Analys av Bitcoins hash-algoritm

Benjamin Bergens, 36028

Kandidatavhandling

Datateknik

Institutionen för informationsteknik

Åbo Akademi, 2015

Innehåll:

1 Inledning

TODO

2 Bakgrund

2.1 Vad är Bitcoin?

Bitcoin är en valuta som överförs mellan individer digitalt, helt utan inblandning av någon form av tredje part såsom en centralbank eller en regering. Detta elektroniska betalningssystem möjliggörs genom att valutan överförs via P2P-nätverk[1] (från engelskans peer-to-peer), vilket innebär att alla datorer i nätverket är uppdelade i noder som fungerar som både klient och server. Noderna i ett P2P-nätverk, även kallat icke-hierarkiskt nätverk, är sammankopplade med varandra så att ingen nod har speciella privilegier, alla är på samma nivå och både ger och tar resurser från varandra om vartannat[2]. Detta skiljer sig från den klassiska uppdelningen med klient-server-nätverk, där de datorer som agerar som klienter helt och håller tar resurser från en dedikerad server som endast ger resurser. Bitcoin är en så kallad kryptovaluta, vilket innebär att generering och handel med valutan sker genom kryptografi[13]. På detta sätt elimineras behovet av en betrodd tredje part som medverkar i transaktionen, som t.ex. en bank eller ett kreditkortsföretag. Bitcoin flyttar alltså ansvaret för säker transaktion från finansiella institutioner för att istället kontrolleras genom kryptering[1].

2.2 Historia

Idén om en decentraliserad kryptovaluta avskuren från finansiella organ nämndes för första gången år 1998 av Wei Dai[3]. Dai kallade konceptet för b-money, och där ingick de grundläggande idéerna för hur en kryptovaluta var tekniskt möjlig. Vid ungefär samma tidpunkt gav Nick Szabo ut en artikel där även han diskuterade

möjligheterna för en digital valuta, som han gav namnet ”bit gold”[4]. Den 31 oktober år 2008 lades en vetenskaplig artikel upp på internet under namnet Satoshi Nakamoto. Namnet på artikeln var ”Bitcoin: A Peer-to-Peer Electronic Cash System”, och den beskrev tillvägagångssätt för att skapa vad Nakamoto kallade ”ett system för elektroniska transaktioner utan att förlita sig på förtroende”[1]. Den 9 januari följande år släpptes den första Bitcoinklienten (Bitcoin v0.1) med öppen källkod på webbsidan sourceforge.net[5][6]. Tre dagar senare ufördes den första Bitcoin-transaktionen, från Satoshi Nakamoto själv till Hal Finney, som år 2004 utvecklade säkerhetsprotokollet ”Reusable proof-of-work (RPOW)”[7], ett system som Bitcoin använder. Skaparen Satoshi Nakamotos identitet är något av ett mysterium. Det har uppmärksammats att namnet högst antagligen är en pseudonym. Nakamoto beskriver sig själv som en 38-årig japansk man[11], men mycket tyder på att så inte är fallet. Bitcoin-mjukvaran är inte kommenterad eller märkt på japanska och hans semantik samt vokabulär är brittisk i hans texter. Tidsanalyser av när han har skrivit och lagt upp meddelanden på internet pekar på att han skulle bo i östra USA, men det är ingenting man har kunnat fastställa. Det spekuleras också huruvida Satoshi Nakamoto är en person eller en grupp med flera personer[12].

2.3 Värdet på Bitcoin

Värdet på Bitcoin har fluktuerat kraftigt sedan 2009. Till en början var Bitcoins praktiskt taget inte värt någonting, utan användes endast av entusiaster till tekniken för kryptovaluta. Den 5 oktober 2009 var 1 309,03 XBT (förkortningen av Bitcoin som valuta[10], inofficiellt även ”BTC”) värt 1 dollar[5]. Den 22 maj 2010 köptes det första verkliga föremålen för Bitcoins. Inköpet var två stycken pizzor, för vilka Bitcoin-ägaren betalade 10 000 XBT. Pizzornas marknadsvärde var ungefär 25 dollar, vilket då gav Bitcoins ett värde på ca 0,0025 dollar per Bitcoin. Värdet fortsatte att öka, och under en femdagarsperiod från den 12 juli till 17 juli samma år ökade Bitcoins värde med 1 000 %, från $0,008/XBT till $0,08/XBT. Under de följande 2-3 åren gick priserna upp och ner, med toppar under juni 2011 och april 2013 då värdet på Bitcoin kortvarigt steg till $31,91/XBT respektive $223,11/XBT, för att sedan sjunka kraftigt de följande veckorna. I oktober år 2013 startade en kraftig ökning i Bitcoins värde som fortsatte genom november, och den 28

november 2013 spräckte Bitcoin tusendollarsgränsen. Två dagar senare hade Bitcoin sitt högsta värde hittills, $1 126,82/XBT. Efter detta maxvärde fortsatte Bitcoin att fluktuera kraftigt, dock med minskande värde över tid[5][8]. I skrivande stund (22.3.2014) ligger marknadsvärdet på $561,74/XBT[9], men värdet ändras hela tiden.

Figur 1. Bitcoins värde i amerikanska dollar de senaste två åren.

Källa: blockchain.info

3 Tekniken bakom Bitcoin

I sin artikel ”Bitcoin: A Peer-to-Peer Electronic Cash System” förklarar Satoshi Nakamoto hur en elektronisk valuta ska kunna genereras, lagras och överföras på ett säkert sätt. Detta inkluderar ett icke-hierarkiskt nätverk, asymmetrisk kryptografi, blockkedjor och hash-baserade proof-of-work-funktioner[1].

3.1 Icke-hierarkiskt nätverk

En av förutsättningarna för en välfungerande kryptovaluta är avsaknaden av ett klient-server-nätverk, där det finns en dedikerad server som erbjuder tjänster och resurser i form av CPU-kraft, minne och lagring till de datorer i nätverket som begär

dessa resurser. Istället använder Bitcoin-mjukvaran ett icke-hierarkiskt nätverk, även kallat P2P-nätverk (från engelskans peer-to-peer), för transaktion av kryptovalutan. I ett icke-hierarkiskt nätverk, som namnet antyder, finns det inga nivåer mellan datorerna i nätverket. Istället för att kommunicera med en central server kopplas datorerna direkt till varandra, och delar på allas resurser samtidigt. Detta ökar integriteten då Bitcoins överförs, och hjälper också till att förebygga dubbelbetalning[1], något som tas upp längre fram i avhandlingen.

3.2 Asymmetrisk kryptografi

Avseendet med kryptografi är att kunna skicka meddelanden mellan två parter utan att en tredje part ska kunna ta del av dem. Detta sker genom att man krypterar meddelandena med en kryptonyckel, som fungerar som en parameter. I symmetrisk kryptografi använder man sig av samma nyckel för båda kryptering och dekryptering av meddelandet. I asymmetrisk kryptografi använder man istället två nycklar då man krypterar och dekrypterar information, en privat nyckel och en allmän (publik) nyckel[16]. Den allmänna nyckeln används för att kryptera meddelanden. Den är offentlig, vilket innebär att alla kan ta del av den, och även kryptera egna meddelanden. Den privata nyckeln används i sin tur för att dekryptera informationen, och den är endast känd av aktören som utför detta[16]. Den privata och den allmänna nyckeln är sammankopplade matematiskt på ett sådant sätt att det är orimligt för en dator att beräkna. Ett exempel på detta är RSA-kryptering.

3.2.1 RSA-kryptering

RSA-kryptering är en av de första verkligt effektiva asymmetriska kryptografierna, presenterad år 1978 av Ron Rivest, Adi Shamir och Len Adleman[17]. RSA-kryptering bygger på problemet att effektivt utföra heltalsfaktorisering, vilket innebär att man bryter ner ett sammansatt tal till primtalsfaktorer. Den allmänna nyckeln i RSA-kryptering innehåller ett stort tal sammansatt av primtalsfaktorer. För att få reda på den privata nyckeln måste man alltså utföra heltalsfaktorisering, något som är extremt tidskrävande. Detta kan illustreras med ett exempel:

Vi har två primtal, t.ex. 73 och 97. En dator eller en människa kan lätt räkna ut produkten av dessa tal, nämligen 7081. Men om man istället försöker beräkna vilka två primtal som utgör faktorerna i talet 7597, blir problemet genast mycket svårare. Detta gäller även för datorer, där även de snabbaste divisionsalgoritmerna såsom Newton-Raphson och Goldschmidt är långsammare än multiplikation. Datorn måste i detta fall gå igenom alla existerande primtal fram till roten av ursprungstalet, något som är väldigt tidskrävande.

RSA-kryptering är alltså fullt möjlig att knäcka, men det är inte tillräckligt effektivt för att knäckas inom en rimlig tidsram. Den högsta RSA-algoritmen som man hittills har lyckats bryta är RSA-768, där produkten som ska faktoriseras är 768 bitar, eller 232 siffror, långt. Detta tog två år för ett stort forskarlag och krävde beräkningar ekvivalent med att en vanlig dator jobbar i cirka 2000 år. I takt med att processorer blir snabbare måste man alltså öka storleken på RSA-siffrorna. Kryptografin som Bitcoin använder kallas ECDSA, och är uppbyggd på samma princip som RSA-kryptering. Den största skillnaden är att man med ECDSA kan signera information utan att känna till den privata nyckeln, vilket är fördelaktigt för Bitcoin.

3.2.2 ECDSA

Elliptic Curve Digital Signature Algorithm

TODO

3.3 Hashfunktioner

Eftersom Bitcoin saknar en centralisering eller institution som hanterar valutan var man tvungen att komma på en metod för förhindra dubbelbetalning. En viktig del i den lösningen är att kunna bevisa att något har utförts, så att samma handling inte

kan upprepas. Bitcoin använder sig av ett proof-of-work-system (sv. bevis på arbete) som kallas hashcash.

TODO

3.4 Blockkedjor

Användandet av blockkedjor när transaktioner utförs är en av de viktigaste egenskaperna hos Bitcoin, och samtidigt den största innovationen som Bitcoin-konceptet har medfört[14]. Bitcoins blockkedja visar öppet alla transaktioner som har ägt rum sedan valutans födelse. Varje block i kedjan innehåller hash-information om föregående block, ända ner till ursprungsblocket (eng. genesis block). Alla block i kedjan leder entydigt tillbaka ursprungsblocket, men ut från ursprungsblocket kan kedjan förgrena sig i sidokedjor. För att ett block ska vara legitimt måste det ingå i den längsta blockkedjan, som måste starta med ursprungsblocket. Med längsta kedjan menas här den svåraste kedjan, alltså den blockkedja som har krävt mest datorkraft för att komma fram till. Detta är en effektiv metod för att förhindra dubbelbetalning, eftersom genuina Bitcoin-ägare bygger på nästa del av kedjan.

TODO: mer ingående information om hur blockkedjan fungerar

Storleken på Bitcoins blockkedja ligger just nu (8.3.2015) på ungefär 30GB, men växer hela tiden i takt med att fler transaktioner registreras.

3.5 Transaktioner

TODO

3.6 Elektroniska plånböcker

Elektroniska plånböcker möjliggör skickande och mottagande av Bitcoin. En elektronisk plånbok är i grund och botten ett program eller en hemsida som har tillgång till blockkedjan i en kryptovaluta. Plånboken består till största delen av transaktionsadresser och privata nycklar för ens egna adresser. Med dessa kan man komma åt sin kontobalans för sina adresser. Det finns egentligen ingen gräns för hur många adresser en plånbok kan innehålla, i princip kan man göra en adress för varje enskild transaktion. Dessa lagras sedan i plånbokens wallet.dat-fil. Den vanligaste elektroniska plånboken är Bitcoin Core, den ursprungliga plånboken skapad av Satoshi Nakamoto. Det finns dock många olika varianter av plånböcker, alla med skilda funktioner och utseende. Vissa plånböcker, t.ex. Bitcoin Core, laddar ner hela blockkedjan och räknas därför som en fullständig nod i kedjan. Att hämta hela blockkedjan kräver dock mycket resurser och lagringsutrymme, vilket har lett till att t.ex. mobila applikationer har hittat på andra lösningar för att hantera plånböcker. Det kan t.ex. vara att ansluta sig till blockkedjan via internet, vilket då förutsätter att man måste lita på organisationen som tillhandahåller kedjan. Andra applikationer laddar ner endast en liten del av blockkedjan, och sparar på så sätt lagringsutrymme.

4 Analys av Bitcoins hash-algoritm

TODO: sha-256, scrypt, x11, jämförelse, hårdvaruutveckling, ASIC

5 Avslutning

TODO

Källor:

[1] Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf [Använd 2.3.2014]

[2] Cope, J. 2002. QuickStudy: Peer-to-Peer Network, http://www.computerworld.com/s/article/69883/Peer_to_Peer_Network [Använd 2.3.2014]

[3] Dai, W. 1998. B-money, http://www.weidai.com/bmoney.txt [Använd 2.3.2014]

[4] Szabo, N. 1998, 1999, 2002, 2005. Secure Property Titles with Owner Authority, http://szabo.best.vwh.net/securetitle.html [Använd 2.3.2014]

[5] Bitcoins hemsida. 2013. History, https://en.bitcoin.it/wiki/History [Använd 2.3.2014]

[6] Nakamoto, S. 2009. Bitcoin v0.1 released, http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html [Använd 2.3.2014]

[7] Finney, H. 2004. RPOW – Reusable Proofs of Work, http://cryptome.org/rpow.htm [Använd 2.3.2014]

[8] http://blockchain.info

[9] http://bitcoincharts.com/markets/ [Använd 22.3.2014]

[10] Matonis, J. 2013. Bitcoin gaining market-based legitimacy as XBT, http://www.coindesk.com/bitcoin-gaining-market-based-legitimacy-xbt/

[11] http://p2pfoundation.ning.com/profile/SatoshiNakamoto [Använd 16.3.2014]

[12] Bitcoins hemsida. 2013 https://en.bitcoin.it/wiki/Satoshi_Nakamoto [Använd 14.3.2014]

[13] Janssen, C. Cryptocurrency http://www.techopedia.com/definition/27531/cryptocurrency [Använd 22.3.2014]

[14] Bitcoins hemsida. 2014. https://en.bitcoin.it/wiki/Block_chain [Använd 8.3.2015]

[15] Blockchain info. 2015. https://blockchain.info/charts/blocks-size [Använd 6.3.2015]

[16] Katz, J. och Lindell Y. Introduction to Modern Cryptography. CRC Press. 2007.

[17] R. L. Rivest, A. Shamir och L. Adleman. A method for obtaining digital signatures and public key cryptosystems. 1978.