Digitala valutor - Mer än bara Bitcoin!

Jonathan Fors

jonathan.fors@liu.se
http://people.isy.liu.se/icg/jonfo33/

Institutionen för Systemteknik
Linköpings Universitet
2014-02-11

LiU expanding reality

Digitala valutor är en het potatis

Jag vill väcka intresse för digitala valutor

Hur fungerar Bitcoin?

Vad gör dem så användbara?

Hur ser framtiden ut?

Jag är doktorand i informationskodning

Civilingenjör i Teknisk Fysik här från LiU

Doktorand sedan 2012

Handledare: Jan-Åke Larsson

Kvantmekanik, kvantkryptering

Kryptografi och informationssäkerhet

Först och främst ingenjör, varken ekonom eller jurist.

Jag är doktorand i informationskodning

Civilingenjör i Teknisk Fysik här från LiU

Doktorand sedan 2012

Handledare: Jan-Åke Larsson

Kvantmekanik, kvantkryptering (men snäll mot katter)

Kryptografi och informationssäkerhet

Först och främst ingenjör, varken ekonom eller jurist.

Digitala valutor är inte virtuella valutor!

Bitcoin har väldigt lite gemensamt med 90-talets ”virtuella” valutor.

1998-2001

1994-2001

2009-2012

Varför var dessa så dåliga?

Varför är gamla tiders virtuella valutor så dåliga?

Centralisering: Vi måste lita på ett företag som centralbank. Detta företag kan ge ut nya pengar bäst det vill.

Alla pengar styrs från en stor server - Vad händer om den hackas?

Det spelar ingen roll hur säker den servern blir, det är helt enkelt ett för attratrivt mål.

Hur ska man få tillit till systemet?

Låt oss skippa centralbanken

Den revolutionerande idén: Distribuerad valuta.

Ingen kan ”starta sedelpressen” och orsaka inflation.

Men hur fungerar en distribuerad valuta?

Svaret: Ett system som garanteras av kryptografi.

Man behöver inte lita på någon, varken utgivaren eller de man handlar med.

Digital information med monetärt värde?

$= \$$

En fil kan kopieras - kopieras då också pengarna?

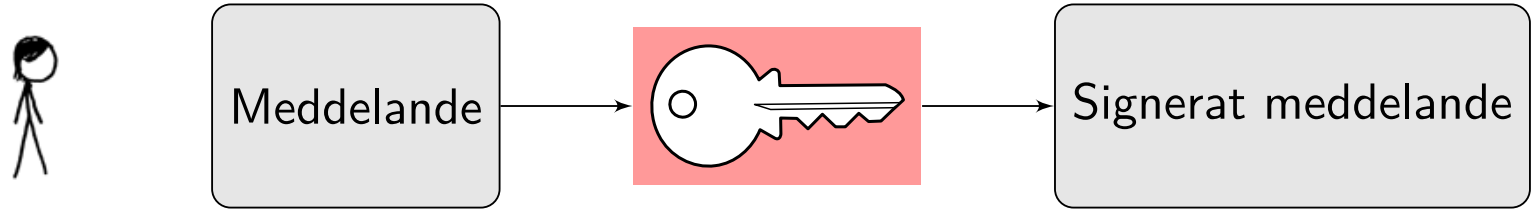
Digital information med monetärt värde?

= $

= $$$??

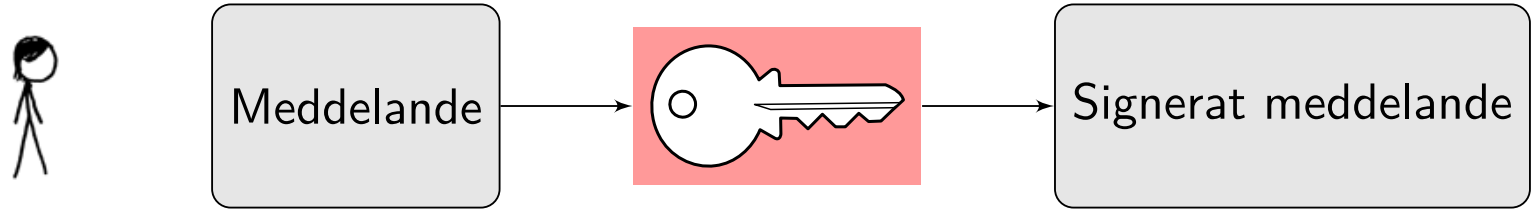
En fil kan kopieras - kopieras då också pengarna?

Publika nycklar möjliggör digitala signaturer

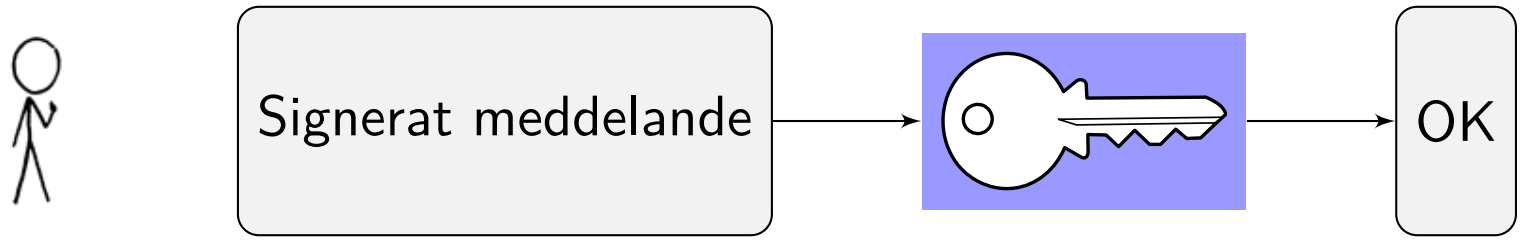


Alice signerar med sin privata nyckel

Publika nycklar möjliggör digitala signaturer

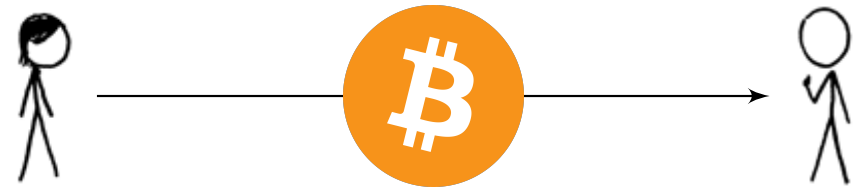


Alice signerar med sin privata nyckel



Bob verifierar med Alices publika nyckel

Alice kan publicera signerade transaktioner



"Jag, Alice, skickar en peng till Bob"

Bob kan se på signaturen att pengarna kommer från Alice.

Alice kan inte ändra sig och senare säga "Nej, jag skickade aldrig dessa pengar".

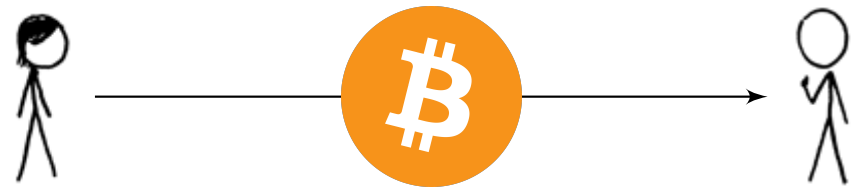
Serienummer gör varje peng unik

Problem: Alice kan skicka pengar till Bob hur många gånger som helst.

Serienummer gör varje peng unik

Problem: Alice kan skicka pengar till Bob hur många gånger som helst.

Lösning: Serienummer.

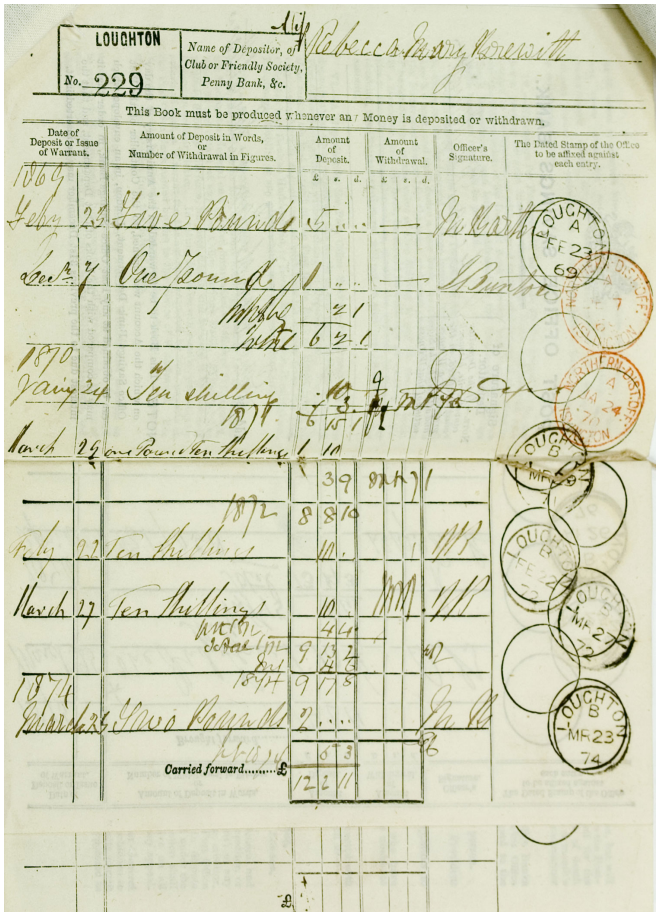


"Jag, Alice, skickar en peng nummer 163829 till Bob"

Alice kan inte spendera samma peng flera gånger.

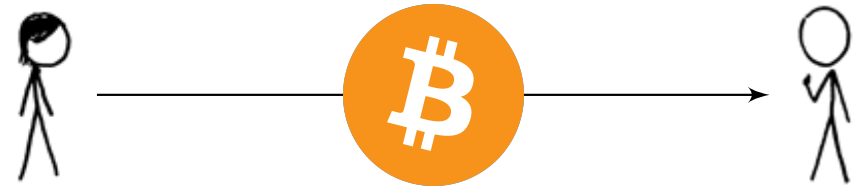
Men nu måste vi ha ett robust system som hanterar serienummer.

Vi inför en ”blockkedja” som innehåller alla transaktioner



Likt en liggare med bokföring vet blockkedjan allt

Bob kollar blockkedjan

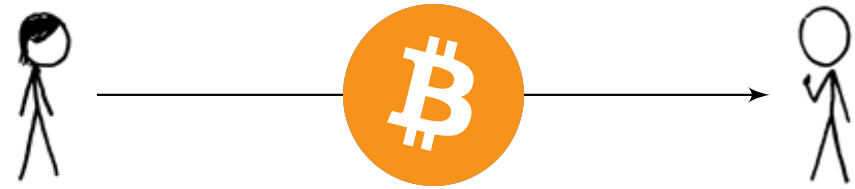


"Jag, Alice, skickar peng nummer 163829 till Bob"

Bob ser i blockkedjan att peng 163829 tillhör Alice.

Både Alice och Bob måste inneha varsin kopia av blockkedjan (den kan vara ganska stor)

Bob kollar blockkedjan



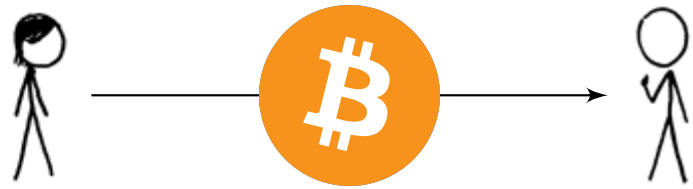
"Jag, Alice, skickar peng nummer 163829 till Bob"

Bob ser i blockkedjan att peng 163829 tillhör Alice.

Både Alice och Bob måste inneha varsin kopia av blockkedjan (den kan vara ganska stor)

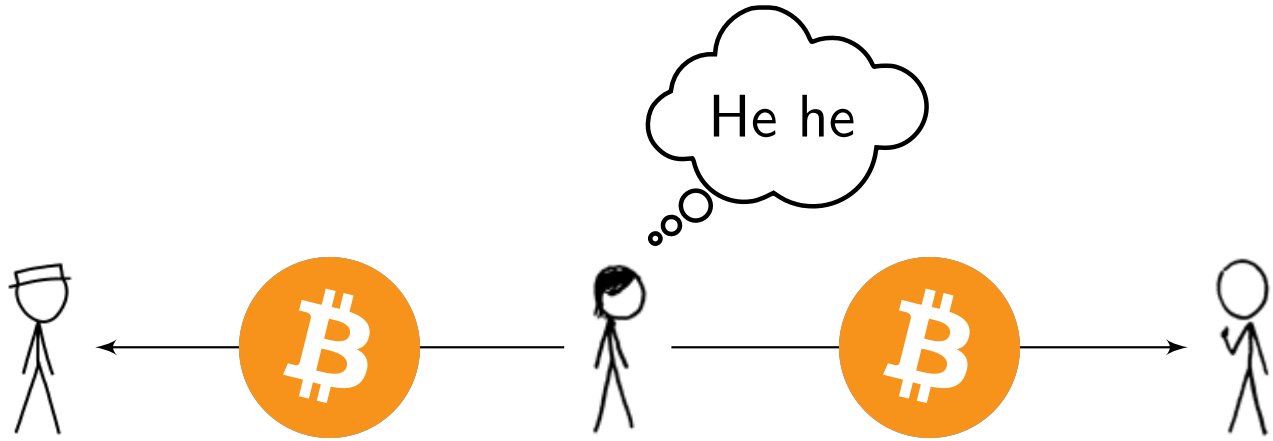
Tyvärr kan Alice fortfarande fuska. . .

Bob måste kontrollera att pengarna verkligen tillhör Alice



”Hm. . . Alices transaktion verkar vara giltig.”

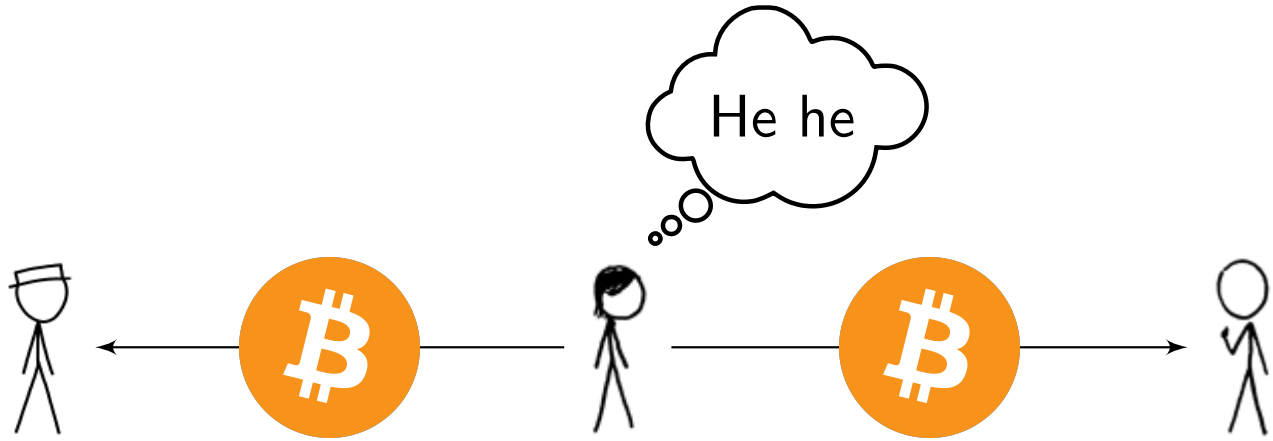
Bob måste kontrollera att pengarna verkligen tillhör Alice



”Hm. . . Alices transaktion verkar vara giltig.”

Det Bob dock inte vet är att Alice samtidigt överför *samma peng* till Charlie.

Bob måste kontrollera att pengarna verkligen tillhör Alice

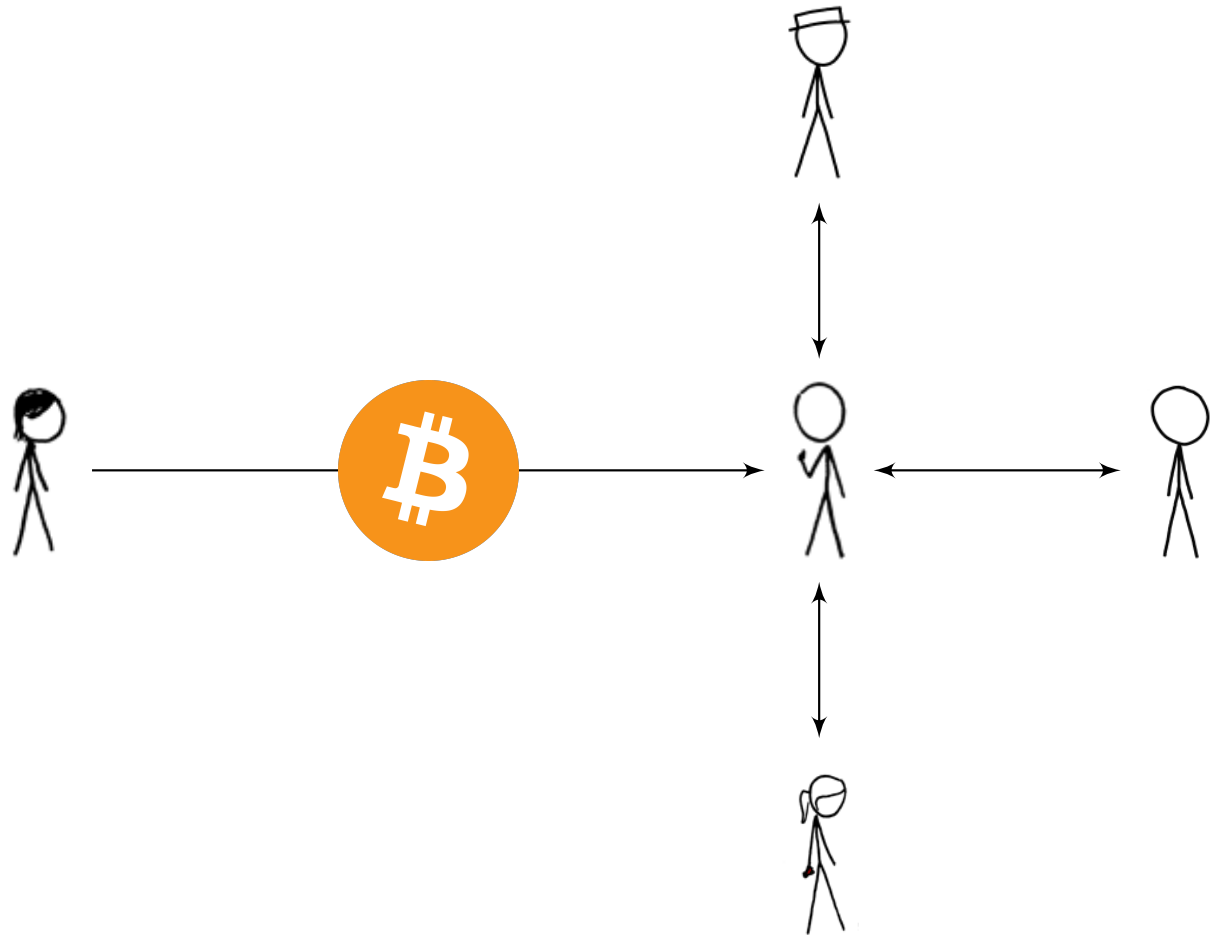


”Hm. . . Alices transaktion verkar vara giltig.”

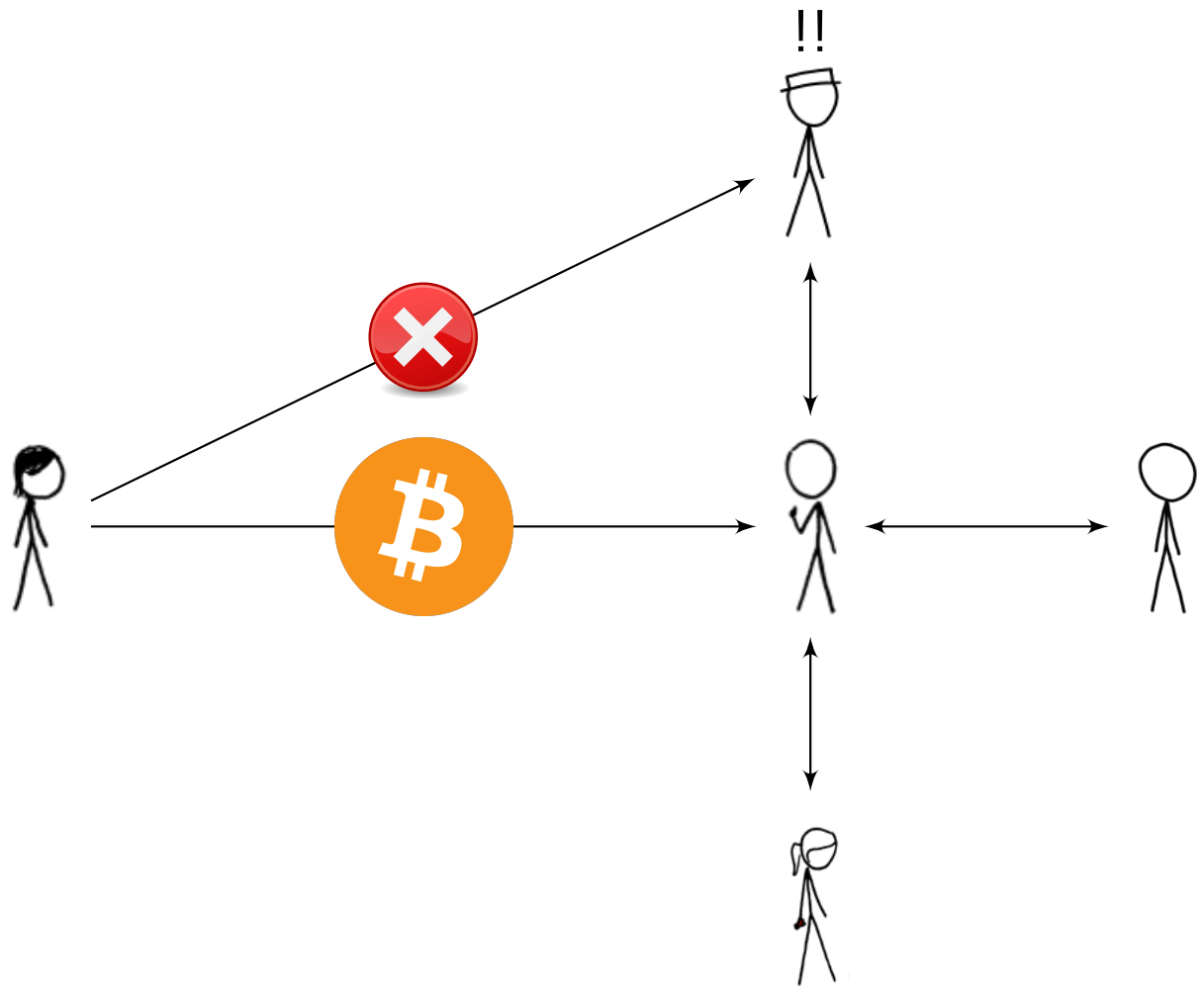
Det Bob dock inte vet är att Alice samtidigt överför *samma peng* till Charlie.
Samtidighet är något som inte existerar i distribuerade system!

I stället låter vi Bob fråga nätverket

I stället låter vi Bob fråga nätverket

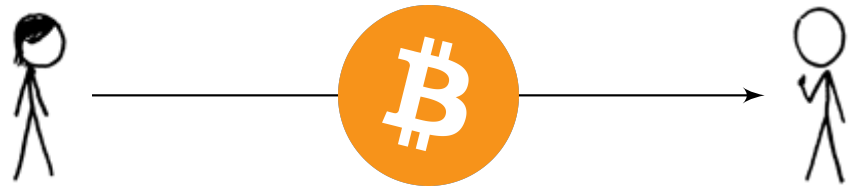


I stället låter vi Bob fråga nätverket

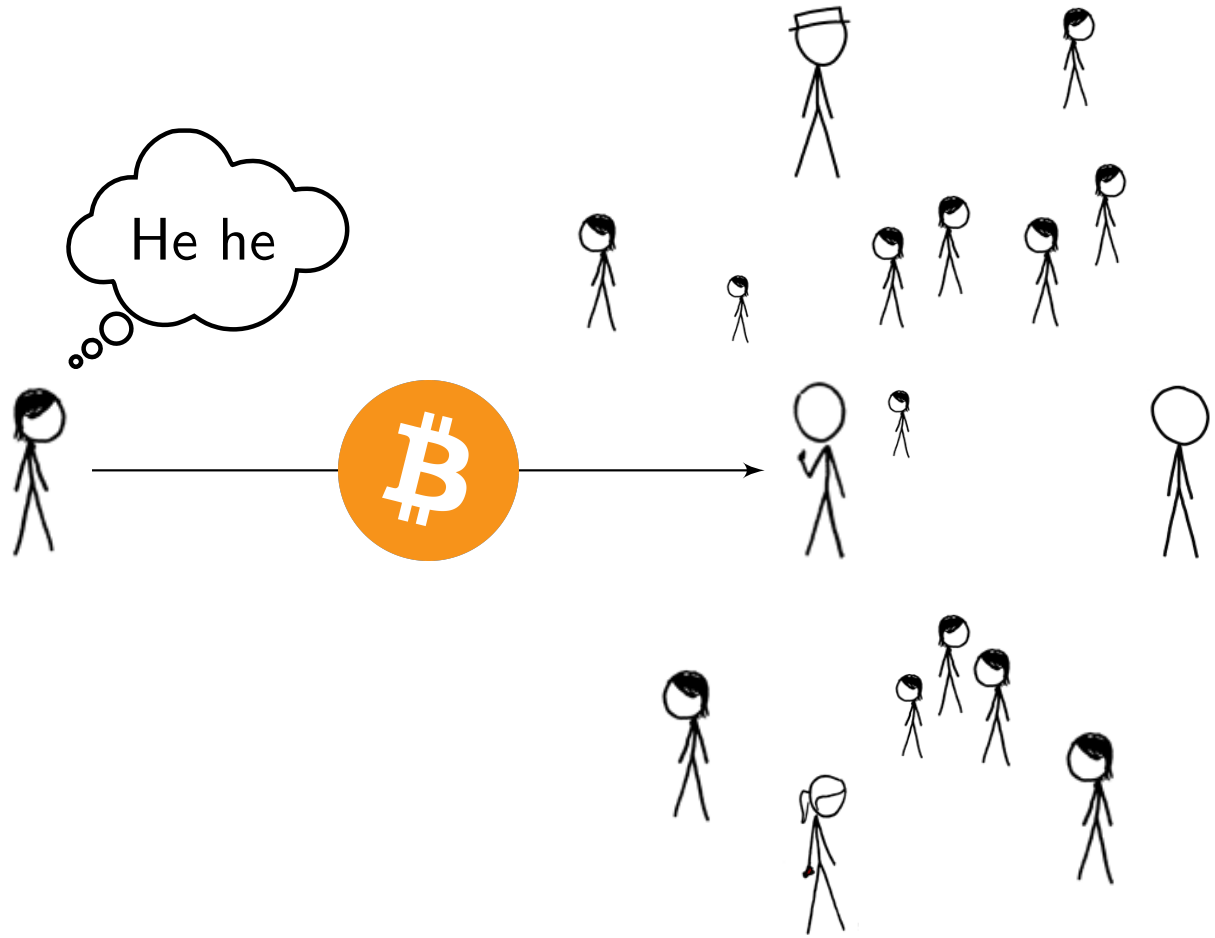


Charlie märker att pengen redan är spenderad

Alice kan luras med ett botnet



Alice kan luras med ett botnet



Hur ska Bob göra nu?

Måste bli dyrt att bekräfta transaktioner

Alice kan fylla nätverket med falska noder.

Samma problem som för e-post, det är *för enkelt* att delta.

Lösning: *Proof of work.*

Måste bli dyrt att bekräfta transaktioner

Alice kan fylla nätverket med falska noder.

Samma problem som för e-post, det är *för enkelt* att delta.

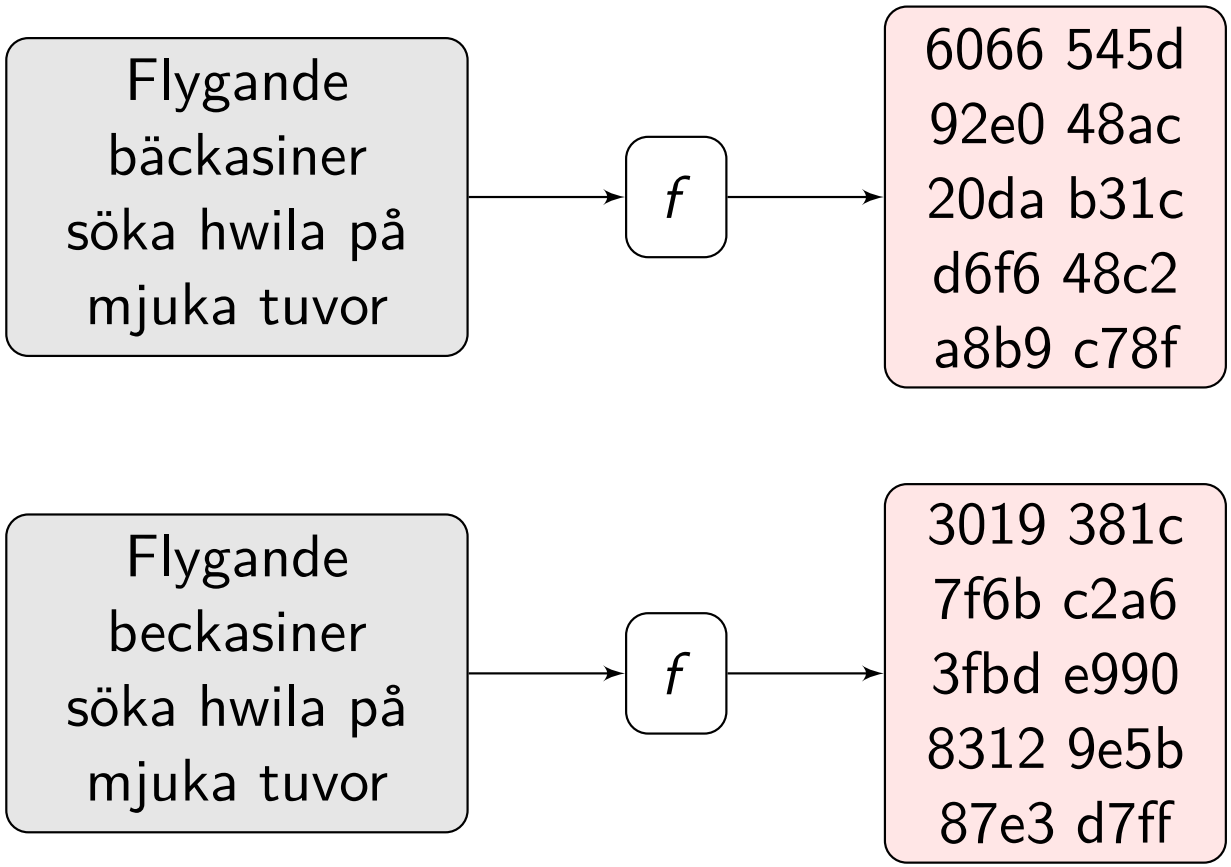
Lösning: *Proof of work.*

Idé: Skapa ett problem med följande egenskaper:

- Svårt att hitta en lösning
- Enkelt att verifiera en lösning

och låt de som verifierar lösa detta problem.

Hashfunktioner är en grundbult i kryptografin



Små skillnader ger totalt annorlunda hashvärde

En bra hashfunktion är svårt att reversera

Givet ett hashvärde, vilket meddelande var det som hashades?

Det finns inget sätt att veta, så man får testa alla kombinationer!
Exempel på hashfunktioner:

Namn	Status	Säker?
`md5`	Mycket vanlig.	Inte längre.
`sha256`	Snabb.	Förmodligen
`scrypt`	Minnesintensiv	Okänt.

Packa ihop en massa transaktioner till block

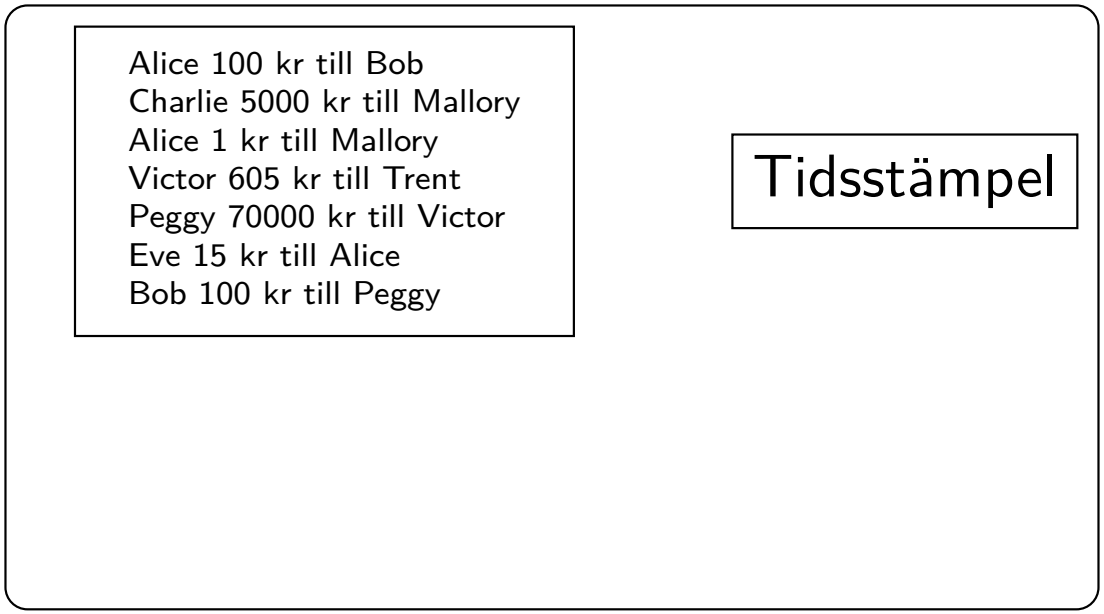
Alice 100 kr till Bob
Charlie 5000 kr till Mallory
Alice 1 kr till Mallory
Victor 605 kr till Trent
Peggy 70000 kr till Victor
Eve 15 kr till Alice
Bob 100 kr till Peggy

Packa ihop en massa transaktioner till block

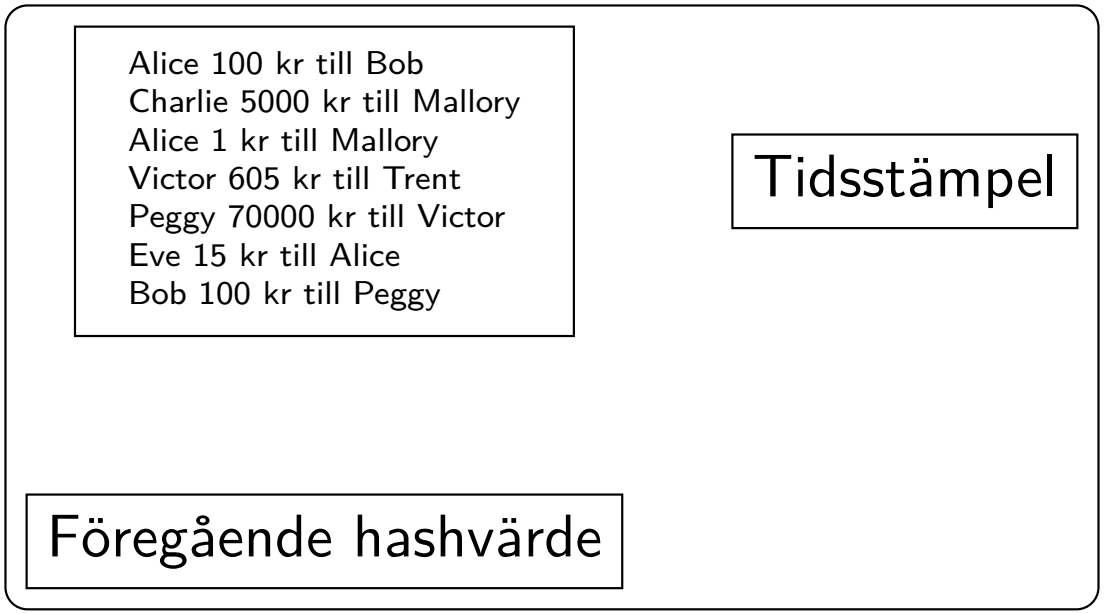
Alice 100 kr till Bob
Charlie 5000 kr till Mallory
Alice 1 kr till Mallory
Victor 605 kr till Trent
Peggy 70000 kr till Victor
Eve 15 kr till Alice
Bob 100 kr till Peggy

Tidsstämpel

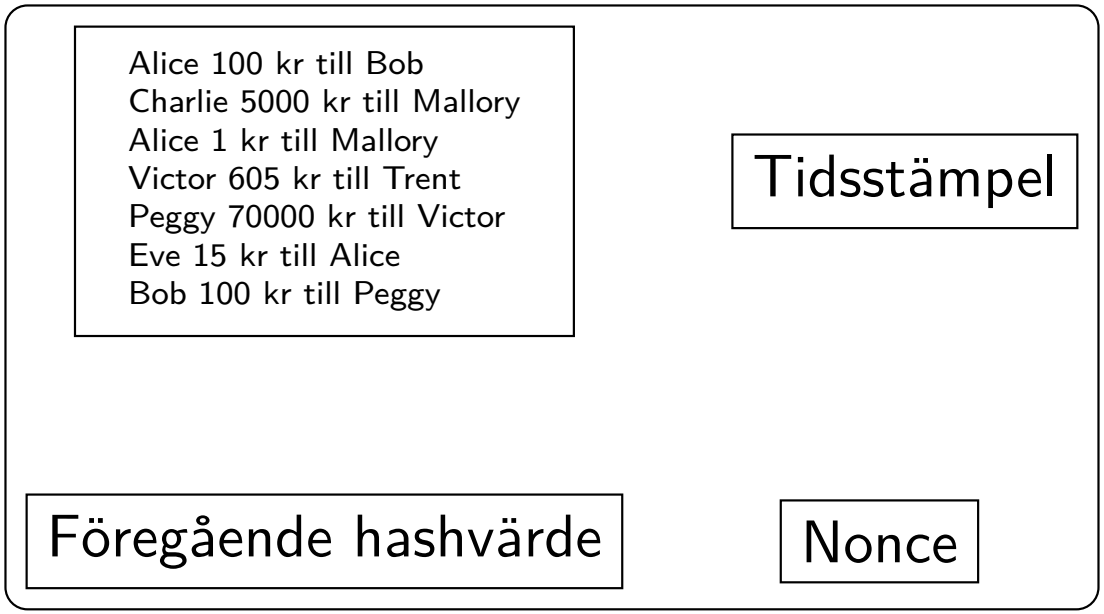
Packa ihop en massa transaktioner till block



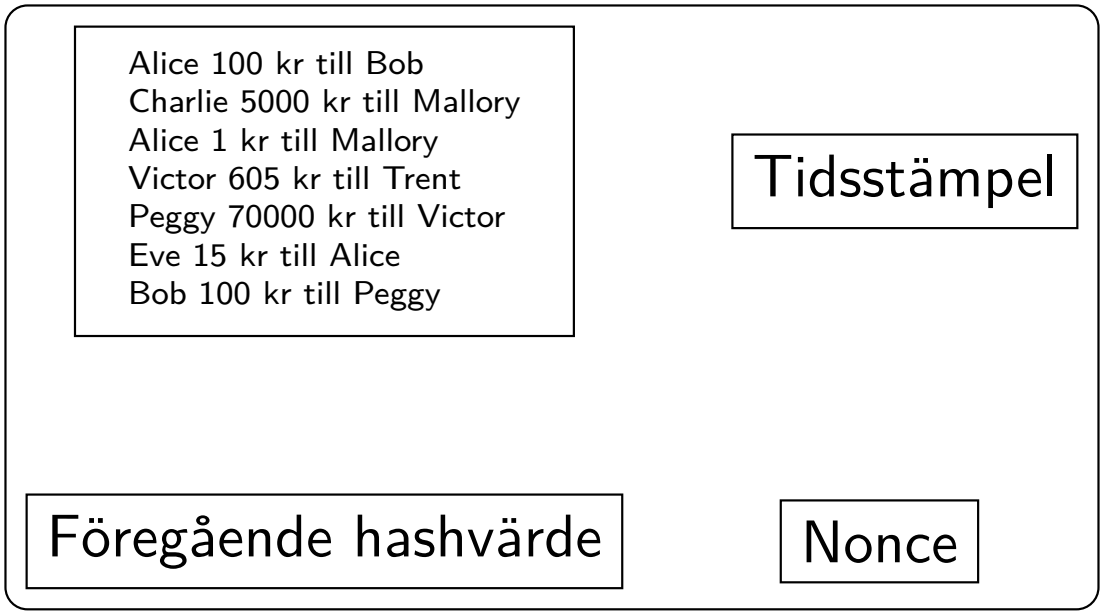
Packa ihop en massa transaktioner till block



Packa ihop en massa transaktioner till block



Packa ihop en massa transaktioner till block



Vi testar olika nonce-värden och beräknar hashvärdet av hela blocket

Proof of work

Vi vill ha ett hashvärde som börjar med ett visst antal nollor (ex. fem).

Testa olika nonce-värden och beräkna hashvärdet.

Nonce	Blockets hashsumma
0	802dbe2e69...

Proof of work

Vi vill ha ett hashvärde som börjar med ett visst antal nollor (ex. fem).

Testa olika nonce-värden och beräkna hashvärdet.

Nonce	Blockets hashsumma
0	802dbe2e69...
1	bbfce0d522...

Proof of work

Vi vill ha ett hashvärde som börjar med ett visst antal nollor (ex. fem).

Testa olika nonce-värden och beräkna hashvärdet.

Nonce	Blockets hashsumma
0	802dbe2e69...
1	bbfce0d522...
2	7bb4db476f...

Proof of work

Vi vill ha ett hashvärde som börjar med ett visst antal nollor (ex. fem).

Testa olika nonce-värden och beräkna hashvärdet.

Nonce	Blockets hashsumma
0	802dbe2e69...
1	bbfce0d522...
2	7bb4db476f...
...	...
770239	00000921ac...

Proof of work

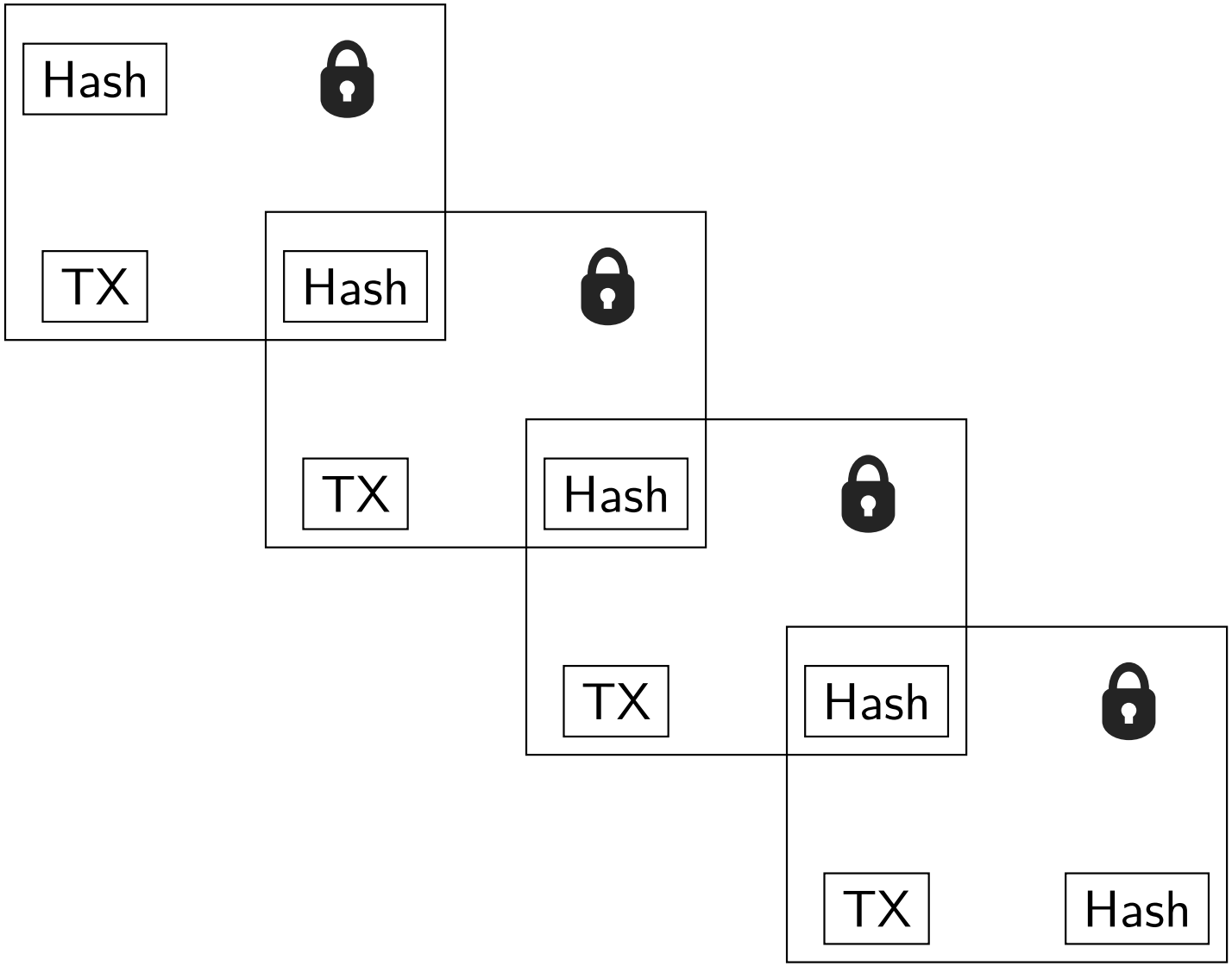
Vi vill ha ett hashvärde som börjar med ett visst antal nollor (ex. fem).

Testa olika nonce-värden och beräkna hashvärdet.

Nonce	Blockets hashsumma
0	802dbe2e69...
1	bbfce0d522...
2	7bb4db476f...
...	...
770239	00000921ac...

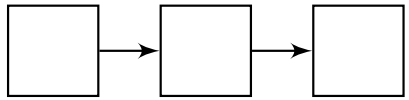
Det tog oss nästan en miljon hashningar att hitta en lösning!

Blocken bildar en lång kedja

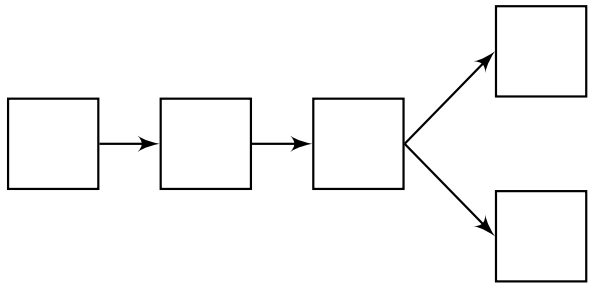


Varje nytt block ger säkerhet till de tidigare

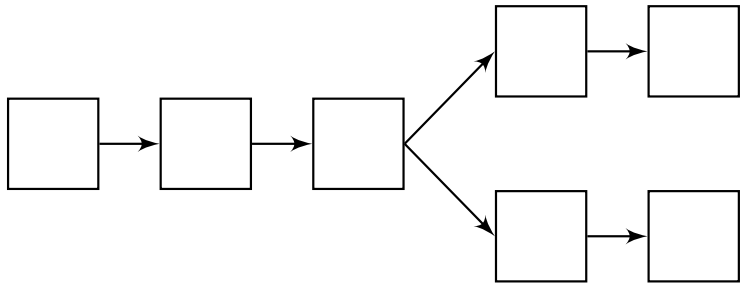
Efter ett antal nya block har vi bekräftelse



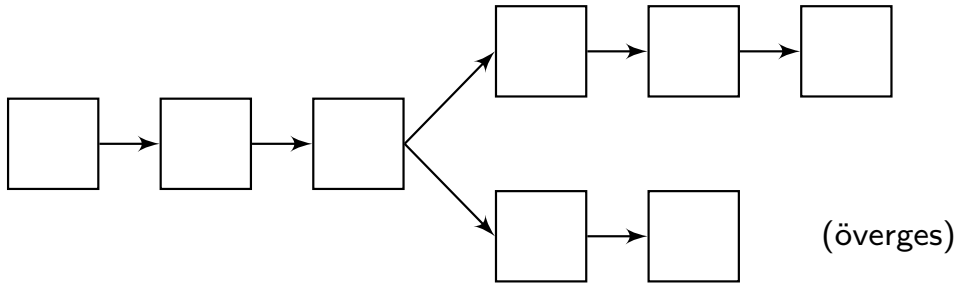
Efter ett antal nya block har vi bekräftelse



Efter ett antal nya block har vi bekräftelse

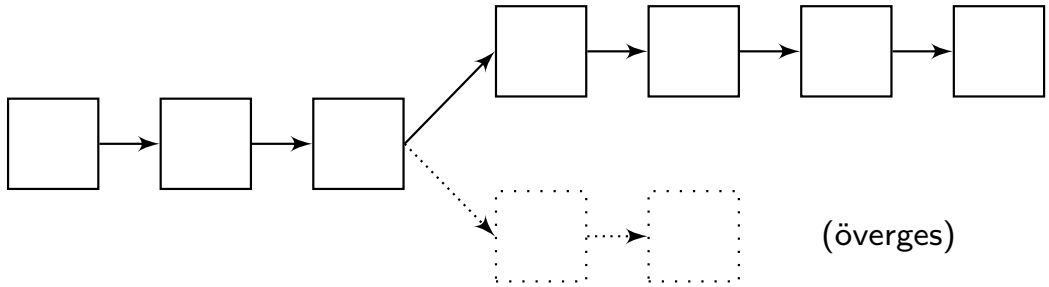


Efter ett antal nya block har vi bekräftelse



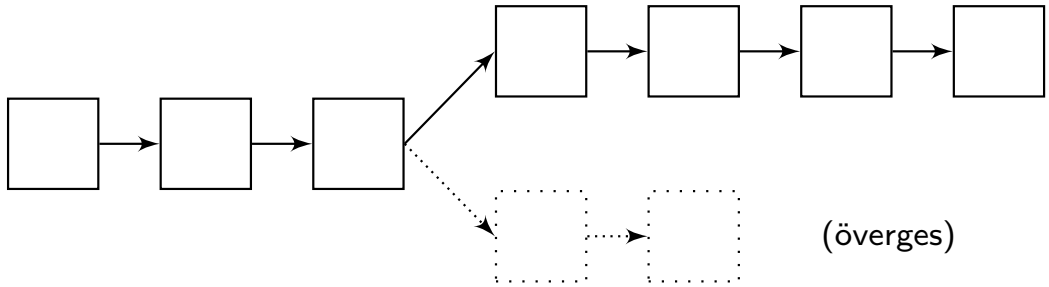
Om flera block hittas samtidigt väljs den längsta grenen.

Efter ett antal nya block har vi bekräftelse

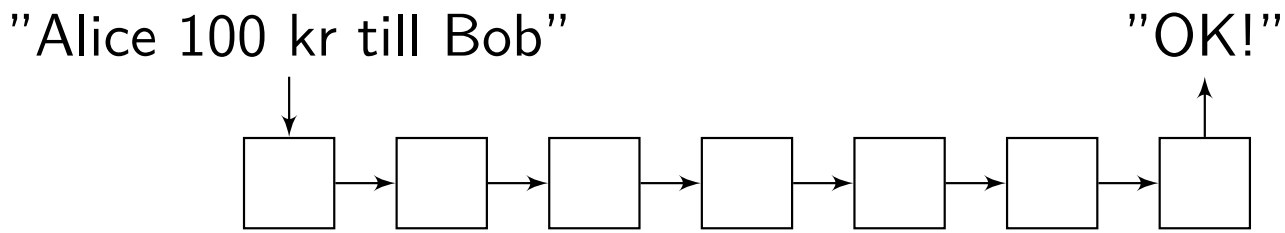


Om flera block hittas samtidigt väljs den längsta grenen.

Efter ett antal nya block har vi bekräftelse



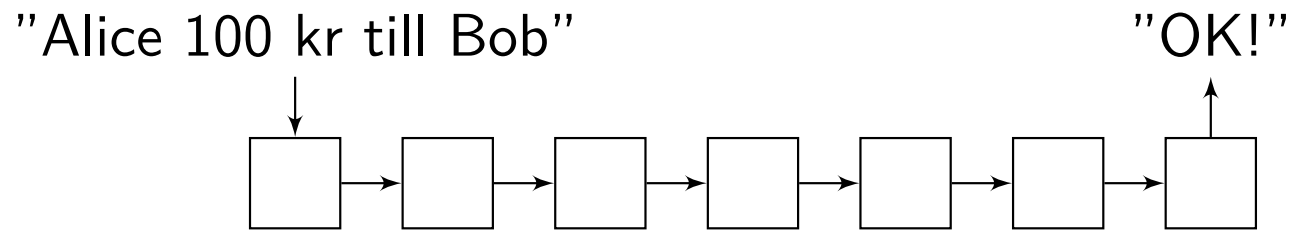
Om flera block hittas samtidigt väljs den längsta grenen.



Vi väntar tills vårt block följs av sex nya block för att vara säkra på att vår transaktion inte överges.

Det är nu mycket svårt att fuska

För att lura Bob måste Alice gräva fram sex block i rad. Detta görs i konkurrens med hela nätverket.

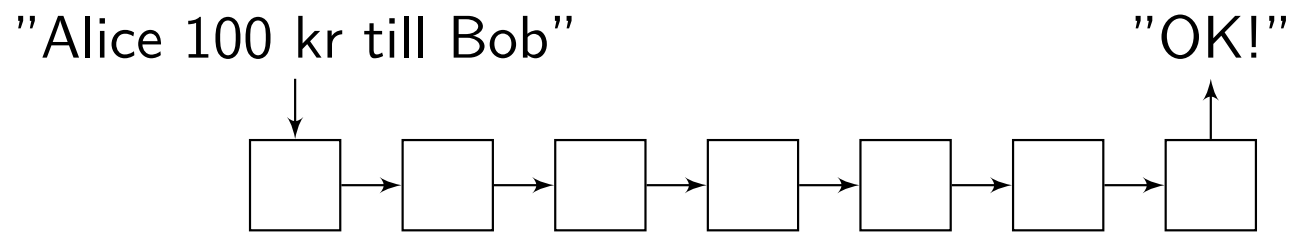


Med 1% av datorkraften är chansen att lyckas mindre än $\left(\frac{1}{100}\right)^6 \approx 10^{-12}$.

En person som har mer datorkraft än resten av världen kan dock göra vad han eller hon vill.

Det är nu mycket svårt att fuska

För att lura Bob måste Alice gräva fram sex block i rad. Detta görs i konkurrens med hela nätverket.



Med 1% av datorkraften är chansen att lyckas mindre än $\left(\frac{1}{100}\right)^6 \approx 10^{-12}$.

En person som har mer datorkraft än resten av världen kan dock göra vad han eller hon vill. (Mer om grävande senare i föredraget)

Nu har vi sett hur transaktioner går till

Liggaren (blockchain) visar allas saldon

Transaktioner verifieras med proof-of-work.

Transaktioner är irreversibla (på gott och ont)

Vi ska titta mer på grävande (mining) andra timmen.

Låt oss titta på exemplet Bitcoin

Det vi lärt oss hittils gäller för alla digitala valutor.

Mer än bara Bitcoin!

Bitcoin med stor bokstav = protokollet
bitcoin med liten bokstav = valutan

Transaktioner är snabba, säkra och enkla

Adress: `1CJYpahGsQmfQCVNzKegTTmML4iTjT8h9E`

Robust format, går inte att skicka till felaktig adress.

Måste vänta minst sex bekräftelser.

QR-koder passar som hand i handske.

Det enda som behövs är en textsträng

En skylt på ESPN gav 24 000 USD

Vem skapade bitcoin?

Satoshi Nakamoto publicerade en whitepaper i november 2008.

Efter publikationen följde den officiella klienten, och det första blocket grävdes fram i Januari 2009.

Vem skapade bitcoin?

Satoshi Nakamoto publicerade en whitepaper i november 2008.

Efter publikationen följde den officiella klienten, och det första blocket grävdes fram i Januari 2009.

Ingen vet vem han/de är, och har inte synts till sedan mitten av 2010

Analyser har visat att han förmodligen bor i samma tidszon som östra USA.

Bitcoin uppfanns 2008

November 2008 Whitepaper

Bitcoin uppfanns 2008

November 2008	Whitepaper
Januari 2009	Genesis-blocket skapas

Bitcoin uppfanns 2008

November 2008	Whitepaper
Januari 2009	Genesis-blocket skapas
Oktober 2009	1309 XBT = 1 USD
Maj 2010	Första pizzaköpet (10 000 XBT = 25 USD)

Bitcoin uppfanns 2008

November 2008	Whitepaper
Januari 2009	Genesis-blocket skapas
Oktober 2009	1309 XBT = 1 USD
Maj 2010	Första pizzaköpet (10 000 XBT = 25 USD)
Februari 2011	1 XBT = 1 USD

Bitcoin uppfanns 2008

November 2008	Whitepaper
Januari 2009	Genesis-blocket skapas
Oktober 2009	1309 XBT = 1 USD
Maj 2010	Första pizzaköpet (10 000 XBT = 25 USD)
Februari 2011	1 XBT = 1 USD
November 2013	1 XBT = 1100 USD följt av krash
December 2013	Kapiton-skandalen
Januari 2013	1 XBT = 800 USD
Februari 2013	Mt. Gox får problem
Idag	1 XBT = 700 USD

De senaste veckans turbulens och Mt. Gox

Mt. Gox: Många tekniska problem genom åren, men sedan någon vecka kan man inte längre ta ut sina bitcoin.

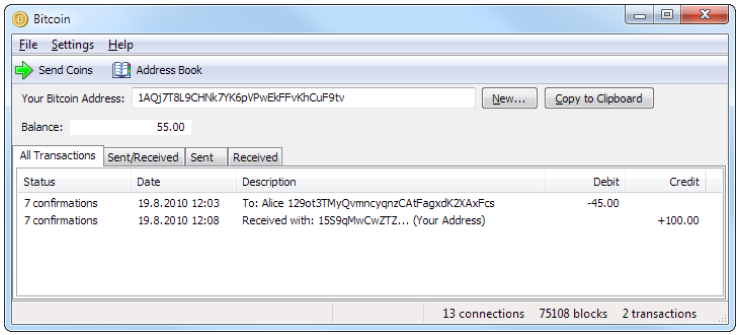
Missnöjet grodde medan Mt. Gox länge teg, tills de härom dagen gick ut och skyllde ifrån sig och påstod att felen låg i Bitcoin-protokollet

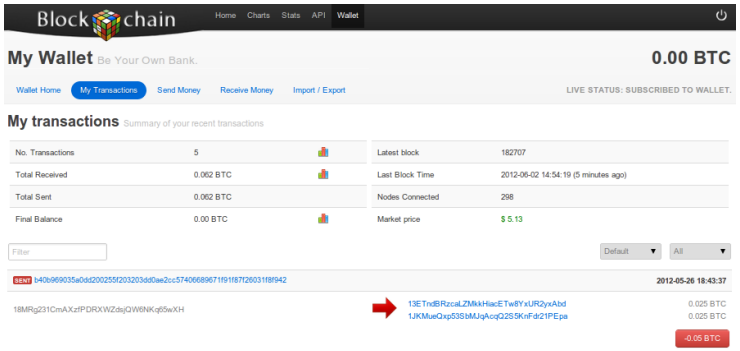
Beskyllningen är rent trams och hänvisar till ett fenomen som är känt och fixat sedan tre år.

Fortfarande tar man emot betalningar. Använd inte Mt. Gox!

Hur använder jag bitcoin?

Skaffa en plånbok





Alla parter i nätverket måste ha den fullständiga blockkedjan.

Idag består den av 285000 block och är 14 gigabyte stor.

Det är enkelt att köpa bitcoin

- Köpa från växlingsföretag.
- Bitcoin-bankomat i Stockholm
- Köpa kontant via localbitcoins.
- Mining (svårt)

Idag, 11 februari: 1 XBT $\approx$ 4500 SEK. Obs: Digitala valutor är (nästan) oändligt delbara.

. . . men var först noga med säkerheten

Det finns många som blivit av med sina bitcoin.

En fil på datorn värd mer än datorn själv?
Aldrig tidigare har datasäkerhet varit så vikigt!

Digitala valutor medför nya risker som aldrig tidigare funnits inom informationssäkerhet.

Plånboken innehåller din privata nyckel.

Hoppsan, hårddisken dog!

Kan man få tillbaka sina pengar?

Hoppsan, hårddisken dog!

Kan man få tillbaka sina pengar?

Nej. Digitala valutor är ju decentraliserade.

Skydd: Se till att ha backuper.

Hoppsan, hårddisken dog!

Kan man få tillbaka sina pengar?

Nej. Digitala valutor är ju decentraliserade.

Skydd: Se till att ha backuper. Flera stycken!

Obehörig får tag på nyckeln

Idag finns virus som letar efter digitala plånböcker.

Obehörig får tag på nyckeln och flyttar bort pengarna.

Transaktioner är irreversibla.

Skydd:

- Långa lösenord
- Tvåfaktorautentisering (lösenord+dosa)
- Sunt föruft

Kalla plånböcker - ett smart skydd

Idé: Spara plånboken offline.

Gör QR-koder av nycklarna och skriv ut på papper.

Lagras i kassaskåp.

Heta plånböcker (online)

Ett annat sätt är att leja bort plånboken.

Fördelar:

- Smidigt
- Pengarna alltid tillgängliga.
- Ingen stor nedladdning behövs.
- Går att koppla till telefonen.

Heta plånböcker (online)

Ett annat sätt är att leja bort plånboken.

Fördelar:

- Smidigt
- Pengarna alltid tillgängliga.
- Ingen stor nedladdning behövs.
- Går att koppla till telefonen.

Nackdelar:

- Säkerhet!
- Vad händer om leverantören går i konkurs?

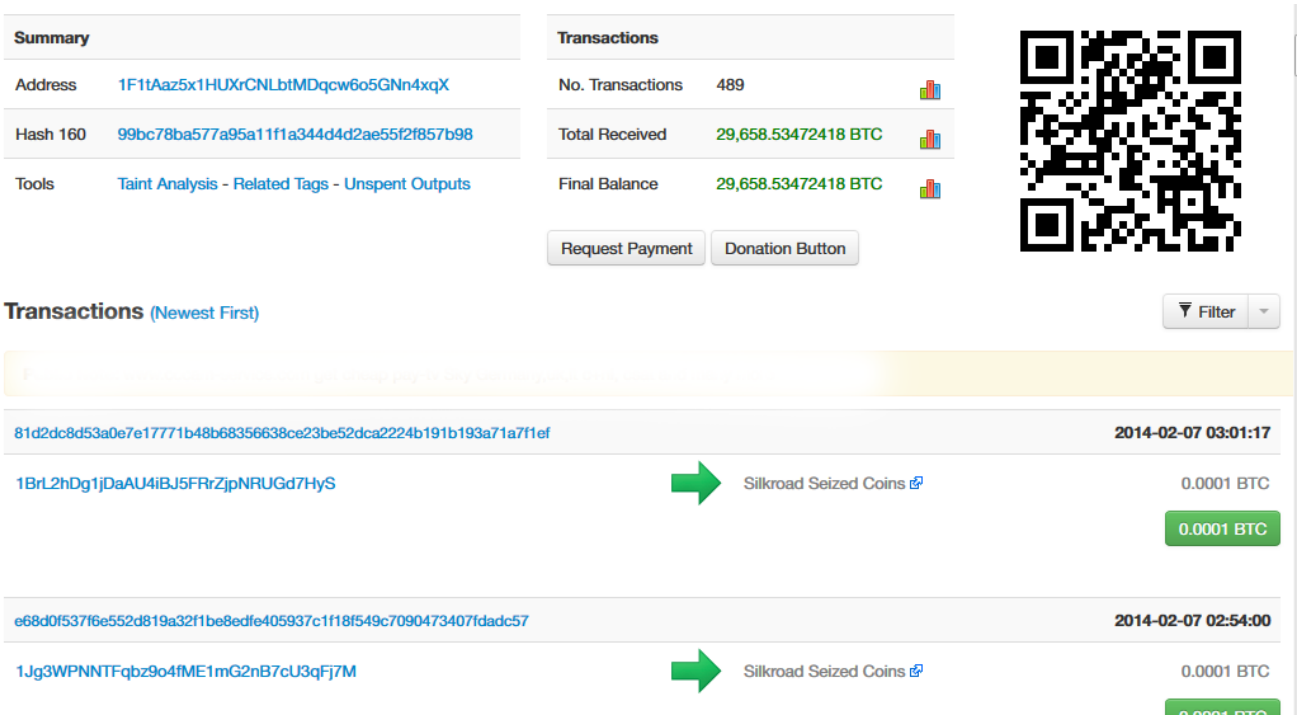
Handla med bitcoin?

Ett 20-tal ställen i Sverige accepterar bitcoin

Se coinmap.org

Jag vill kunna köpa lunch med bitcoin här i Linköping!

Allt som handlas blir offentligt



Summary	
Address	1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX
Hash 160	99bc78ba577a95a11f1a344d4d2ae55f2f857b98
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	489
Total Received	29,658.53472418 BTC
Final Balance	29,658.53472418 BTC

Request Payment | Donation Button

Transactions (Newest First) — Filter

81d2dc8d53a0e7e17771b48b68356638ce23be52dca2224b191b193a71a7f1ef — **2014-02-07 03:01:17**

1BrL2hDg1jDaAU4iBJ5FRrZjpNRUGd7HyS → Silkroad Seized Coins — 0.0001 BTC

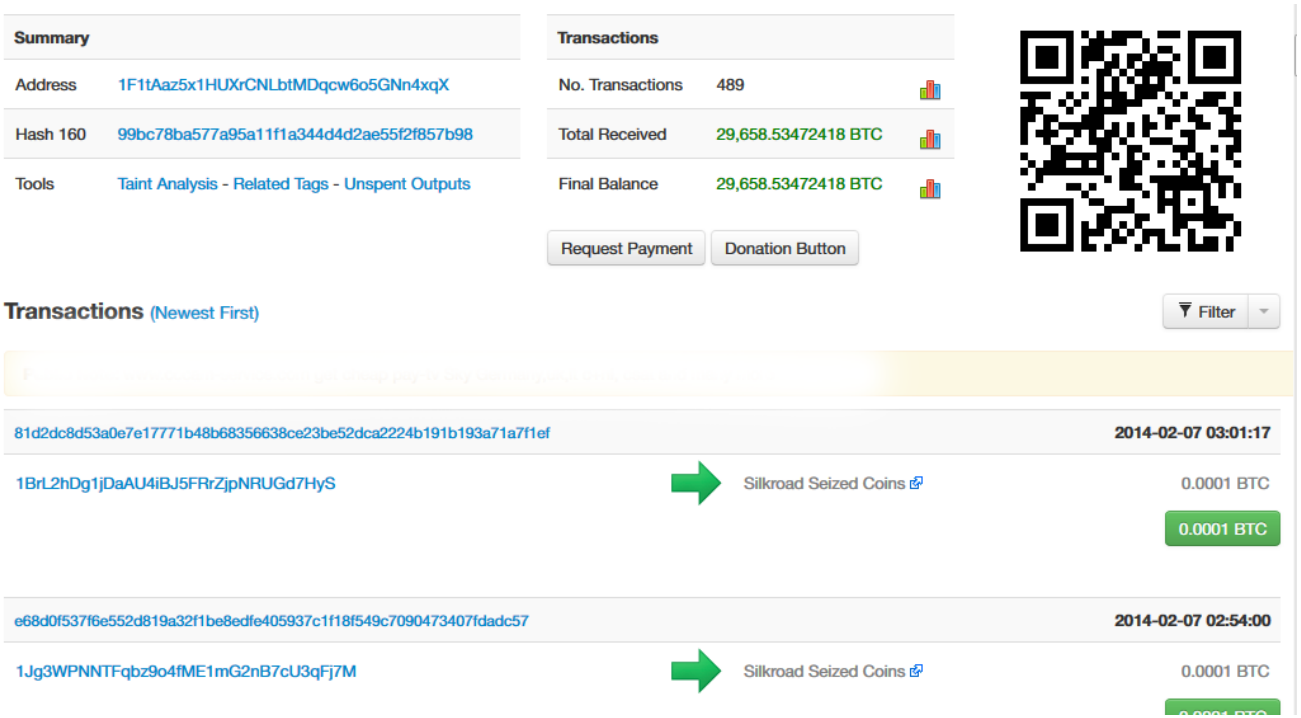
0.0001 BTC

e68d0f537f6e552d819a32f1be8edfe405937c1f18f549c7090473407fdadc57 — **2014-02-07 02:54:00**

1Jg3WPNNTFqbz9o4fME1mG2nB7cU3qFj7M → Silkroad Seized Coins — 0.0001 BTC

Denna adress tillhörde Silk Road innan den stängdes ned av FBI

Allt som handlas blir offentligt



Summary		Transactions	
Address	1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX	No. Transactions	489
Hash 160	99bc78ba577a95a11f1a344d4d2ae55f2f857b98	Total Received	29,658.53472418 BTC
Tools	Taint Analysis - Related Tags - Unspent Outputs	Final Balance	29,658.53472418 BTC

Request Payment | Donation Button

Transactions (Newest First) — Filter

81d2dc8d53a0e7e17771b48b68356638ce23be52dca2224b191b193a71a7f1ef			2014-02-07 03:01:17
1BrL2hDg1jDaAU4iBJ5FRrZjpNRUGd7HyS	→	Silkroad Seized Coins	0.0001 BTC
			0.0001 BTC
e68d0f537f6e552d819a32f1be8edfe405937c1f18f549c7090473407fdadc57			2014-02-07 02:54:00
1Jg3WPNNTFqbz9o4fME1mG2nB7cU3qFj7M	→	Silkroad Seized Coins	0.0001 BTC

Denna adress tillhörde Silk Road innan den stängdes ned av FBI

Ingen anonymitet!

Men hur kan en butik ta betalt i bitcoin?

Som butiksägare måste man skydda sig mot kurssvängningar.

Det går inte att vänta på sex bekräftelser.

Det finns färdiga betalningssystem med bitcoin:

Men hur kan en butik ta betalt i bitcoin?

Som butiksägare måste man skydda sig mot kurssvängningar.

Det går inte att vänta på sex bekräftelser.

Det finns färdiga betalningssystem med bitcoin:

- Omedelbara bekräftelser (betalningsföretaget tar risken)

Men hur kan en butik ta betalt i bitcoin?

Som butiksägare måste man skydda sig mot kurssvängningar.

Det går inte att vänta på sex bekräftelser.

Det finns färdiga betalningssystem med bitcoin:

- Omedelbara bekräftelser (betalningsföretaget tar risken)
- Direkt växling till annan valuta (inga kurssvängningar)

Digitala valutor är gränsöverskridande

I Sverige är vi vana vid att kunna öppna bankkonton och skicka pengar

Hur ser det ut utanför västvärlden? Ganska dåligt.

Digitala valutor gör det möjligt!

Jag vill bekämpa desinformationen

Många medier är förvirrade om vad bitcoin egentligen är.

Tekniken är faktiskt inte svår att förstå!

Låt oss bekämpa några myter:

Jag vill bekämpa desinformationen

Många medier är förvirrade om vad bitcoin egentligen är.

Tekniken är faktiskt inte svår att förstå!

Låt oss bekämpa några myter:

- Myt: ”Bitcoin är anonymt” Svar: *Inte riktig anonymitet*

Jag vill bekämpa desinformationen

Många medier är förvirrade om vad bitcoin egentligen är.

Tekniken är faktiskt inte svår att förstå!

Låt oss bekämpa några myter:

- Myt: "Bitcoin är anonymt" Svar: *Inte riktig anonymitet*
- Myt: "Påhittat värde" Svar: *Ingen skillnad mot USD, SEK, EUR etc.*

Jag vill bekämpa desinformationen

Många medier är förvirrade om vad bitcoin egentligen är.

Tekniken är faktiskt inte svår att förstå!

Låt oss bekämpa några myter:

- Myt: "Bitcoin är anonymt" Svar: *Inte riktig anonymitet*
- Myt: "Påhittat värde" Svar: *Ingen skillnad mot USD, SEK, EUR etc.*
- "...det är ju ett pyramidspel, så uppfattar jag det", Leif Jakobsson (S), vice ordförande i skatteutskottet.
  Svar: *Visst har kursen gått upp, men tidiga investerare tog en enorm risk. Samma sak idag.*

Skattefrågan är ännu oklar

Förhandsbeslut från i oktober (Skatterättsnämnden):

> *Omsättning av den tjänst som ansökan avser omfattas av undantag från skatteplikt enligt 3 kap. 9 § första stycket mervärdesskattelagen (1994:200), ML.*

Beslutet är överklagat av Skatteverket som vill ha momsplikt.
Fortsättning följer!

Nu ska vi titta på mining

För att verifiera transaktioner behövs grävande (eng. *mining*).

De som hittar ett block får en belöning.

Kom ihåg: Vanliga användare av valuta behöver inte bry sig om mining.

Denna belöning är det enda sättet som ny valuta kan skapas.

Svårigheten regleras så att tiden mellan block förblir konstant.

Grävande kräver mycket datorkraft

Olika digitala valutor använder olika hashalgoritmer. Exempel:

Valuta	Hashalgoritm
Bitcoin, Namecoin m.fl.	`sha256`
Litecoin, Dogecoin m.fl.	`scrypt`
Ethereum	`dagger`
Primecoin, Quark m.fl.	Hybrid

Låt oss se hur man gräver fram dessa valutor. . .

Valutor baserade på `sha256` grävs idag med specialbyggd hårdvara

Bitcoin, den första digitala valutan, bygger på `sha256`. Denna algoritm lämpar sig väl för att göras i hårdvara.

Belöningen för ett block ligger idag på 25 bitcoin.

Device	MHash/s	MHash/J	bitcoin/dag
Core i7 950	20	0.12	3.8μ

Valutor baserade på `sha256` grävs idag med specialbyggd hårdvara

Bitcoin, den första digitala valutan, bygger på `sha256`. Denna algoritm lämpar sig väl för att göras i hårdvara.

Belöningen för ett block ligger idag på 25 bitcoin.

Device	MHash/s	MHash/J	bitcoin/dag
Core i7 950	20	0.12	3.8μ
Radeon 6970	300	1.4	55μ

Valutor baserade på `sha256` grävs idag med specialbyggd hårdvara

Bitcoin, den första digitala valutan, bygger på `sha256`. Denna algoritm lämpar sig väl för att göras i hårdvara.

Belöningen för ett block ligger idag på 25 bitcoin.

Device	MHash/s	MHash/J	bitcoin/dag
Core i7 950	20	0.12	3.8μ
Radeon 6970	300	1.4	55μ
ModMiner Quad	800	20	150μ

Valutor baserade på `sha256` grävs idag med specialbyggd hårdvara

Bitcoin, den första digitala valutan, bygger på `sha256`. Denna algoritm lämpar sig väl för att göras i hårdvara.

Belöningen för ett block ligger idag på 25 bitcoin.

Device	MHash/s	MHash/J	bitcoin/dag
Core i7 950	20	0.12	3.8μ
Radeon 6970	300	1.4	55μ
ModMiner Quad	800	20	150μ
KnC Jupiter	500 000	400	0.09

Valutor baserade på `sha256` grävs idag med specialbyggd hårdvara

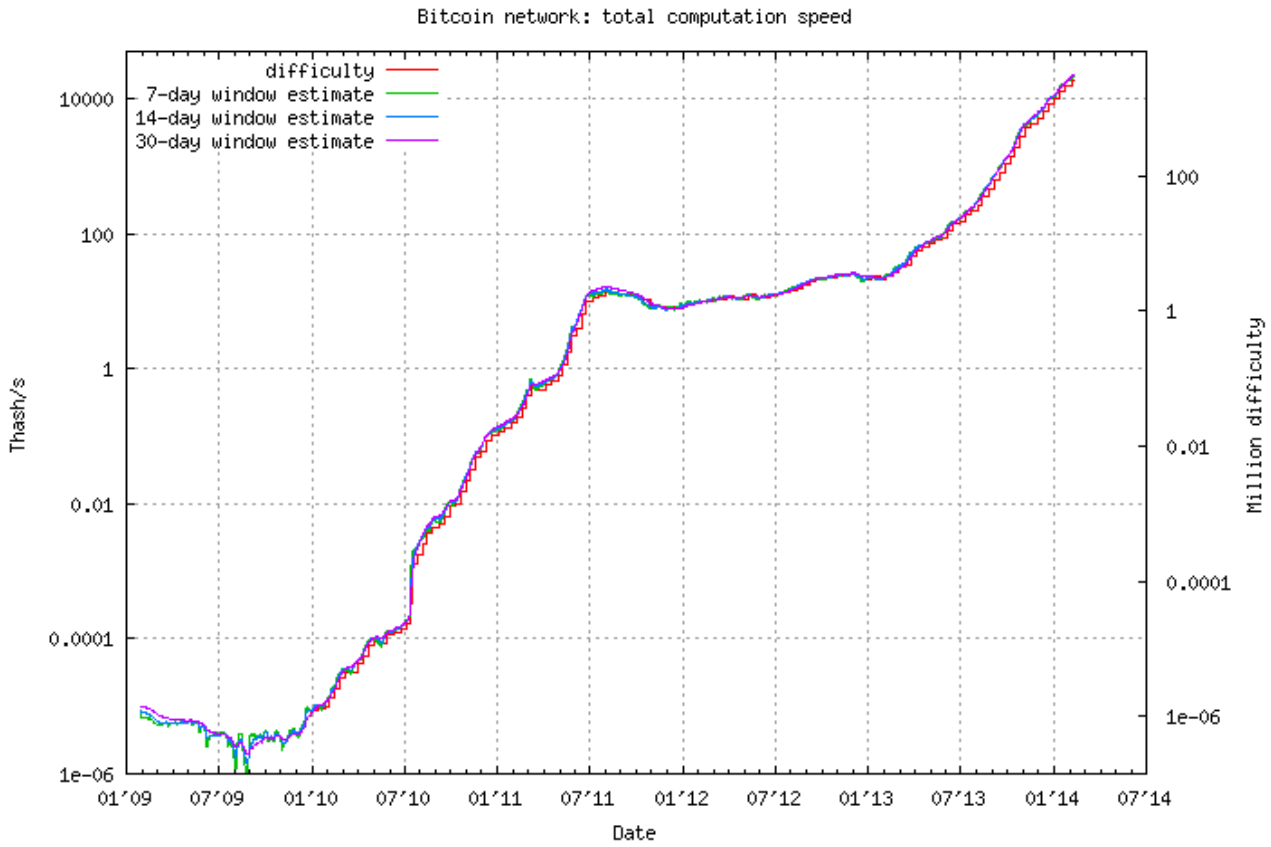
Bitcoin, den första digitala valutan, bygger på `sha256`. Denna algoritm lämpar sig väl för att göras i hårdvara.

Belöningen för ett block ligger idag på 25 bitcoin.

Device	MHash/s	MHash/J	bitcoin/dag
Core i7 950	20	0.12	3.8μ
Radeon 6970	300	1.4	55μ
ModMiner Quad	800	20	150μ
KnC Jupiter	500 000	400	0.09
KnC Neptune	3 000 000	1400	0.57

Extrem teknikutveckling!

Extrem konkurrens inom bitcoin-mining



Mining-svårigheten har exploderat (log-skala)

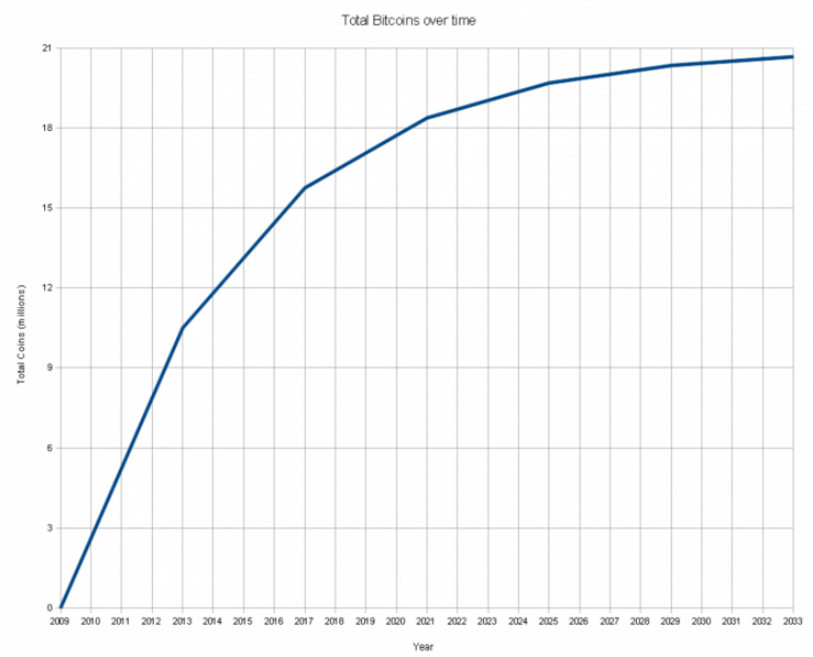
Idag, 31 januari: 22 Phash/s

Gemene man kan inte längre gräva bitcoin

Den ASIC-baserade bitcoingrävaren Neptune, kostnad 10 000 USD.

Ny valuta tillförs systemet enbart genom grävning

Var fjärde år halveras block-belöningen. Idag: 25 bitcoin.



Antalet bitcoin i omlopp (prognos).

Om 100 år kommer belöningen sjunka under 1×10^{-8}, vilket ger oss en total tillgång på 21 miljoner.

scrypt är tänkt att förhindra specialhårdvara

Efter den extrema utvecklingen hot bitcoin skapades nya valutor som baserar sig på den minnesintensiva algoritmen `scrypt`.

Tanken är att vem som helst ska kunna gräva utan dyr specialhårdvara.

Device	KHash/s	kr/dag	kWh/dag
Intel Core i7 2700K	50	1.2	2
AMD Radeon 6970	500	15	6
AMD Radeon 290x	850	27	10

Exemplet visar grävning efter litecoin, 11 februari.
Notera: Inga ASIC-kretsar!

scrypt-valutor kan grävas med grafikkort

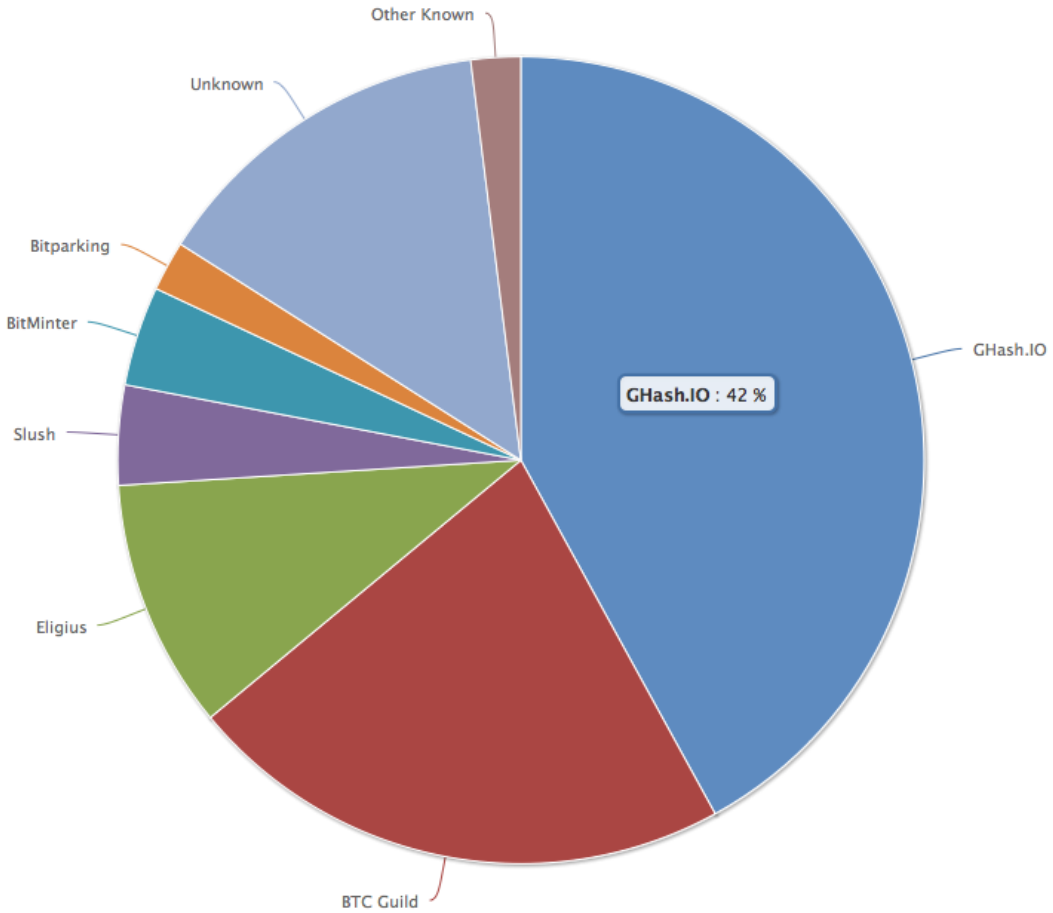
Kan man sova i samma rum?

scrypt-grävande får grafikkort att sälja som smör

Vissa är galnare än andra. Ett enda grafikkkort kostar ett antal tusenlappar.

Majoritetsgrävare kan kidnappa hela systemet

Om någon aktör gräver fortare än resten av nätverket kan denna ta full kontroll över nätverket.



Skulle `GHash` och `BTC Guild` gått ihop hade de haft majoritet.

Communityn är viktig

Bitcoin skapades av en anonym utvecklare, men det är communityn som gjort valutan användbar.

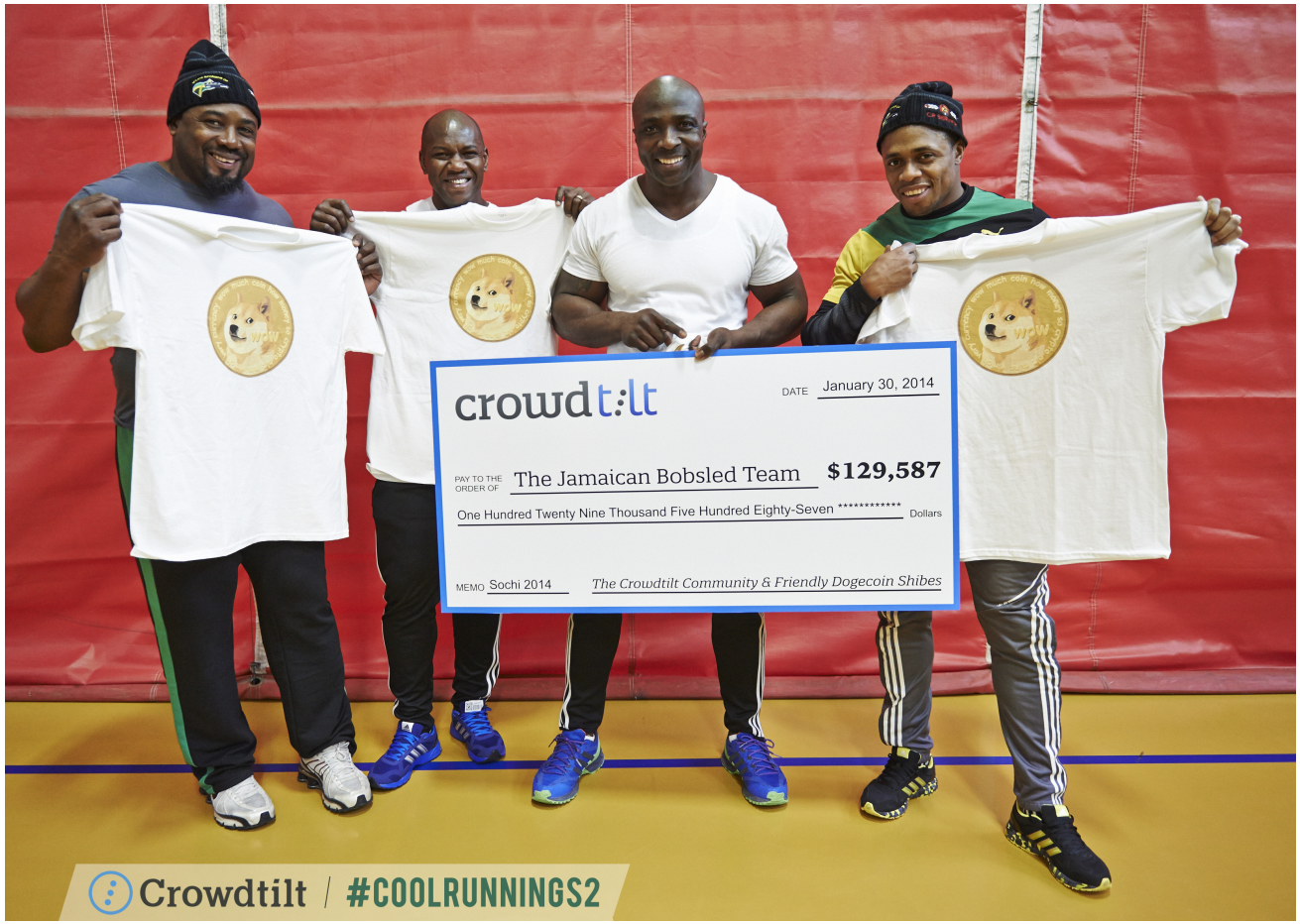
Communityn är viktig

Bitcoin skapades av en anonym utvecklare, men det är communityn som gjort valutan användbar.

Ett tydligt exempel är Dogecoin, som började som ett skämt.

Dogecoin är en lättsam variant till bitcoin.

Dogecoin är aktuellt även nu under OS



Totalt skänktes 30000 dollar i Dogecoin till det jamaicanska laget i Bob som tävlar i Sochi på söndag.

Nya tillämpningar väntar runt hörnet

Digitala valutor är som gjorda för att byggas in i andra system.

Varje dag lanseras nya tjänster.

- Dricks
- Escrow-tjänster
- Ett smidigt sätt för artister att få betalt?
- Hasardspel
- Säker e-handel (jfr. PayPal)
- Musikbranschen?

Digitala valutor är här för att stanna

Bollen är redan i rullning.

Lika svårt att stoppa som t.ex. fildelning.

Massor av desinformation. Utbildning och kunskap viktigt!

Många ogillar konkurrens

Det är enkelt att se vilka som har att förlora på digitala valutor:

> *Som vi ser det är det en bubbla. Jag ser inga praktiska applikationer som är intressanta i stor skala.*
>
> *(Sebastian Siemiatkowsk, VD för Klarna AB)*

Härom dagen kastade Apple utan förklaring ut bitcoin-appen från Appstore.

Flera storbanker stoppar transaktioner och konton relaterade till bitcoin.

Många ogillar konkurrens

Det är enkelt att se vilka som har att förlora på digitala valutor:

> *Som vi ser det är det en bubbla. Jag ser inga praktiska applikationer som är intressanta i stor skala.*
>
> *(Sebastian Siemiatkowsk, VD för Klarna AB)*

Härom dagen kastade Apple utan förklaring ut bitcoin-appen från Appstore.

Flera storbanker stoppar transaktioner och konton relaterade till bitcoin.

Jag tror vi i framtiden kommer se tillbaka på sådant beteende med förakt.

Bitcoin har många släktingar

Bitcoin	Pionjären
Litecoin	Näst störst efter Bitcoin
Dogecoin	Lättsamt och roligt?
Namecoin	Intressant alternativ till DNS
Peercoin	”Proof-of-stake”
Primecoin	Lösa primtalsproblem
...	

Hundratals! Se upp för lurendrejare.

Bra med diversifiering.

Det finns många aktuella frågeställningar

Håll koll på Ethereum, ”Kryptovaluta 2.0”.

Skattefrågan.

Var noga med säkerheten.

Mycket desinformation i pressen.

Läs mer på nätet

Denna presentation är bara en liten glimt

Whitepaper: `http://bitcoin.org/bitcoin.pdf`

`http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/`

Reddit Bitcoin: `http://www.reddit.com/r/bitcoin`

Ethereum: `http://ethereum.org`

Vem vet hur framtiden ser ut?

- Digitala valutor är här för att stanna...
- ...men måste inte stavas ”bitcoin”.

Vem vet hur framtiden ser ut?

- Digitala valutor är här för att stanna...
- ...men måste inte stavas ”bitcoin”.
- Ett komplement till dagens valutor

Vem vet hur framtiden ser ut?

- Digitala valutor är här för att stanna...
- ...men måste inte stavas ”bitcoin”.
- Ett komplement till dagens valutor
- Ungefär som e-post vs snigelpost

Vem vet hur framtiden ser ut?

- Digitala valutor är här för att stanna...
- ...men måste inte stavas ”bitcoin”.
- Ett komplement till dagens valutor
- Ungefär som e-post vs snigelpost
- Tekniken är inte svår att förstå

Vem vet hur framtiden ser ut?

- Digitala valutor är här för att stanna. . .
- . . . men måste inte stavas ”bitcoin”.
- Ett komplement till dagens valutor
- Ungefär som e-post vs snigelpost
- Tekniken är inte svår att förstå
- En global valuta

Bildkällor

Framsida: George Frey/Bloomberg

Carl Bildt: Carl Bildts twitterflöde

Asic-grävare: http://ilyavaliev.livejournal.com/6383777.html

Streckgubbar av Randall Munroe för xkcd.com under Creative Commons

Attribution-Noncommercial 2.5 license.

Paper wallet: Mike Caldwell

Jordklot. Foto: NASA

KnC Neptune. Foto: KnC Miner

Scrypt-grävare: http://imgur.com/a/olq6e

Bob-laget: http://blog.crowdtilt.com/tilting-jamaican-bobsled-team-sochi/