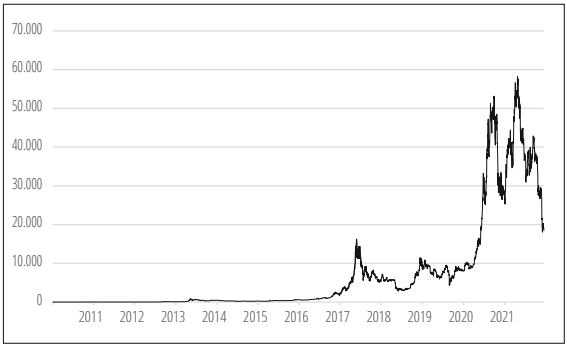
SPIEKBRIEF



Het koersverloop van de bitcoin in euro's tot 1 juli 2022.

Het koersverloop van de bitcoin in euro's tot 1 juli 2022 op een logaritmische schaal.

SPIEKBRIEF

Aantal nieuw gecreëerde bitcoins bij het mijnen

Periode	Blokken	Jaren	Beloning per blok	Aantal bitcoins toegevoegd	Totaal aantal bitcoins einde periode	Percentage bitcoins einde periode
1	0-209999	2009-2012	50	10.500.000	10.500.000	50,000000055%
2	210000-419999	2012-2016	25	5.250.000	15.750.000	75,000000083%
3	420000-629999	2016-2020	12,5	2.625.000	18.375.000	87,500000096%
4	630000-839999	2020-2024*	6,25	1.312.500	19.687.500	93,750000103%
5	840000-1049999	2024-2028*	3,125	656.250	20.343.750	96,875000107%
6	1050000-1259999	2028-2032*	1,5625	328.125	20.671.875	98,437500108%
7	1260000-1469999	2032-2036*	0,78125	164.062,5	20.835.937,5	99,218750109%
8	1470000-1679999	2036-2040*	0,390625	82.031,25	20.917.968,75	99,609375110%
9	1680000-1889999	2040-2044*	0,1953125	41.015,625	20.958.984,375	99,804687610%
10	1890000-2099999	2044-2048*	0,09765625	20.507,8125	20.979.492,1875	99,902343860%
11	2100000-2309999	2048-2052*	0,04882812	10.253,9052	20.989.746,0927	99,951171980%
12	2310000-2519999	2052-2056*	0,02441406	5.126,9526	20.994.873,0453	99,975586040%
13	2520000-2729999	2056-2060*	0,01220703	2.563,4763	20.997.436,5216	99,987793070%
14	2730000-2939999	2060-2064*	0,00610351	1.281,7371	20.998.718,2587	99,993896580%
15	2940000-3149999	2064-2068*	0,00305175	640,8675	20.999.359,1262	99,996948330%
16	3150000-3359999	2068-2072*	0,00152587	320,4327	20.999.679,5589	99,998474200%
17	3360000-3569999	2072-2076*	0,00076293	160,2153	20.999.839,7742	99,999237130%
18	3570000-3779999	2076-2080*	0,00038146	80,1066	20.999.919,8808	99,999618590%
19	3780000-3989999	2080-2084*	0,00019073	40,0533	20.999.959,9341	99,999809320%
20	3990000-4199999	2084-2088*	0,00009536	20,0256	20.999.979,9597	99,999904680%
21	4200000-4409999	2088-2092*	0,00004768	10,0128	20.999.989,9725	99,999952360%
22	4410000-4619999	2092-2096*	0,00002384	5,0064	20.999.994,9789	99,999976200%
23	4620000-4829999	2096-2100*	0,00001192	2,5032	20.999.997,4821	99,999988120%
24	4830000-5039999	2100-2104*	0,00000596	1,2516	20.999.998,7337	99,999994080%
25	5040000-5249999	2104-2108*	0,00000298	0,6258	20.999.999,3595	99,999997060%
26	5250000-5459999	2108-2112*	0,00000149	0,3129	20.999.999,6724	99,999998550%
27	5460000-5669999	2112-2116*	0,00000074	0,1554	20.999.999,8278	99,999999290%
28	5670000-5879999	2116-2120*	0,00000037	0,0777	20.999.999,9055	99,999999660%
29	5880000-6089999	2120-2124*	0,00000018	0,0378	20.999.999,9433	99,999999840%
30	6090000-6299999	2124-2128*	0,00000009	0,0189	20.999.999,9622	99,999999930%
31	6300000-6509999	2128-2132*	0,00000004	0,0084	20.999.999,9706	99,999999970%
32	6510000-6719999	2132-2136*	0,00000002	0,0042	20.999.999,9748	99,999999990%
33	6720000-6929999	2136-2140*	0,00000001	0,0021	20.999.999,9769	100,000000000%

*Schatting

Inhoud in vogelvlucht

1 Bitcoins: de basis

IN DIT DEEL . . .

Heden, verleden en toekomst

Bitcoins in vogelvlucht

IN DIT HOOFDSTUK

Hoofdstuk 1

Satoshi Nakamoto, de uitvinder van de bitcoin

De uitvinder van de **bitcoin** heet **Satoshi Nakamoto**. Althans, zo noemt hij zichzelf, want het is vrijwel zeker een pseudoniem. Satoshi Nakamoto is een mysterie. Wie hij is, weet niemand. En wat we wel van hem weten is weinig, maar dat het een pientere tante (of oom) is, dat is wel duidelijk.

Een nieuw elektronisch geldsysteem

Op 3 januari 2009, toen wij net onze tanden in de laatste oliebol zetten, zette Satoshi Nakamoto zijn computer in werking en zag het fenomeen bitcoin het levenslicht.

Twee maanden daarvoor had hij zijn uitvinding aangekondigd op een mailinglijst voor cryptografie-experts: 'Ik heb een nieuw elektronisch geldsysteem gemaakt dat geheel peer-to-peer is, zonder tussenkomst van een vertrouwenspartij.' In de mailinglijst verwees hij naar een artikel dat hij geschreven had met de titel *Bitcoin: een peer-to-peersysteem voor elektronisch geld*. De inleiding van het artikel begint als volgt:

> ‘Handelen op internet is bijna volledig afhankelijk geworden van financiële instellingen die als vertrouwenspartij optreden bij het verwerken van elektronische transacties. Het systeem werkt goed genoeg voor de meeste transacties, maar er zijn inherente zwakheden verbonden aan het op vertrouwen gebaseerde model. Uiteindelijk kunnen transacties altijd teruggedraaid worden, omdat financiële instellingen niet kunnen voorkomen dat ze moeten bemiddelen bij geschillen. De kosten van bemiddeling verhogen de transactiekosten waardoor kleine transacties niet goed mogelijk zijn, en betalingen zijn altijd terug te draaien, ook voor diensten die al geleverd zijn en niet teruggenomen kunnen worden. Omdat betalingen teruggedraaid kunnen worden, is meer vertrouwen nodig. Handelaren moeten op hun hoede zijn voor hun klanten, die daardoor meer informatie moeten geven dan eigenlijk noodzakelijk is. Een bepaald fraudepercentage wordt als onvermijdelijk geaccepteerd. Deze kosten en betalingsonzekerheden kunnen worden vermeden door contant geld te gebruiken, maar er bestaat geen mechanisme om betalingen via een communicatiekanaal zonder een vertrouwenspartij te verrichten.
>
> Wat nodig is, is een elektronisch betalingssysteem op basis van cryptografisch bewijs in plaats van vertrouwen, waardoor twee partijen rechtstreeks transacties kunnen doen zonder tussenkomst van een vertrouwenspartij. Transacties die rekenkundig vrijwel onmogelijk terug te draaien zijn beschermen verkopers tegen fraude en er kunnen eenvoudig mechanismen worden geïmplementeerd om ook de kopers te beschermen.’

Voor deze aankondiging had nog nooit iemand van de naam Satoshi Nakamoto gehoord. Satoshi Nakamoto gebruikte een e-mailadres en een website die niet te traceren waren. Op Google leverde een zoekopdracht naar de naam Satoshi Nakamoto niets op. Hij communiceerde met andere ontwikkelaars om de software te verbeteren, maar gaf nooit een enkel detail over zijn ware identiteit prijs. Op zijn online profiel stond dat hij 36 jaar was en uit Japan kwam, maar hij schreef honderden berichten in perfect Engels. In zijn artikel gebruikte hij de Amerikaanse schrijfwijze, maar in alle verdere communicatie schreef hij als een Brit. Ook zijn manier van uitdrukken kwam over als die van iemand uit Groot-Brittannië.

Wie is Satoshi Nakamoto?

De mysterieuze identiteit van Satoshi Nakamoto bleef de gemoederen bezighouden. De wildste theorieën deden de ronde. Sommigen dachten dat het pseudoniem Satoshi Nakamoto een aanwijzing op zich was. Zo opperde iemand dat de naam misschien een samentrekking zou kunnen zijn van de namen van vier Japanse technologiebedrijven: Samsung, Toshiba, Nakamichi en Motorola. Een leuke theorie, ook al is Samsung, een van de grootste elektronicabedrijven ter wereld, Zuid-Koreaans. Een ander wist zeker dat de Central Intelligence Agency (CIA, de Amerikaanse inlichtingendienst) erachter zat: in Japan noem je namelijk eerst de achternaam en dan de voornaam (dus is het Nakamoto Satoshi), en Nakamoto betekent ‘centrale herkomst’, en Satoshi betekent ‘helder denkend, gevat, wijs’, oftewel intelligent. Samengenomen kom je dus op ‘Centraal Intelligent’. ‘Interessante gedachte,’ zei weer iemand, ‘maar Nakamoto betekent eigenlijk bron. Dan moet het dus bron van wijsheid, oftewel broncode zijn.’

Ook een aantal bitcoinprogrammeurs werd er van 'verdacht' eigenlijk Satoshi Nakamoto te zijn. De meest genoemde naam is die van Gavin Andresen, een bitcoinontwikkelaar van het eerste uur en degene die het meest contact met Satoshi Nakamoto onderhouden lijkt te hebben. Zelf heeft Gavin Andresen altijd ontkend. Een andere bitcoinontwikkelaar, met de naam Dustin Trammell, werd in verband gebracht met enkele van de eerste bitcointransacties, maar ook hij ontkende de uitvinder van de bitcoin te zijn.

De bitcoinprogrammeurs zelf hebben natuurlijk ook wel over de identiteit van Satoshi Nakamoto gespeculeerd. Sommigen dachten dat het niet om een individu maar om een groep of een collectief ging. De software was erg goed ontworpen, bijna te goed om het werk van één persoon te zijn.

Genie of team?

'Ethisch hacker' Dan Kaminsky, die in 2008 een fundamentele fout in het internet ontdekte die het hele web had kunnen platleggen, wierp één blik op de broncode en wist zeker dat hij de code kon kraken. 'De code zag er niet uit,' zei hij, 'alleen de meest paranoïde, overijverige programmeur ter wereld kon dit foutloos doen.' Kaminsky vond al snel negen manieren waarop hij het systeem dacht te kunnen breken en ging voor elke manier op zoek naar de plek in de code waarop hij aan kon vallen. Maar telkens als hij de juiste plaats in de code gevonden had, was Satoshi Nakamoto hem voor geweest en was de zwakke plek gedicht. 'Ik heb nog nooit zoiets gezien', zei Kaminsky. 'Hij is een eersteklas programmeur en hij heeft grondige kennis van de programmeertaal C++, van economie, van cryptografie en van peer-to-peernetwerken. Óf dit is gemaakt door een heel team van mensen, óf Satoshi Nakamoto is een genie.'

Tot nu toe is er maar eenmaal een zwakte in de bitcoinsoftware ontdekt en uitgebuit. In augustus 2010 bleek dat transacties niet helemaal goed werden gecontroleerd voor ze in de blockchain werden opgenomen, waardoor het mogelijk was om oneindig veel bitcoins aan te maken. Op 15 augustus 2010 werden er 184 miljard bitcoins in één transactie gegenereerd. Die transactie werd echter al snel opgemerkt, de bug werd binnen een paar uur opgelost, het blok met de transactie en blokken die erna kwamen werden verwijderd en de blockchain werd opnieuw gegenereerd.

Satoshi Nakamoto onthulde weinig over zichzelf. Hij zei dat hij er meer dan een jaar over had gedaan om de bitcoinsoftware te schrijven, en voor de rest beperkte hij zich tot technische discussies erover. Maar toen op 5 december 2010 bitcoinaanhangers op een forum WikiLeaks opriepen om donaties in bitcoins te accepteren, reageerde hij ongekend krachtig. 'Nee, niet doen. Het project moet langzaam groeien zodat we de software kunnen verbeteren. Ik roep WikiLeaks op om het niet te proberen. Bitcoin staat nog maar in de kinderschoenen. Financieel zal het WikiLeaks weinig opleveren, maar de aandacht die je ermee genereert zal ons in dit stadium waarschijnlijk kapot maken.'

Verdwijntruc

Een week later leverde hij, met een berichtje over enkele technische bijzonderheden van de nieuwste versie van de software, zijn laatste bijdrage aan het forum. Sommige ontwikkelaars mailden nog met hem, maar hij antwoordde niet altijd meer, en in april 2011 stuurde hij Gavin Andresen een mailtje waarin hij liet weten dat hij 'zich nu met andere dingen bezighield' en 'dat men in het openbaar niet te veel de nadruk moet leggen op de "mysterieuze grondlegger"'. Sindsdien is er nooit meer iets van hem vernomen.

De verdwijntruc van Satoshi Nakamoto is minstens zo briljant als zijn software. Niet alleen zorgt het voor voortdurende publiciteit, het geeft bitcoin bijna iets mythisch, waardoor mensen erin geïnteresseerd blijven. Het past ook bij een peer-to-peersysteem om geen leider te hebben. Consensus is een belangrijk onderdeel van de technologie, en met een leider is het lastig om iedereen tevreden te houden. Was Satoshi Nakamoto er nog geweest om vragen te beantwoorden of te zeggen welke kant het op moet met de bitcoin, dan was de kans groot geweest dat hij onder vuur was komen te liggen.

Er is nóg een reden voor Satoshi Nakamoto om anoniem te willen blijven: hij heeft het netwerk gestart en was in het begin de enige die bitcoins mijnde. Daardoor heeft hij meer dan 1,1 miljoen bitcoins in bezit. Dat is meer dan vijf procent van alle bitcoins die er ooit zullen zijn. Op 1 juli 2022 waren die 1,1 miljoen bitcoins zo'n 21 miljard euro waard. Op papier behoort hij daarmee tot de honderd rijkste mensen op aarde, maar hij heeft die bitcoins nooit aangeraakt. De vraag is of hij dat ooit zal gaan doen. Het zou iets van de mystiek van de verdwenen grondlegger wegnemen, en het zou ook het vertrouwen in het netwerk niet ten goede komen als die grondlegger na al die jaren besluit te cashen. Aan de andere kant: wie haalt er zijn neus op voor 21 miljard euro?

Na het vertrek van Satoshi Nakamoto uit de bitcoingemeenschap werd de zoektocht naar hem natuurlijk een aantrekkelijk onderwerp voor de media. In 2011 publiceerde *The New Yorker* een artikel waarin de auteur op zoek ging naar de ware identiteit van Satoshi Nakamoto. Hij kwam uit bij een Ierse student, die hartelijk moest lachen om de suggestie dat hij Satoshi Nakamoto zou zijn. De student verwees hem naar een Finse onderzoeker in Helsinki, die de anonimiteit en de anarchie die met bitcoin gepaard gaan echter helemaal geen goed idee vond.

Er verschenen meer publicaties. In 2014 dacht het tijdschrift *Newsweek* te weten wie Satoshi Nakamoto was. Er verscheen een artikel met de titel *Het gezicht achter bitcoin* waarin de 'vondst' van Satoshi Nakamoto – inclusief foto – werd aangekondigd. Het enige wat de geportretteerde in dat artikel zegt is: 'Ik heb daar niets meer mee te maken en ik kan het niet bespreken. Andere mensen zijn er nu mee bezig. Zij gaan er nu over. Ik ben er niet meer aan verbonden.' Niet veel later verscheen er een interview met *Associated Press* waarin de man, Dorian Satoshi Nakamoto, zegt niets met bitcoin te maken te hebben en dat het allemaal op een misverstand berust omdat Engels niet zijn eerste taal is. Dat het hier echt om de uitvinder van de bitcoin ging, lijkt erg onwaarschijnlijk.

TECHNISCHE INFO

SATOSHI'S MILJOENEN

Toen ik met dit boek begon, bleef de waarde van de bitcoin maar toenemen. Elke dag kon je wel iets lezen over nieuwe bitcoinmiljonairs, over mensen waarvan jaren geleden de harde schijf stuk was gegaan en die daardoor honderden bitcoins verloren hadden (en hoeveel die nu waard zouden zijn geweest) of over de Winklevoss-tweeling die vier jaar geleden naar verluidt voor 8,5 miljoen euro één procent van alle bitcoins gekocht heeft. En overal las je hoe groot je winst zou zijn als je een paar jaar geleden een bescheiden bedrag in bitcoins had geïnvesteerd.

Weinig mensen hebben waarschijnlijk meer geprofiteerd van de koersstijgingen dan Satoshi Nakamoto – op papier althans. Bitcoinontwikkelaar Sergio Lerner heeft in 2013 geprobeerd om te achterhalen hoeveel bitcoins Satoshi Nakamoto heeft. Hij heeft een behoorlijk overtuigende analyse van de blockchain gemaakt en kwam tot de conclusie dat Satoshi Nakamoto er 1.148.800 heeft. Dat is 5,5 procent van alle bitcoins die er ooit zullen zijn. Op 1 juli 2022 was zijn totale bitcoinvermogen meer dan 21 miljard euro waard.

Het is echter de vraag of hij dat bedrag ervoor zou krijgen als hij die enorme berg bitcoins zou proberen te verkopen. Omdat het er zo veel zijn zou de wet van vraag en aanbod in werking treden en kun je een sterke prijsdaling verwachten, of zou de markt zelfs compleet kunnen instorten.

Het is ook niet bekend of Satoshi Nakamoto nog toegang heeft tot zijn bitcoinfortuin. Misschien is hij nooit van plan geweest om zijn bitcoins te besteden nadat hij zich uit het project had teruggetrokken, en heeft hij zijn 'wallet', de digitale portemonnee, weggegooid om er zeker van te zijn dat zijn bitcoins voor altijd onbereikbaar blijven.

Er is binnen de bitcoingemeenschap zelfs een discussie geweest over wat er moet gebeuren met de bitcoins die Satoshi Nakamoto heeft gemijnd. Sommige leden van de gemeenschap vinden dat de bitcoins vernietigd moeten worden om te voorkomen dat de koers instort als ze in circulatie zouden komen. Voorstanders stellen dat dit zou kunnen gebeuren als de bitcoins op de een of andere manier van Satoshi Nakamoto gestolen zouden worden, of als de beveiliging van bitcoin in de verre toekomst door kwantumcomputers gekraakt zou worden. De kans dat de bitcoins daadwerkelijk vernietigd gaan worden lijkt klein. Er zou een onwenselijk precedent geschapen worden als een beperkt aantal programmeurs besluit om derden zomaar van bitcoins te ontdoen. Bovendien zijn de bitcoins uiteindelijk Satoshi Nakamoto's eigendom, en het zou immoreel zijn om die zomaar te vernietigen.

3

De werking van bitcoins

IN DIT DEEL . . .

De techniek achter bitcoins: het bitcoinnetwerk, bitcoinadressen, transacties, de blockchain en mijnen

Versleuteling met openbare en geheime sleutels

Een mogelijke toekomst: het lightning-netwerk

IN DIT HOOFDSTUK

- **De werking van het bitcoinnetwerk**
- **Verschillende rollen**
- **Onderlinge communicatie**

Hoofdstuk 8
Het bitcoinnetwerk

Het bitcoinnetwerk is een peer-to-peernetwerk. *Peer* is het Engelse woord voor gelijke, dus het bitcoinnetwerk is een netwerk waarbij alle deelnemende computers (ook wel deelnemers, gebruikers, *clients* of *nodes* genoemd) gelijkwaardig zijn. Dat wil niet zeggen dat iedere deelnemer precies dezelfde rol binnen het netwerk speelt, maar er zijn in ieder geval geen centrale computers (servers) waar alle andere deelnemende computers van afhankelijk zijn. Met andere woorden: er is binnen het netwerk in principe geen sprake van een bepaalde hiërarchie. Het voordeel van peer-to-peernetwerken is dat ze zeer robuust zijn. Als er een of meer deelnemers uitvallen, kan de rest van het netwerk gewoon doorgaan alsof er niets aan de hand is.

Satoshi Nakamoto's keuze voor een peer-to-peernetwerk zonder centrale of 'speciale' computers reflecteert zijn wens om een geldsysteem te creëren waarbij niemand de macht heeft en de regels van het netwerk gebaseerd zijn op consensus. De gelijkwaardigheid van gebruikers betekent ook dat die gebruikers elkaar niet zomaar kunnen vertrouwen. Als de ene gebruiker A zegt, en de andere zegt B, wat is dan de waarheid?

De regels van het bitcoinnetwerk worden met behulp van cryptografie in stand gehouden, waardoor valsspelen onmogelijk is. Hoewel verschillende gebruikers tijdelijk een verschillende kijk op de waarheid kunnen hebben, resulteren de regels uiteindelijk in één waarheid waar iedereen het over eens is.

Verschillende rollen

Als ik het over gebruikers heb, dan bedoel ik zowel de personen als de software die ze draaien. Alle gebruikers zijn in hiërarchisch opzicht gelijk, maar ze spelen niet allemaal dezelfde rol binnen het netwerk.

Volledige gebruikers en lichtgewichtgebruikers

De meeste gebruikers draaien alleen een lichtere versie van de software en houden geen volledige kopie van de blockchain bij. Zij zijn afhankelijk van zogenaamde volledige gebruikers. Volledige gebruikers hebben wel een volledige kopie van de blockchain en geven informatie over transacties aan lichtgewichtgebruikers door als die daarom vragen.

Voor het netwerk zijn lichtgewichtgebruikers en volledige gebruikers gelijkwaardig, maar lichtgewichtgebruikers hebben dus wel een informatieachterstand ten opzichte van volledige gebruikers. Lichtgewichtgebruikers hebben geen een-op-eenrelatie met volledige gebruikers: ze kunnen zelf kiezen van welke volledige gebruiker ze transactie-informatie willen ontvangen. Een lichtgewichtgebruiker moet de volledige gebruiker tot op zekere hoogte vertrouwen, maar kan de informatie altijd bij een andere volledige gebruiker controleren.

Mijners

Een bijzondere groep volledige gebruikers wordt gevormd door de mijners. Ook zij houden een volledige kopie van de blockchain bij en controleren transacties, maar daarnaast organiseren zij die transacties in blokken, waarbij er bitcoins uit het niets ontstaan (vandaar de term mijnen).

Mijngroepen

Om het risico op verlies te verkleinen, hebben veel mijners zich georganiseerd in mijngroepen. Ze mijnen samen en als iemand in de mijngroep een blok vindt, dan worden de opbrengsten gedeeld. Mijnen kun je een beetje vergelijken met een loterij. Meedoen met die loterij is duur en de kans dat je wint is niet groot. Een mijngroep kun je vergelijken met een groep collega's die samen een aantal loten koopt. Omdat er meerdere loten zijn is de kans op winnen groter. Is er een winnend lot, dan verdelen de collega's de opbrengst onder elkaar.

De afzonderlijke mijners zijn verbonden met een centrale computer, de beheerder van de mijngroep. De beheerder van de groep is gelijkwaardig aan alle andere computers in het bitcoinnetwerk, maar de mijners in de groep staan lager in de hiërarchie dan de beheerder. Door de komst van mijngroepen is er dus iets van het gelijkwaardige karakter binnen het bitcoinnetwerk verloren gegaan.

Contact maken met andere gebruikers

Als je als gebruiker de software na installatie voor het eerst start, dan heb je een probleem. Hoe kan je computer immers ooit weten welke andere gebruikers er zijn om mee te verbinden? Op de een of andere manier zul je aan een of meer IP-adressen van andere gebruikers op het netwerk moeten komen. Dit probleem is opgelost door de naam van een aantal zogenaamde *DNS-seeds* (*Domain Name System*) in de code van de software op te nemen. Je computer kan verbinding met een of meer van die DNS-seeds leggen, waarna deze seeds een aantal IP-adressen van beschikbare gebruikers doorgeven. Je verbindt met die andere gebruikers, die jou op hun beurt weer aan meer IP-adressen kunnen helpen enzovoort. Op die manier kun je na enkele stappen een goede verbinding met veel verschillende gebruikers van het netwerk opzetten.

Ook het gebruik van een aantal vaste DNS-seeds gaat ten koste van het decentrale karakter van het bitcoinnetwerk. Nu zijn er toch weer een paar speciale computers die jouw computer introduceren tot de rest van het netwerk. Als je dat echt een probleem vindt, dan kun je de DNS-seeds passeren door het IP-adres van een of meer vertrouwde gebruikers op te geven bij het starten van je software.

Elke gebruiker blijft in contact met een handjevol andere gebruikers. Op die manier ontstaat er een onderling sterk verbonden netwerk. Omdat andere gebruikers komen en gaan, worden er steeds nieuwe verbindingen opgezet naarmate andere verbindingen verloren gaan.

Als je de software afsluit, dan onthoudt jouw computer de IP-adressen waarmee hij verbonden is geweest. Start je de software daarna weer op, dan probeert je computer eerst opnieuw contact te leggen met de andere gebruikers in de lijst. Je computer gebruikt de DNS-seeds nu dus niet meer. Alleen als geen van de opgeslagen IP-adressen thuisgeeft, gaat je computer opnieuw te rade bij de DNS-seeds, en begint het kennismakingsproces met het bitcoinnetwerk van voor af aan.

Communicatie tussen gebruikers

De software kan allerlei berichten sturen. In totaal worden er ongeveer vijfentwintig verschillende soorten berichten gebruikt, die er uiteindelijk vooral toe moeten leiden dat gebruikers elkaar informatie over transacties en blokken kunnen toesturen.

Gebruikers sturen elkaar alleen transacties toe die nog niet in de blockchain zijn opgenomen. Deze transacties houden de gebruikers bij in de zogenaamde *memory pool*, een tijdelijk geheugen voor niet-bevestigde transacties. Zodra een transactie door een mijner in een blok is opgenomen en het blok bij de gebruiker arriveert, wordt de transactie uit het tijdelijke geheugen verwijderd.

Een gebruiker kan aan een andere gebruiker vragen welke blokken en transacties hij kent, maar zodra een gebruiker een blok of een transactie ontvangt, kan hij

ook aan andere gebruikers vertellen dat hij kennis van die transactie of dat blok heeft. De andere gebruikers kunnen vervolgens desgewenst die transactie of dat blok bij hem opvragen.

Naast informatie over transacties en blokken is er ook nog enige tijd een notificatiesysteem voor het doorgeven van berichten over het bitcoinnetwerk actief geweest.

Volledige gebruikers

Zoals gezegd houden volledige gebruikers een volledige kopie van de blockchain met alle transacties bij. Daardoor kunnen ze zelfstandig alle transacties in de blockchain controleren. Vergeet niet dat het bitcoinnetwerk een netwerk is waarbij andere gebruikers niet per se te vertrouwen zijn, dus het is goed om transacties autonoom te kunnen controleren. Het allereerste blok dat ooit door Satoshi Nakamoto gemijnd is, wordt het genesisblok genoemd. Het is in de software van elke gebruiker ingebakken. Het controleproces begint bij het genesisblok en vanaf dat blok bouwt de volledige gebruiker zelfstandig de blockchain op met de blokken die hij van andere gebruikers ontvangt. Elke volledige gebruiker is alleen van andere gebruikers afhankelijk voor het ontvangen van nieuwe blokken. Voor het controleren van blokken en transacties is een volledige gebruiker verder compleet onafhankelijk.

Wanneer je de software voor een volledige gebruiker voor het eerst installeert, kent de software alleen het genesisblok en moet de hele blockchain vanaf daar gereconstrueerd worden. De software moet zich eerst met de rest van het netwerk synchroniseren door alle bestaande blokken van andere gebruikers te downloaden en te controleren. Halverwege 2022 bestond de blockchain uit bijna 750.000 blokken met een totale omvang van meer dan 400 gigabyte. Je kunt je voorstellen dat de computer meerdere dagen zoet is om dat allemaal binnen te halen en na te lopen.

Je kunt je de blockchain voorstellen als een stapel blokken, waarbij elk nieuw blok bovenaan de stapel wordt toegevoegd. De stapel wordt dus steeds hoger, en elk blok heeft een nummer, dat de blokhoogte genoemd wordt. De software legt verbinding met verschillende andere volledige gebruikers en vraagt hen wat de blokhoogte van hun laatst bekende blok is. Dat gebeurt wanneer de software voor het eerst opgestart wordt, maar ook telkens wanneer de software herstart wordt. De software vergelijkt de doorgegeven blokhoogte met de eigen versie van de blockchain, en als de stapel bij een andere gebruiker hoger is dan zijn eigen stapel, vraagt hij die andere gebruiker de ontbrekende blokken te versturen. Als hij erg ver achter ligt, bijvoorbeeld omdat de software nieuw geïnstalleerd is en hij alleen over het genesisblok beschikt, dan verdeelt hij de verzoeken voor nieuwe blokken over meerdere gebruikers, om ze niet te veel te belasten.

Lichtgewichtgebruikers

Niet alle gebruikers zijn in staat om de volledige blockchain op te slaan. Voor gebruikers met smartphones, tablets of andere kleine apparaten is er een speciale methode om te kunnen functioneren zonder de volledige blockchain. Ook de meeste wallets die eindgebruikers op hun computer draaien maken gebruik van deze methode. De methode wordt **vereenvoudigde betalingsverificatie** (*Simplified Payment Verification* of SPV) genoemd, en de gebruikers ervan zijn lichtgewichtgebruikers. Veruit de meeste gebruikers op het bitcoinnetwerk zijn lichtgewichtgebruikers. Omdat lichtgewichtgebruikers niet constant online zijn, en volledige gebruikers meestal wel, is het aandeel volledige gebruikers dat op elk moment online is echter groot.

Voor een goed begrip van de werking van de vereenvoudigde betalingsverificatie is het nodig om eerst wat meer over de structuur van blokken en de blockchain te weten, en over zogenaamde Merkle-bomen. Dat komt in hoofdstuk 12 aan de orde. Voor nu volstaat het om te melden dat een lichtgewichtgebruiker met deze methode niet wijs gemaakt kan worden dat een bepaalde transactie zich in de blockchain bevindt als dat niet zo is. Als een lichtgewichtgebruiker echter met een oneerlijke volledige gebruiker communiceert, dan kan die laatste een transactie wel voor de lichtgewichtgebruiker verborgen houden. Hij kan net doen of een transactie nooit heeft plaatsgevonden, terwijl dat wel zo is.

Om zich tegen een oneerlijke volledige gebruiker te beschermen, moet een lichtgewicht gebruiker met verschillende volledige gebruikers in contact staan, om zo de kans te vergroten dat er een eerlijke gebruiker tussen zit. Dit systeem is echter niet waterdicht, want een oneerlijke gebruiker kan valse identiteiten aannemen en de lichtgewichtgebruiker zo volledig van het bitcoinnetwerk afschermen. In de praktijk zal zo'n aanval niet gemakkelijk uit te voeren zijn en is deelname aan het bitcoinnetwerk in de vorm van lichtgewichtgebruiker vaak de juiste afweging tussen praktische uitvoerbaarheid en veiligheid.

Het notificatiesysteem

Naast transacties en blokken konden een tijd lang ook notificaties verstuurd worden. Met het notificatiesysteem konden de programmeurs berichten over ernstige problemen met het netwerk aan alle gebruikers sturen, bijvoorbeeld over een bug waarvoor handmatig ingrijpen noodzakelijk was.

Op 15 augustus 2010 was er een ernstig probleem met het protocol aan het licht gekomen, waardoor er in één transactie 180 miljard bitcoins uit het niets werden gecreëerd. Die transactie is teruggedraaid door het protocol te wijzigen en een paar blokken opnieuw te mijnen. Hoewel het probleem snel opgelost kon worden, was het aanleiding voor Satoshi Nakamoto om een notificatiesysteem te ontwikkelen. Na implementatie is het systeem bijna twee jaar niet gebruikt, waarna er tussen februari 2012 en april 2014 een stuk of tien keer een notificatie is geweest.

Notificaties werden cryptografisch ondertekend met een openbare sleutel. Slechts een handjevol programmeurs kende de bijbehorende geheime sleutel. Wanneer een gebruiker een notificatie ontving, dan controleerde hij de digitale handtekening en ging hij na of de notificatie nog niet verlopen was. Als de notificatie aan alle eisen voldeed, dan werd die doorgestuurd aan de andere gebruikers waarmee de gebruiker verbonden was.

In 2016 is besloten om met het systeem te stoppen. Een systeem waarbij het vermogen om berichten te versturen slechts bij enkelen geconcentreerd was, ging in tegen het decentrale karakter van het bitcoinnetwerk. Ook bestond de angst dat de geheime sleutel wellicht in verkeerde handen was gevallen.