Bitcoins

voor dummies®

Michiel Kelder

BBNC uitgevers

Amersfoort, 2018

Inhoud in vogelvlucht

Inleiding

'Opa, had jij vroeger écht elke dag stukjes ijzer en allemaal papiertjes bij je om dingen mee te kopen?' Denk jij ook dat er een tijd komt dat kinderen dat aan hun grootvader zullen vragen?

Fast backward naar 2018. We doen weleens denigrerend over vroeger tijden waarin ze nog met 'kraaltjes en spiegeltjes' betaalden, maar als je er goed over nadenkt leven we eigenlijk gewoon nog steeds in dat tijdperk. Er is echter een andere wind gaan waaien. Ene Satoshi Nakamoto vond een digitale cryptomunt uit: de bitcoin. Bijna een decennium lang was het een onderwerp waar alleen nerds en whizzkids over spraken, maar als je er intussen niet van gehoord hebt, dan heb je onder een steen gelegen. Bitcoin is *all over the news*, maar ik kan me voorstellen dat je bij jezelf denkt: waar gaat dit over? Met dit boek hoop ik je op die vraag een antwoord te geven.

In dit boek gebruikte conventies

In dit boek kom je een paar conventies tegen die jou het lezen gemakkelijker maken:

- **Vetgedrukt** is gebruikt wanneer het om een begrip of een specifieke term gaat. Deze term kun je terugvinden in de verklarende woordenlijst.
- *Cursief* geeft aan dat het om een (van oorsprong) Engelstalige term gaat, maar wordt ook gebruikt voor de titels van boeken.

Mijn ideeën over jou

Dit boek is voor iedereen die geïnteresseerd is in bitcoins. Voorkennis is niet vereist. Het is wel handig als je een computer kunt bedienen en als je een beetje snapt hoe het internet werkt.

De opbouw van dit boek

Ik heb geprobeerd om het boek zo te schrijven dat alle hoofdstukken min of meer op zichzelf staan. Omdat het een vrij complex onderwerp is, valt echter niet te voorkomen dat er soms materie aan bod komt die in een eerder hoofdstuk al behandeld is. Ik heb in die gevallen geprobeerd om zo min mogelijk in herhaling

te treden, maar als je het desondanks als irritant ervaart dan bied ik nu alvast mijn oprechte excuses aan.

Om je te helpen met het opzoeken van specifieke informatie is er aan het begin van het boek een inhoudsopgave opgenomen en een index achterin. Achterin vind je ook een verklarende woordenlijst, waarin de belangrijkste begrippen onder elkaar staan en verklaard worden.

Omdat al het goede in drieën komt, bestaat *Bitcoins voor Dummies* uit vier delen. Elk deel bevat een aantal hoofdstukken. Op die manier is het voor jou makkelijker om de informatie te vinden die je zoekt. De indeling vind je hieronder.

Deel 1: Bitcoins: de basis

Zie het eerste deel maar als een soort opwarmertje. Het bestaat uit twee hoofdstukken. In het eerste hoofdstuk vertel ik iets over de geschiedenis van bitcoins. En omdat ik als een van de weinige mensen op aarde over een kristallen bol beschik, vertel ik je ook precies wat er in de toekomst met de bitcoin zal gaan gebeuren.

In hoofdstuk 2 beschrijf ik de werking van bitcoins in een notendop. Maar de kans bestaat dat je dat vermoeden al had toen je de titel van het hoofdstuk zag.

Deel 2: Bitcoins in de dagelijkse praktijk

Misschien denk je bij jezelf: leuk hoor, die bitcoins, maar hoe functioneert dat nou in de dagelijkse praktijk? Dan is dit deel echt iets voor jou. In dit deel komt onder andere aan bod hoe je bitcoins in *wallets* kunt bewaren en hoe je bitcoins koopt en verkoopt. Ook is er een hoofdstuk gewijd aan het met bitcoins verdienen van geld.

Als je geld wilt verdienen met bitcoins, dan kun je gebruikmaken van het feit dat de koers van de bitcoin enorm op en neer gaat. De vader van Jantje doet dat bijvoorbeeld. De vader van Jantje is namelijk bitcoinhandelaar. Hij vroeg aan Jantje wat hij voor zijn verjaardag wilde. Jantje dacht even na en zei toen: een bitcoin. Waarop zijn vader zei: een bitcoin? Maar dat is 14.682 euro. 14.336 euro is hartstikke veel geld! Wat moet jij in godsnaam met 14.893 euro?

Deel 3: De techniek

Omdat de bitcoin een technische uitvinding is, is dit het dikste deel van het boek. Maar maak je geen zorgen, het is echt niet nodig om professor in de computerkunde te zijn om dit deel te kunnen snappen.

In dit deel behandel ik de werking van het bitcoinnetwerk, bitcoinadressen, transacties, de blockchain en het mijnen. Ook is er een hoofdstuk waarin wordt uitgelegd hoe versleuteling met geheime en openbare sleutels werkt.

Deel 4: Het deel van de tientallen

Als je bekend bent met de *Voor Dummies*-boeken, dan weet je dat ze allemaal afgesloten worden met het deel van de tientallen. In het laatste hoofdstuk van dit boek bespreek ik tien alternatieve cryptovaluta.

Pictogrammen die in dit boek worden gebruikt

In dit boek staan in de marge verschillende pictogrammen die in alle *Voor Dummies*-boeken gebruikt worden. De volgende pictogrammen kom je tegen:

Vergeet niet deze belangrijke punten te onthouden. Of maak een ezelsoor in de pagina's zodat je ze later terug kunt vinden.

Omdat de bitcoin een behoorlijk technische aangelegenheid is, kom je dit pictogram geregeld tegen. Ik gebruik het ook om lastige informatie aan te geven, die je echter niet altijd direct hoeft te begrijpen om de werking van bitcoins beter te leren kennen.

Dit pictogram wordt gebruikt wanneer in een passage een voorbeeld wordt toegepast, waarmee bijvoorbeeld de werking van het bitcoinnetwerk verduidelijkt wordt.

Dit pictogram waarschuwt je voor gevaar. Als er gevaar dreigt moet je niet in paniek raken en zeker niet gaan peeuwen. Als je dit pictogram ziet, dan blijf je altijd koelbloedig.

1 Bitcoins: de basis

IN DIT DEEL . . .

Heden, verleden en toekomst

De werking van bitcoins in vogelvlucht

IN DIT HOOFDSTUK

Hoofdstuk 1

Het verhaal

Ik kan me heel goed voorstellen dat je dit boek gekocht hebt omdat je wilt weten hoe bitcoins werken, en dat je nu zwaar teleurgesteld bent omdat je kennelijk eerst een heel verhaal over bitcoins moet doorwerken. Ik kan je op twee manieren geruststellen. Ten eerste hoef je dit boek niet van voor naar achter te lezen, blader dus gerust verder. Ten tweede is het een interessant verhaal. De uitvinder van bitcoins heeft de bitcoin namelijk uitgevonden omdat hij een probleem wilde oplossen. Als je het probleem begrijpt, is het gemakkelijker om de oplossing van dat probleem ook te begrijpen.

Satoshi Nakamoto

Die 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. 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 elek-

tronische 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.

Satoshi Nakamoto: 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.'