
Time Left  
02:23:57:37

**Your files will be lost on**  
5/20/2017 00:47:55  
Time Left  
06:23:57:37

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)

**Send \$300 worth of bitcoin to this address:**  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

# 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



- 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.





# 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 webbläsare för att gräva
- XMR accepteras numera av flera DNM
- 2017: Första ransomware med XMR
- Troligt att XMR kommer öka betydligt



A Crypto Miner  
for your Website

# 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

## 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](mailto:jonathan.jogenfors@sectra.com)

# SECTRA

*Knowledge and passion*

**Jonathan Jogenfors**

Research Manager  
[jonathan.jogenfors@sectra.com](mailto:jonathan.jogenfors@sectra.com)