

Cryptovaluta minen voor dummies®

SPIEKBRIEF

Cryptovaluta minen is een relatief nieuw concept dat langzaam begon en gedurende ongeveer een decennium is ontwikkeld tot een hele industrie met een reputatie die vergelijkbaar is met de goudkoorts in het Wilde Westen. Het minen van 'digitaal goud' in de vorm van cryptovaluta wordt vaak afgeschilderd als een scam om snel rijk te worden, met vergelijkingen met de tulpenmanie en de goudkoorts uit het verleden. De industrie staat inderdaad bol van hypes, scams en misleidende promoties, en er kan veel misgaan. Toch zijn er inderdaad winstgevende miningondernemingen, en is er nog steeds ruimte voor jou, als nieuwe miner. Als je onderzoek doet, je huiswerk doet en nauwkeurig plant, kun ook jij profiteren van het minen van cryptovaluta.

Basis van cryptovaluta minen

Eenheden van cryptovaluta, zoals bitcoin en andere, worden gegenereerd en beveiligd door een algoritmisch proces dat in de praktijk *mining* wordt genoemd. Het proces van minen ondersteunt cryptovaluta door transacties te verifiëren en ordenen. Miners draaien mining rigs, computerapparatuur die nieuwe blokken van transacties genereert die moeten worden toegevoegd aan de blockchain van de cryptovaluta. In ruil hiervoor worden miners beloond met nieuw geslagen cryptomunten en transactiekosten. Cryptovaluta minen versterkt het peer-to-peernetwerk van nodes en maakt het duurder en moeilijker om het netwerk aan te vallen. Miners zijn van vitaal belang om het systeem te beschermen tegen hackers en anderen die de cryptovaluta proberen te ontwrichten.

Het is belangrijk om up-to-date te blijven op het gebied van cryptovaluta, dus bekijk de volgende lijst van bronnen om op de hoogte te blijven van wat er speelt:

- » **Bitcoin Talk.** Gebruik Bitcoin Talk om je te informeren over bijna ieder cryptovalutaonderwerp, waaronder (maar zeker niet beperkt tot) mining. Ondanks de naam is het niet langer alleen voor bitcoin; er worden veel verschillende cryptovaluta besproken. Het is bijvoorbeeld waar de meeste populaire alternatieve cryptovaluta werden aangekondigd voordat ze uitgebracht werden.
- » **Bitcoin subreddit.** Dit is een uitstekend forum voor het laatste nieuws en actualiteiten en geeft een kijkje naar het huidige sentiment van de gemeenschap. Het is niet alleen maar serieus; er zijn meer dan genoeg memes, grapjes en andere nonminingcontent.
- » **Bitcoin Beginners subreddit.** De bitcoin beginner-subreddit is een nog betere bron voor nieuwkomers in het ecosysteem en heeft veel uitstekende informatie voor groentjes.
- » **CoinDesk.** CoinDesk is een fatsoenlijke nieuwsbron in een industrie die vol zit met ondeugdelijke nieuwszenders. Er zijn ook gegevens over de wisselkoers voor diverse cryptovaluta te vinden.
- » **CoinJournal.** CoinJournal is ook een goede bron voor cryptovaluta-gerelateerd nieuws, maar maakt een duidelijk onderscheid tussen persberichten en nieuwsartikelen zodat gebruikers het verschil zien tussen public relations en journalistiek.
- » **Bitcoin Magazine.** Bitcoin Magazine is al lang een betrouwbare nieuwsbron binnen het domein van cryptovaluta. Hoewel het tijdschrift al jaren niet meer gedrukt wordt, is er op de site nog

Cryptovaluta minen voor dummies®

SPIEKBRIEF

steeds goede en regelmatige berichtgeving te vinden.

- » **Merkle Report.** Merkle Report ordent een ruim assortiment aan relevante content van diverse nieuwsbronnen in het domein van cryptovaluta. Het is een goede one-stop-shop voor nieuws over de hele industrie.
- » **Messari.** Messari heeft een heleboel gegevens, onderzoek en nieuws over de hele cryptovaluta-industrie. Ze hebben ook een dagelijkse nieuwsbrief om op de hoogte te blijven van huidige ontwikkelingen.
- » **Block Digest.** Block Digest is een excellente nieuwsbron in de vorm van een wekelijkse podcast waarin enkele leden van de gemeenschap nieuws en koppen uit het Bitcoin-domein bespreken en samenvatten.
- » **Stack Exchange.** De Bitcoin Stack Exchange heeft een schat aan vragen die beantwoord zijn door andere enthousiastelingen van cryptovaluta. Iedereen kan een vraag of antwoord plaatsen. Als je naar bepaalde informatie zoekt, dan is er een grote kans dat iemand je vraag al beantwoord heeft.

Een cryptovaluta om te minen kiezen

Maak geen overhaaste keuze over welke cryptovaluta je gaat minen. De rendabiliteit van minen staat of valt met deze keuze. Enkele van de belangrijkste kenmerken om in overweging te nemen bij het kiezen van een cryptovaluta om te minen zijn levensduur, veiligheid, steun van de gemeenschap, relatieve decentralisatie, methode van cryptomuntverdeling, en persoonlijke voorkeur. Als de cryptovaluta die je kiest om te minen een of meerdere van deze essentiële eigenschappen van een goed functionerend peer-to-peersysteem mist, dan is het misschien moeilijk om op de lange termijn levensvatbaarheid en winstgevendheid te behouden.

In de volgende tabel staat achtergrondinformatie over vaak geminede cryptovaluta:

Munt	Ticker Symbol	Max Afgegeven Munten	% Afgegeven	Jaren Actief	Huidige Prijs	Netwerk-Hashrate	Mining- Algoritme
Bitcoin	BTC/XBT	21.000.000	85%	10	\$ 10.385	72 EH/s	SHA-256d
Ethereum	ETH	–	n.v.t.	4	\$ 185	172 TH/s	Ethash
Bitcoin Cash	BCH	21.000.000	85%	2	\$ 310	2.2 EH/s	SHA-256d
Litecoin	LTC	84.000.000	75%	8	\$ 75	340 TH/s	Scrypt
Grin	GRIN	—	n.v.t.	1	\$ 3	4.14 GH/s	Cuckoo Cycle
Monero	XMR	—	n.v.t.	5	\$ 81	327 MH/s	CryptoNight
Dash	DASH	18.900.000	51%	5	\$ 94	3 PH/s	X11
Zcash	ZEC	21.000.000	34%	3	\$ 50	5 GH/s	Equihash

Inhoud in vogelvlucht

Inleiding	1
Deel 1: De basis van cryptovaluta	5
HOOFDSTUK 1: Cryptovaluta: een introductie	7
HOOFDSTUK 2: Cryptovaluta minen	31
HOOFDSTUK 3: Blokken bouwen: de reis van de transactie naar de blockchain	41
HOOFDSTUK 4: Verschillende vormen van mining ontdekken	55
Deel 2: De evolutie van cryptovaluta minen	77
HOOFDSTUK 5: De evolutie van minen	79
HOOFDSTUK 6: De toekomst van cryptovaluta minen	89
Deel 3: Een cryptovalutaminer worden	103
HOOFDSTUK 7: Eenvoudig minen: een poolaccount opzetten	105
HOOFDSTUK 8: Cryptovaluta om te minen kiezen	131
HOOFDSTUK 9: Je miningapparatuur verzamelen	161
HOOFDSTUK 10: Je mininghardware installeren	187
Deel 4: De economie van minen	215
HOOFDSTUK 11: De cijfers nalopen: is het het waard?	217
HOOFDSTUK 12: Nadelen verminderen en een stapje voor krijgen	245
HOOFDSTUK 13: Je cryptovalutabedrijf runnen	267
Deel 5: Het deel van de tientallen	293
HOOFDSTUK 14: Zo'n tien tips voor als de markt daalt	295
HOOFDSTUK 15: Tien manieren om ROI te boosten	315
HOOFDSTUK 16: Tien informatiebronnen voor cryptovaluta	327
HOOFDSTUK 17: Tien kritiekpunten van cryptovaluta en minen	335
Index	349

1

De basis van cryptovaluta

IN DIT DEEL . . .

Neem je de basis van cryptovaluta door.

Begrijp je de blockchain en hashing.

Werk je met wallets.

Gebruik je publieke sleutel (public key)-encryptie om ownership te bewijzen.

Ontdek je de rol van de cryptovalutaminer.

Leer je hoe je berichten in de blockchaintransactie opneemt.

Onderteken je transactieberichten.

Begrijp je het netwerk.

Hoofdstuk 1

Cryptovaluta: een introductie

Je hebt vast zin om te beginnen met je miningoperatie, maar voordat je cryptovaluta kunt creëren, willen we zeker weten dat je begrijpt wat cryptovaluta nu echt is.

Dit hele cryptogebeuren is zo nieuw (of tenminste, de interesse erin is recent, hoewel er al verschillende soorten cryptovaluta rondgaan sinds de jaren tachtig van de vorige eeuw), dat de meeste mensen een nogal wankel begrip hebben ontwikkeld van wat cryptovaluta is en hoe het werkt. De gemiddelde eigenaar van cryptovaluta weet bijvoorbeeld misschien niet wát hij nu echt bezit.

In dit hoofdstuk nemen we de geschiedenis van cryptovaluta door en bekijken we hoe de verschillende onderdelen samen functioneren. Je hebt een betere basis om cryptovaluta te minen als je begrijpt wat het is.

Een korte geschiedenis van digitale dollars

Cryptovaluta is slechts één vorm van digitale valuta... een speciale vorm. Uiteindelijk kan cryptovaluta beschouwd worden als een vorm van digitale valuta.

Dus wat is dat dan, *digitale valuta*? Nou, digitale valuta is een hele brede term die meerdere dingen omvat. In algemene zin is het geld dat bestaat in een digitale vorm in plaats van een tastbare vorm (denk aan munten en bankbiljetten). Je kunt digitale valuta verplaatsen over een elektronisch netwerk, of dat nu internet is of een netwerk voor private banking.



TIP

Eigenlijk zijn zelfs betalingen met pinpassen en creditcards transacties van digitale valuta. Als je je pinpas of creditcard bij een winkel gebruikt (online of offline), dan wordt het geld immers elektronisch overgeschreven. Het netwerk verstuurt geen pakketje van bankbiljetten per post.

Ten eerste: internet

Het verhaal van cryptovaluta begint eigenlijk allemaal met internet. Er bestonden digitale valuta voordat internet wijdverspreid was, maar goed, als een digitale valuta nuttig moet zijn, heb je wel een manier nodig om die valuta digitaal te vervoeren. Als vrijwel niemand een digitaal communicatienetwerk gebruikt (en voor 1994 deed bijna niemand dat), wat is dan het nut van digitale valuta?

Maar na 1994 gebruikten miljoenen mensen een globaal, digitaal communicatienetwerk, namelijk internet. Er ontstond een probleem: hoe kun je online geld uitgeven? Oké, tegenwoordig is het antwoord nogal simpel: je gebruikt creditcards, pinpassen of een PayPal-account. Maar in het midden van de jaren negentig was dit ingewikkelder.

Voeg daar creditcardverwarring aan toe

Zoals sommigen van jullie je misschien nog weten (veel van jullie waren toen te jong om het je te herinneren, besef ik), waren mensen in het midden van de jaren negentig nogal huiverig om creditcards op internet te gebruiken. Toen ik in 1997 mijn eigen uitgeverij had en boeken verkocht via mijn website, ontving ik (Peter, Tyler is te jong om zich 1997 te herinneren) vaak afgedrukte productpagina's van mijn website per post, samen met een cheque om het gekochte boek te betalen. Ik nam online credit-

cards aan, maar veel mensen wilden ze gewoonweg niet gebruiken; ze vertrouwden er niet op dat het 'interweb' hun waardevolle stukjes plastic veilig zou houden.

Bovendien was het voor verkopers moeilijk en duur om een betaalmethode voor creditcards op te zetten. Tegenwoordig is het best makkelijk om creditcardverwerking aan een website toe te voegen. Het is ingebouwd in zowat alle e-commercesoftware, en met laagdrempelige diensten als Stripe en Square is het maken van een *account* als verkoper niet meer zo moeilijk en duur.

Natuurlijk hebben we het hier over commerciële transacties, maar hoe zit het dan met persoonlijke transacties? Hoe kan iemand geleend geld naar een vriend terugsturen, of hoe kan een ouder geld voor bier sturen naar zijn studerende kind? (Ik heb het over PPP... pre-PayPal en online transacties tussen bankrekeningen.) Als we gingen leven in een digitale wereld, dan hadden we zeker ook digitaal geld nodig.



Een belangrijk kenmerk van contant geld is dat cash transacties nagenoeg anoniem zijn. Er is geen papierwerk of elektronisch dossier over de transactie. Veel mensen dachten dat een vergelijkbare vorm van anonieme of pseudonieme digitale valuta een enorme verbetering zou zijn ten opzichte van traditionele betaalmethoden.

Dus, veel mensen dachten dat er een betere manier moest zijn. We hadden een digitale valuta nodig voor een digitale wereld. Tegenwoordig lijkt die visie wellicht naïef; terugkijkend was het voor de hand liggend dat de kredietbedrijven niet gewoon gedag zouden wuiven naar biljoenen dollars aan online transacties. Ze wilden een deel van de winst, en waren niet bereid om hun monopolie op te geven. Daarom bestaan de belangrijkste transactiemethoden in de Verenigde Staten en een groot deel van Europa tegenwoordig vooral uit verschillende soorten bankpassen.

Voeg een snufje David Chaum toe

In het midden van de jaren negentig gingen mensen online en om verscheidene redenen wilden veel, of konden veel, geen creditcards gebruiken (zie voorgaande paragraaf). Cheques waren nog lastiger (tenzij je ze per post wilde versturen) en contant geld was geen optie. (Een grapje voor de oudere nerds onder jullie: ik herinner me nog wel een vriend die me vroeg om de \$10 die ik hem schuldig was om te zetten in UUENCODE en naar hem te e-mailen. Wederom, dit is Peter aan het woord; ik durf te wedden dat Tyler te jong is om te weten wat UUENCODE is.)

Maar in 1983 schreef een man genaamd David Chaum een paper met de titel 'Blind Signatures for Untraceable Transactions'. Chaum was een cryptograaf (iemand die werkt in de cryptografie) en een professor in informatica. In zijn paper beschreef hij een manier om cryptografie te gebruiken voor een digitaal geldsysteem met anonieme transacties, net als met contant geld. (Moderne cryptografie is de wetenschap die zich bezighoudt met het beveiligen van online communicatie; hier komen we later op terug.) Chaum wordt vaak zelfs gezien als de Vader van Digitale Valuta en de Vader van Online Anonimiteit.

Resultaat? DigiCash, e-gold, Millicent, CyberCash en meer

Wat krijg je als je internet, ingewikkelde online transacties, een angst voor het online gebruiken van creditcards, een wens voor anonieme online transacties net als contant geld, en David Chaums werk in de jaren tachtig samenvoegt?

Om te beginnen, DigiCash, David Chaums digitale geldsysteem uit 1990. Helaas lijkt meneer Chaum er te vaak te vroeg bij te zijn, en was DigiCash in 1998 weer buiten bedrijf. Er was ook e-gold, een digitaal geldsysteem dat zogenaamd gedekt was door goud, Millicent van DEC (ja, ja, de meesten van jullie zijn ook te jong om je DEC te herinneren... Ik begin me oud te voelen door het schrijven van deze 'historische' paragraaf), First Virtual, CyberCash, b-money, Hashcash, eCash, BitGold, Cybercoin en nog veel meer. Dan had je ook nog Beenz, met 100 miljoen dollar investeringskapitaal; Flooz, onderschreven door Whoopi Goldberg (echt waar!); Liberty Reserve (dat gestopt werd na beschuldigingen van witwassen); en China's QQ Coins.

Al deze digitale valuta bestaan nu niet meer, met uitzondering van QQ Coins, die nog gebruikt worden op Tencents QQ Messenger. Opvallend is dat veel van deze vroege digitale valuta op een of andere manier gecentraliseerd waren.

Toch was het verhaal van cryptovaluta nog niet klaar. Het had een moeilijke start, met veel vallen en opstaan, maar veel mensen dachten nog steeds dat de wereld cashachtige (oftewel, anonieme) online transacties nodig had. Een nieuw tijdperk stond op het punt te beginnen: het tijdperk van cryptovaluta.

De vroegere digitale valuta waren inderdaad ook gebaseerd op cryptografie, maar ze stonden niet bekend als cryptovaluta. De term 'cryptovaluta' kwam pas echt in opkomst toen cryptovaluta in 2008 gecombineerd werd met een blockchain, en de term werd pas wereldwijd verspreid rond 2012. (Block-

chain? Het is een speciale soort database, die we later in dit hoofdstuk gedetailleerder beschrijven.)

De Bitcoin-whitepaper

In 2008 publiceerde en plaatste Satoshi Nakamoto op een forum voor cryptografie genaamd de 'Cypherpunk Mailing List' een document getiteld 'Bitcoin: A Peer-to-Peer Electronic Cash System'. Hij zei: 'Ik heb gewerkt aan een nieuw elektronisch geldsysteem dat volledig peer-to-peer is, zonder vertrouwde derde partij.'

Volgens Nakamoto waren de volgende kenmerken essentieel voor Bitcoin:

- » Dubbele uitgaven zijn niet mogelijk door een peer-to-peernetwerk.
- » Geen munthuizen of andere vertrouwde partijen.
- » Deelnemers kunnen anoniem zijn.
- » Nieuwe cryptomunten worden gemaakt volgens het Hashcash-systeem van proof of work.
- » De proof of work voor het genereren van nieuwe cryptomunten stelt het netwerk in staat om dubbele uitgaven te voorkomen.

Het document is nogal droge stof, maar het is het waard om er een paar minuten naar te kijken. Je kunt het makkelijk vinden op <https://bitcoin.org/bitcoin.pdf> of <https://www.bitcoinspot.nl/de-bitcoin-paper-maar-dan-in-het-nederlands/> voor een Nederlandse vertaling. Het abstract van de Bitcoin-whitepaper begint met de volgende stelling: 'Een volledig peer-to-peerversie van elektronisch geld staat toe om online betalingen direct te versturen van de ene partij naar de andere zonder langs een financiële instantie te gaan', schreef Nakamoto. Hij legt uit dat deze methode de kwestie van 'dubbele uitgaven' oplost. Dit probleem teisterde de vroegere digitale valuta: het was een uitdaging om te verzekeren dat een digitale valuta niet twee keer uitgegeven kon worden.

Nakamoto beschrijft ook het gebruik van blockchainfunctionaliteit, al verschijnt de term blockchain nergens in de whitepaper.

'Wij stellen een oplossing voor... via het gebruik van een peer-to-peernetwerk. Het netwerk voorziet de transacties van een tijdstempel door ze in een doorlopende keten van een op hashes gebaseerd systeem van proof of work te plaatsen, met als resultaat een record die niet kan worden gewijzigd zonder de proof of work weer opnieuw uit te voeren.'

Bitcoin: de eerste toepassing van blockchain

Begin januari 2009 lanceerde Nakamoto het Bitcoin-netwerk, met gebruik van blockchain (een concept dat al sinds de vroege jaren negentig bestond, al was dit de eerste keer dat het correct geïmplementeerd werd) en creëerde hij het eerste blok in de blockchain, bekend als het *genesisblok*.

Dit blok bevatte 50 bitcoins, en de tekst *'The Times 03/Jan/2009 Chancellor on brink of second bailout for banks'* als een rechtvaardiging en uitleg waarom een systeem als Bitcoin zo belangrijk was. Nakamoto bleef updates in het protocol coderen en een node runnen en minede ongeveer een miljoen bitcoin, een getal dat hem eind 2017 een van de rijkste mensen ter wereld zou maken ('op papier', tenminste).

Aan het eind van 2010 plaatste Satoshi Nakamoto zijn laatste post op het forum en stopte hij officieel met het project. Tegen die tijd hadden echter vele enthousiastelingen van cryptovaluta zich aangesloten, en waren ze begonnen met minen en het ondersteunen van opensourcecode en de rest is geschiedenis.

Wie (of wat) is Satoshi Nakamoto?

Dus, wie was deze Satoshi Nakamoto? Een man... een vrouw... of een organisatie? Niemand weet het. Satoshi Nakamoto lijkt geen echte naam te zijn; het is waarschijnlijk een pseudoniem. En als iemand al zeker weet wie Nakamoto echt is, dan houdt diegene zijn lippen stijf op elkaar. Het is het grote mysterie van cryptovaluta.

Er is een Japans-Amerikaanse man genaamd Dorian Prentice Satoshi Nakamoto, kennelijk geboren als Satoshi Nakamoto. Deze persoon was een natuurkundige, systeemingenieur en computeringenieur voor financiële bedrijven. Misschien was hij dé Satoshi Nakamoto. Toch heeft hij dit meerdere keren ontkend.

Wat dacht je van Hal Finney, die slechts een paar straten van Dorian Prentice Satoshi Nakamoto's huis woonde? Hij was al voor bitcoin een cryptograaf en was een van de eerste mensen die bitcoin gebruikte. Hij beweert via e-mail gecommuniceerd te hebben met de oprichter van bitcoin. Sommige mensen opperen dat hij Satoshi Nakamoto's naam 'leende' en gebruikte als pseudoniem.

Dan is er ook Nick Szabo, die zich al lang bezighoudt met digitale valuta en zelfs een whitepaper publiceerde over bit gold, nog voor Nakamoto's

whitepaper over bitcoin. En hoe zit het dan met Craig White, die op een gegeven moment beweerde Nakamoto te zijn, maar die later beschuldigd werd van fraude? Of dr. Vili Lehdonvirta, een Finse economisch socioloog, of Michael Clear, een Ierse masterstudent in cryptografie, of de drie jongens die een octrooi aanvroegen met daarin een vage zinsnede ('computationally impractical to reverse') die ook gebruikt werd in Nakamoto's Bitcoin-whitepaper, of de Japanse wiskundige Shinichi Mochizuki of een of andere overheidsinstelling, of een ander soort team van mensen, of Elon Musk, of... nou, niemand weet het, maar er zijn meer dan genoeg theorieën.

Het op één na grootste bitcoinmysterie? Nakamoto bezat zo'n miljoen bitcoin, wat in december 2017 ongeveer 19 of 20 miljard dollar waard was. Het gehele bitcoinfortuin van Nakamoto is niet verplaatst of uitgegeven. Waarom heeft hij of zij (of hebben zij) het geld niet aangeraakt?

Wat is de blockchain?

Om cryptovaluta te snappen, moet je het een en ander over blockchains begrijpen. Blockchaintechnologie is ingewikkeld, maar dat geeft niet. Je hoeft niet alles te begrijpen. Je moet alleen de basis weten.

Blockchains zijn soorten databases. Een *database* is simpelweg een verzameling van gestructureerde data. Stel je voor dat je wat namen, adressen, e-mailadressen en telefoonnummers verzamelt en in een tekstverwerker typt. Dat is geen database. Dat is gewoon een verzameling tekst.

Maar stel je voor dat je die gegevens invoert in een spreadsheet. De eerste kolom is de voornaam, de tweede is de achternaam van die persoon en dan heb je kolommen voor de e-mailadressen, telefoonnummers, huisadressen, steden, postcodes, landen enzovoort... dat is gestructureerde data. Dat is een database.

De meeste mensen gebruiken constant databases. Als je een financial managementprogramma gebruikt, zoals Quickbooks, Quicken of Mint, dan zijn je gegevens opgeslagen in een database. Als je een programma gebruikt om contactgegevens op te slaan, dan zijn die ook opgeslagen in een database. Databases zijn achter de schermen een integraal deel van het moderne digitale leven.

Blockchain wereldwijd: het blockchainnetwerk

De blockchain is een database; hij slaat gegevens op in een gestructureerde vorm. Je kunt blockchains voor veel verschillende doeleinden gebruiken, bijvoorbeeld voor het registreren van *eigendomsrechten* (van wie is dit stuk land en hoe komen ze eraan?), of het volgen van een *supplychain* (waar komt je wijn of vis vandaan en hoe is het bij jou gekomen?). Blockchains kunnen alle soorten data opslaan. In het geval van cryptovaluta, slaan blockchains transactiegegevens op: wie heeft welke hoeveelheid cryptovaluta, wie heeft het aan hen gegeven en aan wie hebben zij het gegeven (hoe hebben ze het uitgegeven)?

Natuurlijk hebben blockchains ook enkele speciale kenmerken. Ten eerste zitten ze op een netwerk. Er is een Bitcoin-netwerk, een Litecoin-netwerk, een Ethereum-netwerk, net als dat er een e-mailnetwerk of een world wide web (www) is.

Bitcoin is bijvoorbeeld een netwerk van duizenden nodes of servers, verspreid over de hele planeet.

Deze nodes hebben ieder een exemplaar van de bitcoinblockchain en ze communiceren met elkaar en blijven synchroon. Ze gebruiken een *consensusmechanisme* om overeenstemming te bereiken over hoe de huidige, geldige blockchainedatabase eruitziet. Dat wil zeggen, ze hebben allemaal dezelfde versie van de blockchain.

Hashing: blokken voorzien van ‘vingerafdrukken’

Het is krachtig om de blockchain te distribueren naar veel verschillende computers, waardoor deze veel moeilijker is om te hacken of manipuleren. Maar er is iets anders dat ook krachtig is: *hashing*. Een *hash* is een lang nummer dat een soort vingerafdruk voor data is. De blockchain gebruikt dit als volgt:

- 1. Een computer die een node runt, verzamelt en valideert bitcoin-transacties (records over bitcoin verstuurd tussen adressen binnen de blockchain) die toegevoegd gaan worden aan de blockchain.**
- 2. Wanneer de computer genoeg transacties heeft verzameld, creëert deze een blok van data en *hasht* hij de data.** Dat wil zeggen

dat hij de data door een speciaal hashingalgoritme stuurt, dat de hash terugstuurt.

Hier is een voorbeeld van een echte hash, van een blok in de bitcoin-blockchain:

```
00000000000000000000000297f87446dc8b8855ae4ee2b35260dc4af61e1f5eec579Th
```

Een hash is een vingerafdruk voor de data en dankzij de magie van complexe wiskunde, kan deze onmogelijk bij een andere dataset passen. Als de gehashte data ook maar een klein beetje veranderd wordt, bijvoorbeeld een 0 verandert in een 5 of een A naar een B, dan past de vingerafdruk niet meer bij de originele data.

- 3. De hash wordt toegevoegd aan het blok van transacties.**
- 4. Het blok wordt toegevoegd aan de blockchain.**
- 5. Meer transacties worden verzameld voor het volgende blok.**
- 6. Wanneer een volledig blok van transacties klaar is, wordt de hash van het vorige blok toegevoegd aan het huidige blok.**
- 7. De blokken (de transacties en de hash van het vorige blok) worden weer gehasht.**
- 8. Het proces herhaalt zich, waardoor er een keten van blokken met tijdstempels ontstaat.**

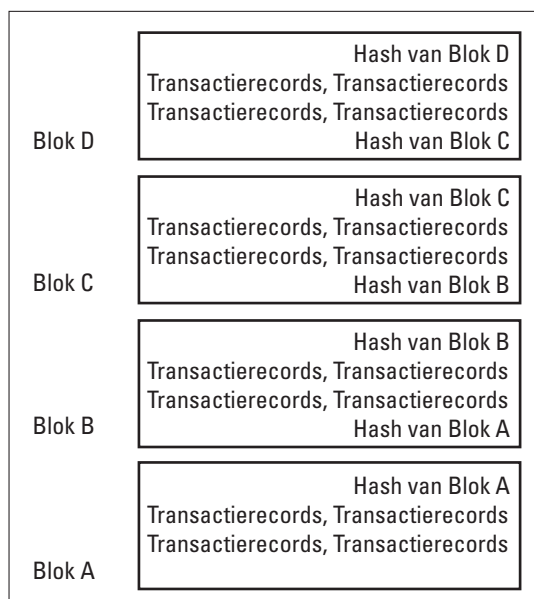
Ieder blok bevat dus twee hashes: de hash van het vorige blok en de hash van het huidige blok, die gecreëerd wordt door de combinatie van alle bitcointransacties en de hash van het vorige blok te hashen.

Dat is hoe blokken geketend zitten in de blockchain (zie figuur 1.1). Ieder blok bevat de hash van het vorige blok; in wezen een kopie van de unieke vingerafdruk van het vorige blok. Ieder blok geeft in feite ook zijn plek in de blockchain aan; de hash van het vorige blok geeft de volgorde aan waar het huidige blok zich in bevindt.

Blockchain is 'onveranderbaar'

Misschien heb je gehoord dat de blockchain nagenoeg *onveranderbaar* is, wat simpel gezegd betekent dat hij niet makkelijk gewijzigd kan worden. Als de bitcoinblockchain zegt dat je x bitcoin hebt, dan heb je ook x bitcoin en kan daar geen onenigheid over zijn... en niemand kan teruggaan in de blockchain en het op een manier hacken of veranderen of aanpassen.

FIGUUR 1.1:
De hash van ieder blok is opgeslagen in het volgende datablok. De hashes maken van de blokken een overzichtelijke keten.



Stel je voor wat er zou gebeuren als iemand in een blok zou gaan (we noemen dit Blok A) en een beetje data zou veranderen; bijvoorbeeld dat je in plaats van 1 bitcoin, 9 bitcoins naar iemand hebt gestuurd.

Nou, de hash in Blok A zou niet meer matchen met zijn data. Onthoud dat een hash een vingerafdruk is die de data identificeert, dus als je de data verandert, matcht de hash niet meer.

Oké, maar de hacker zou de data van Blok A kunnen rehashen en de ‘gecorrigeerde’ hash op kunnen slaan. Maar wacht, nu klopt het volgende blok (Blok B) niet meer omdat Blok B de hash van Blok A bevat. Dus laten we nu zeggen dat de hacker de hash van Blok A die in Blok B zit opgeslagen aanpast.

Maar nu past de hash van Blok B niet bij de data van Blok B, omdat die hash gecreëerd is vanuit een combinatie van de transactiegegevens van Blok B en de hash van Blok A!

Blok B zal dus gerehasht moeten worden en de hash geüpdatet. Maar wacht! Dit betekent dat de hash van Blok B die in Blok C zit opgeslagen nu niet meer matcht!

Zie je waar we heen gaan? Dit sneeuwbaaleffect beïnvloedt de volledige blockchain. De hele blockchain is nu verbroken, alleen maar door het aanpassen van één enkel teken in een lager blok. Om het probleem op te lossen, moet de hele blockchain opnieuw berekend worden. Alles vanaf

het gehackte blok moet opnieuw gemined worden. Wat lijkt op een simpele hack en wijziging in de database verandert nu in een enorm rekenkundig probleem dat niet makkelijk opgelost kan worden.

Dus, deze hashfunctie, samen met het feit dat duizenden andere nodes synchroon moeten lopen met identieke exemplaren van de blockchain, maakt de blockchain nagenoeg onveranderbaar. Hij kan gewoon niet makkelijk gehackt worden.

Niemand kan hem veranderen of vernietigen. Hackers kunnen niet het peer-to-peernetwerk ingaan en een transactie creëren om crypto te stelen, overheden kunnen het niet uit de lucht halen (China zou bijvoorbeeld kunnen proberen om bitcoin binnen zijn grenzen te stoppen, maar de blockchain zou nog steeds bestaan in veel andere landen), een terroristische groep kan het niet vernietigen, een land kan niet een ander land aanvallen en zijn blockchain verwoesten enzovoort. Omdat er zoveel exemplaren van de blockchain zijn, is het praktisch onveranderbaar en onvernietigbaar, zolang genoeg mensen willen blijven werken met de blockchain.

Waar is het geld?

Je vraagt je misschien af: ‘Waar is de cryptovaluta dan? Waar is het geld?’ Of misschien heb je gehoord over wallets voor cryptovaluta en denk je dat het geld daar opgeslagen is. Fout. Er zit geen geld in een wallet voor cryptovaluta. In feite is er geen cryptovaluta.

Blockchains voor cryptovaluta worden vaak beschreven als ledgers. Een *ledger* is een grootboek waarin lijsten met ontvangsten en uitgaven (transacties) worden opgetekend. Grootboeken worden al honderden jaren gebruikt om transacties van individuen, bedrijven, overheidsafdelingen enzovoort bij te houden. Het afschrift dat je krijgt van je bankrekening of creditcard is een vorm van een ledger, dat je je afzonderlijke transacties laat zien; geld dat je betaalt aan anderen en geld dat je ontvangt van anderen.

In de context van cryptovaluta is de blockchain een ledger (digitaal grootboek) dat cryptovaluta die je stuurt naar anderen, en cryptovaluta die je ontvangt van anderen, registreert.

Bekijk het eens zo: stel dat je een beetje dwangmatig bent en graag een verslag bijhoudt over het contante geld in je broekzak. Je hebt een notitieblok bij je om elke keer dat je geld in je zak stopt en elke keer dat je geld

uitgeeft het vast te leggen en je huidige saldo te berekenen. Dat notitieblok is een soort grootboek van transacties, toch?

Cryptovaluta is erg vergelijkbaar met dit grootboek van contante transacties... alleen is er geen broekzak. De blockchain is het grootboek; het bewaart een record van elke transactie (wanneer je de cryptovaluta voor het eerst kocht of kreeg, wanneer je deze uitgifte of verkocht en het saldo dat je bezit).



JE SALDO IN DE BLOCKCHAIN VINDEN

Nou, oké, de blockchain slaat niet letterlijk een saldo op voor ieder adres. Nergens in de blockchain staat hoeveel van de cryptovaluta een bepaalde eigenaar in zijn bezit heeft of hoeveel een bepaald adres eraan gekoppeld heeft. In plaats daarvan kun je met een blockchain explorer al je transacties volgen, ingaand en uitgaand, en kan de blockchain explorer je saldo afleiden op basis van deze transacties.

Maar er is geen broekzak en er is nergens een opslag met cryptovaluta erin. De blockchain is slechts een serie van 'mythische' (of virtuele) transacties opgeslagen in de ledger. Er wordt geen fysieke valuta overgedragen; we updaten gewoon de record om te laten zien dat valuta overgemaakt is.

De ledger toont aan dat je cryptovaluta hebt, dus iedereen kan dit valideren en accepteren dat je het bezit. En onthoud, dit digitale grootboek kan niet gewijzigd worden nadat het in de keten zit. Het kan niet gehackt worden. (Zie de voorgaande paragraaf voor meer over dit onderwerp.) Dus als de ledger aangeeft dat je bijvoorbeeld een halve bitcoin hebt, dan heb je dat ook echt. Je kunt die halve bitcoin aan iemand verkopen door in het digitale grootboek te zetten dat dit nu de eigenaar is!

Maar hoe zit het dan met de wallet? De wallet moet wel geld opslaan, toch? Nee, wallets voor cryptovaluta bewaren geen cryptovaluta. Ze slaan privésleutels (private keys), publieke sleutels (public keys) en adressen op. Privésleutels zijn het belangrijkste omdat zij de adressen waarmee je cryptovaluta in de blockchain geassocieerd is, beheren.

Wat is de crypto in cryptovaluta?

De *crypto* in cryptovaluta verwijst naar cryptografie. Dus, wat is cryptografie precies?

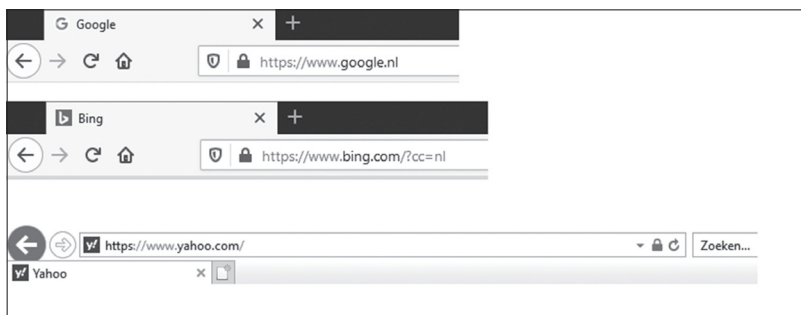
Volgens het online woordenboek woorden.org, 'wordt cryptografie gebruikt om gegevens over te dragen die niet leesbaar mogen zijn door andere partijen'. Wikipedia geeft een complexere definitie: 'Cryptografie ... houdt zich bezig met technieken voor het verbergen of zodanig versleutelen van te verzenden informatie, dat het ... onmogelijk is om tegen aanvaardbare inspanning uit de getransporteerde data af te leiden welke informatie er door de zender was verzonden en welke partijen daarbij betrokken waren.'

De geschiedenis van cryptografie gaat ten minste 4000 jaar terug. Mensen hebben altijd al zo nu en dan geheime berichten moeten versturen en dat is waar cryptografie om draait.

De cryptografie van tegenwoordig, in een wereld met computers, is veel ingewikkelder dan de vroegere versleutelingen van de klassieke wereld, en het wordt ook op veel grotere schaal gebruikt. Cryptografie is zelfs een integraal deel van internet; zonder cryptografie zou internet gewoon niet werken op de manier die we willen.

Bijna elke keer dat je je webbrowser gebruikt, maak je gebruik van cryptografie. Ken je dat kleine slotpictogram, zoals je ziet in figuur 1.2, in de adresbalk van je browser?

FIGUUR 1.2:
Het slotpictogram in je browser betekent dat de data die je naar de webserver verstuurt, versleuteld wordt met cryptografie.



Het slotpictogram betekent dat de pagina beveiligd is. Als je informatie van en naar de browser naar de webserver verstuurt en omgekeerd, zal die informatie worden *versleuteld* (gecodeerd). Mocht ze worden onderschept tijdens de honderden of duizenden kilometers lange weg op internet dan kan ze niet worden gelezen. Wanneer je bijvoorbeeld je creditcardnummer verstuurt naar een e-commercesite, wordt deze door je

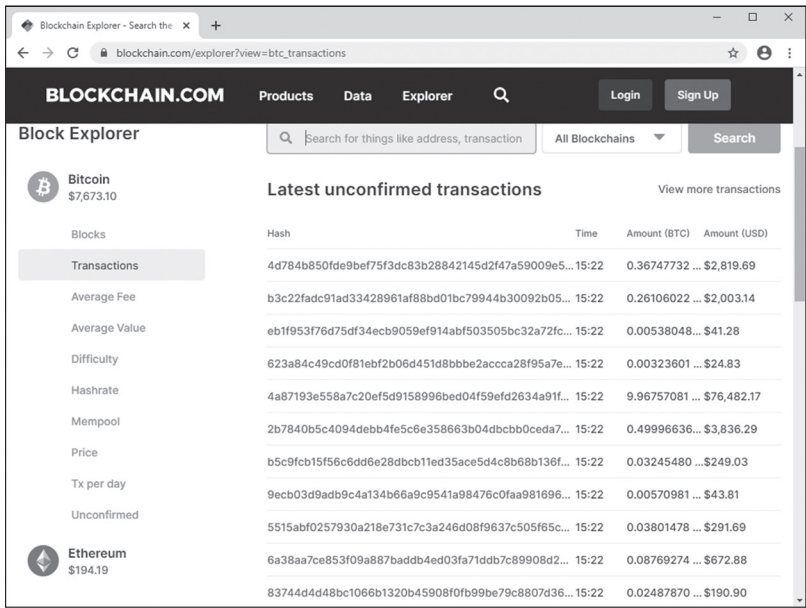
browser gecodeerd, verstuurd naar de webserver en daar ontcijferd door de ontvangende server.

Ah, dus de blockchain is versleuteld, toch? Nou, nee. Cryptovaluta maakt gebruik van cryptografie, maar niet om de gegevens in de blockchain te coderen. De blockchain is vrij toegankelijk, openbaar en controleerbaar. In figuur 1.3 zie je een voorbeeld van een blockchain explorer die ontworpen is voor bitcoin. Met behulp van een blockchain explorer kan iedereen de blockchain inzien en elke transactie sinds het genesisblok (het eerst gecreëerde blok van bitcoin) volgen.

VERSLEUTELDE BLOCKCHAIN



Het is mogelijk om versleutelde blockchains te bouwen en om data in een blockchain te versleutelen. De bitcoinblockchain is niet versleuteld en vrij toegankelijk voor controle door iedereen (zie de blockchain explorer in figuur 1.3). Toch is het wel mogelijk om versleutelde blockchains te creëren die transactiegegevens verbergen, zoals Zcash. In het algemeen zijn blockchains echter niet versleuteld, zodat iedereen inzicht heeft in de transacties die erin opgeslagen zijn.



FIGUUR 1.3:

Een voorbeeld van een blockchain explorer, te vinden op blockchain.com/explorer.

Nee, cryptografie wordt niet gebruikt om de data in de blockchain te versleutelen. Het wordt gebruikt om berichten die je naar de blockchain verstuurt te ondertekenen. Deze berichten triggeren transacties en updates in de ledger van de blockchain.

De magie van asymmetrische cryptografie

Asymmetrische cryptografie, soms ook wel bekend als publieke sleutel (public key)-cryptografie, is een slim trucje dat mogelijk is met digitale cryptografie. Deze type versleuteling is trouwens het resultaat van enorm ingewikkelde wiskunde, het soort wiskunde dat zelfs de meeste afgestudeerde wiskundigen niet begrijpen, het soort wiskunde met namen als *Carmichael-getallen* en *Goppa Codes*, het soort wiskunde dat wij zeker niet begrijpen en jij vermoedelijk ook niet (de meesten van jullie dan, tenminste). Maar dat geeft niet: zwaartekracht wordt ook niet goed begrepen, maar we gebruiken het allemaal iedere dag.

Dus, vergeet even hoe deze geweldige dingen werken en bekijk in plaats daarvan wat het uiteindelijk bereikt. Stel je een kluis voor met twee sleutelgaten en twee bijbehorende sleutels. Een is een publieke sleutel (public key) en een is een privésleutel (private key). Beeld je nu in dat je iets in de kluis stopt en deze op slot doet met de publieke sleutel. Als de deur eenmaal dicht en op slot zit, heeft de publieke sleutel niet langer toegang tot de kluis; je kunt de kluis er niet mee openmaken en het voorwerp er weer uit halen. De privésleutel werkt echter wel. De enige manier om de kluis te openen is met de privésleutel.

Deze magische wiskundige kluis werkt zelfs beide kanten op. Je kunt hem op slot doen met de privésleutel, maar nadat je hem op slot doet, kun je de kluis niet meer openmaken met de privésleutel. Alleen de publieke sleutel kan een kluis openen die op slot is gedaan door een privésleutel.

O, en deze twee sleutels zijn ook magisch verbonden. Ze werken alleen met elkaar en niet met andere sleutels. Privésleutel X werkt alleen met Publieke Sleutel X en vice versa. Je kunt dus niet de kluis op slot doen met Publieke Sleutel X en de kluis dan bijvoorbeeld ontgrendelen met Privésleutel W of Privésleutel K.

Oké, denk nu aan hetzelfde principe, maar dan met elektronische berichten. Je kunt een elektronisch bericht op slot doen met een publieke sleutel, dat wil zeggen, je kunt met een sleutel het bericht coderen, of versleutelen. Dat bericht kan een e-mail zijn of informatie die je vanaf je browser naar een webserver stuurt.

Nadat dat vergrendelde (versleutelde) bericht ontvangen is aan de andere kant (de ontvanger van de e-mail of de webserver), kan alleen de privésleutel dit openen; de publieke sleutel is nu waardeloos. En het moet ook de magisch bijbehorende (oké, mathematisch bijbehorende) sleutel zijn en geen andere.

Versleuteling is een handig middel. Het betekent dat ik je een publieke sleutel kan geven en dat jij me een bericht kunt schrijven en versleutelen met de publieke sleutel, en dat eenmaal versleuteld niemand ter wereld het bericht kan lezen tenzij ze de privésleutel hebben. Dus, als ik mijn sleutel zorgvuldig bescherm, ben ik de enige persoon ter wereld die het kan lezen.

De namen van deze sleutels zijn niet willekeurig. De privésleutel moet ook echt privé zijn. Alleen jij, en niemand anders op de wereld, moet er toegang toe hebben. De openbare sleutel kan ook echt openbaar zijn. Je kunt deze weggeven. Als je bijvoorbeeld wilt dat mensen hun berichten naar je e-mailen, dan kun je je publieke sleutel openbaar maken; op je website, in de voetregel van je e-mails, op je visitekaartje of wat dan ook. Iedereen die aan jou een bericht kan sturen kan dit versleutelen met de publieke sleutel, wetende dat jij de enige persoon ter wereld bent die het kan lezen (omdat je de privésleutel geheimhoudt).



TIP

Hoe versleutel je e-mails? E-mailversleuteling bestaat al tientallen jaren, maar is gewoonweg nooit aangeslagen bij het grote publiek. Toch kun je met de meeste e-mailprogramma's e-mails versleutelen, zoals met Outlook, Gmail en Yahoo!Mail en er zijn programma's, zoals ProtonMail, die berichten standaard versleutelen.

Dit proces is in principe wat je webbrowser gebruikt als je je creditcardinformatie online verstuurt; de browser gebruikt de publieke sleutel van de webserver om de gegevens te coderen zodat alleen de webserver, met de bijbehorende privésleutel, de creditcardinformatie kan ontcijferen en lezen. (Oké, dat is een vereenvoudiging. De communicatie van browser naar server is ingewikkelder dan deze beschrijving en omvat ook tijdelijke sessiesleutels en dergelijke; maar het basisprincipe geldt nog steeds.)

Berichten naar de blockchain

Je gebruikt asymmetrische cryptografie wanneer je transacties verstuurt naar de blockchain. Wanneer je bijvoorbeeld bitcoin wilt versturen naar iemand anders, dan verstuur je een versleuteld bericht naar de blockchain met daarin 'stuur x.xx van mijn bitcoin naar dit adres'.

Maar wacht. Ik vertelde net dat de blockchain niet versleuteld is en nu zeg ik dat de berichten naar de blockchain versleuteld zijn! Dus waarom maakt het uit of het bericht naar de blockchain versleuteld is als je het toch weer gaat ontcijferen?

Nou, onthoud dat ik zei dat dit vergrendelen/ontgrendelen beide kanten op werkt. Je kunt met de publieke sleutel vergrendelen en met de pri-

vé sleutel ontgrendelen of met de privé sleutel vergrendelen en met de publieke sleutel ontgrendelen. In beide gevallen is de data gecodeerd. Het verschil ligt hem in wie de mogelijkheid heeft deze te ontcijferen. Als je iets met de publieke sleutel codeert, is de enige persoon ter wereld die het kan ontcijferen de persoon met de privé sleutel. Maar als je het met de privé sleutel codeert, dan is de enige persoon ter wereld die het kan openen... iedereen! Werkelijk iedereen kan bij de publieke sleutel. Het is openbaar, weet je nog!

Dus, wat is dan het doel van een bericht versleutelen met de privé sleutel? Niet om het te beveiligen, logischerwijs, want iedereen kan het ontcijferen. Nee, het doel is om het bericht (transactie) te *ondertekenen* en ownership (eigendom) van de bijbehorende privé sleutel te bewijzen.

Een bericht ondertekenen met de privé sleutel

Stel dat ik mijn publieke sleutel openbaar maak op mijn website, in mijn e-mails en op mijn visitekaartjes. Op een dag krijg je een bericht dat van mij lijkt te komen. Maar hoe weet je nu zeker dat het ook echt van mij is? Nou, ik heb het bericht versleuteld met mijn privé sleutel. Dus jij neemt mijn publieke sleutel (die openbaar toegankelijk is) en gebruikt deze om het bericht te ontcijferen. Als het bericht echt van mij komt, dan ontcijfert mijn publieke sleutel het en kun je het lezen. Als het bericht niet van mij komt, dan werkt de ontcijfering niet.

Dus, door het versleutelen van het bericht met de privé sleutel, heb ik in feite het bericht ondertekend en bewezen dat het van mij komt. De ontvanger weet dat het bericht gecreëerd is door de persoon die de privé sleutel heeft die hoort bij de publieke sleutel die het bericht opende en leesbaar maakte.

Het blockchainadres: je geld

Alle cryptovaluta in de blockchain is verbonden aan adressen. Hier is zomaar een adres uit de Bitcoin-blockchain dat ik heb gevonden met de blockchain explorer op blockchain.com, bijvoorbeeld:

```
1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq
```

Er zijn biljoenen verschillende adrescombinaties mogelijk, dus dit adres is in wezen uniek. Waar komt dit adres dan vandaan? Het kwam van een wallet, die het genereerde vanuit de privé sleutel. In die wallet zit een publieke sleutel en een privé sleutel.



De publieke sleutel hoort bij de privésleutel; hij is zelfs gecreëerd vanuit de privésleutel. Het adres hoort bij de publieke sleutel; het is zelfs gecreëerd vanuit de publieke sleutel. Dus alle drie zijn mathematisch en op unieke wijze met elkaar verbonden.

Een transactiebericht versturen

Dus, hier zie je hoe cryptografie gebruikt wordt wanneer je een transactie naar de blockchain wilt sturen, om een saldo van cryptovaluta over te maken naar iemand anders. Stel dat er een adres is in de blockchain waar bitcoin aan verbonden zit. Toen ik keek, had 1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq een balans van 0,10701382 bitcoin. Nou, stel dat dit jouw bitcoin is en dat je misschien 0,05 bitcoin wilt versturen naar een vriend, een beurs of een verkoper van wie je goederen of diensten afneemt.



Het adres dat ik gebruik in dit voorbeeld is een echt adres; je kunt het zelf bekijken in een blockchain explorer. (Gebruik deze link om er te komen: <https://blockstream.info/address/1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq>.) Op het moment van schrijven had het 0,10701382 bitcoin. Tegen de tijd dat jij het ziet kan dat getal natuurlijk anders zijn.

Je stuurt een bericht naar de blockchain waarin je in essentie zegt, 'Ik ben eigenaar van adres 1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq en ik wil 0,05 bitcoin sturen naar adres 1NdaT7URGYG67L9nP2TuBZjYV6y-L7XepS.'

Als ik gewoon een bericht in platte tekst (niet versleuteld) verstuur naar de blockchain, dan is er een enorm probleem van verificatie en validiteit. Hoe zou de bitcoinnode die dit bericht ontvangt, weten dat ik inderdaad eigenaar ben van dit adres en het bijbehorende geld? Ik zou deze informatie gewoon uit mijn duim kunnen zuigen, toch?

Wat we doen, is dat we de wallet gebruiken om het bericht te ondertekenen met de privésleutel die bij het adres hoort. In andere woorden, we gebruiken de privésleutel om het bericht te versleutelen. Dan nemen we de publieke sleutel, voegen we deze bij het versleutelde bericht en sturen we het geheel naar het cryptovalutanetwerk.



TECHNISCHE
INFO

BERICHT NAAR DE BLOCKCHAIN

Hoe stuur je een bericht naar de blockchain? Dat is wat je walletsoftware doet. In feite is walletsoftware niet echt een 'wallet': in je wallet zit geen cryptovaluta. Het is meer een soort e-mailprogramma. Je e-mailprogramma verstuurt berichten over het e-mailnetwerk. Je wallet verstuurt berichten (over transacties) over het cryptovalutanetwerk.

Het bericht ontcijferen

Dus, de node (een computer die een exemplaar heeft van de cryptovaluta-blockchain) ontvangt het bericht. Hij gebruikt de publieke sleutel die bijgevoegd is en ontcijfert het bericht. De node komt hier iets te weten: 'Dit bericht moet versleuteld (ondertekend) zijn door de privésleutel die bij de publieke sleutel hoort.' Dat zegt natuurlijk niet zoveel. Het is nagenoeg een tautologie! Als een publieke sleutel een bericht kan ontcijferen, dan moet dat bericht per definitie versleuteld zijn door de bijbehorende privésleutel. Goh, wat een verrassing.

Maar onthoud dat de publieke sleutel wiskundig geassocieerd is met het adres `1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq`. Dus nu kan de node de twee bestuderen en in feite vragen: 'Hooft de publieke sleutel bij dit adres?' Als het antwoord ja is, dan weet de node ook dat de privésleutel hoort bij het adres (alle drie horen op unieke wijze bij elkaar). Dus, wat zegt de node tegen zichzelf?



TECHNISCHE
INFO

DE EIGENAAR VAN DE PRIVÉSLEUTELS IS DE EIGENAAR VAN HET GELD

Goed, misschien zijn er meer mensen met toegang tot de sleutel. Maar wat de technologie betreft doet dat er niet toe. Wie toegang heeft tot de privésleutel heeft het cryptografische recht om het geld dat toebedeeld is aan het blockchainadres dat bij de sleutel hoort te beheren. Misschien heb je de leuzen 'de eigenaar van de privésleutels is de eigenaar van het geld' of 'niet jouw privésleutel, niet jouw bitcoin' weleens gehoord. Misschien zijn ze er niet op rechtmatige wijze aan gekomen of zijn ze wettelijk gezien niet de eigenaar, maar ze kunnen het wel beheren. Dus, bescherm je privésleutels!



TECHNISCHE
INFO

PSEUDONIEME CRYPTOVALUTA

Sommige cryptovaluta zijn anoniemer dan andere. Bitcoin wordt bijvoorbeeld vaak *pseudoniem* genoemd omdat het maar deels anoniem is. Stel dat iemand de transactieafschriften voor een beurs dagvaardt en ontdekt dat je een paar bitcoins op de beurs hebt gekocht, en dat je identiteit aan die transacties verbonden zit via de Wwft (Wet ter voorkoming van Witwassen en Financiering van Terrorisme)- en KYC (Know Your Customer)-dataverzamelingsprocedures die wettelijk verplicht zijn in Nederland. Ze hebben het adres dat de beurs gebruikte om de bitcoins op te slaan, toch? Nou, nu kunnen ze de transacties van dat adres traceren door de blockchain met behulp van een blockchain explorer. En verschillende adressen kunnen op bepaalde manieren met elkaar in verband worden gebracht, dus het zou mogelijk zijn voor iemand met de informatie (een belastingautoriteit, bijvoorbeeld, of een politiedienst) om vanaf één startpunt een volledig overzicht van iemands bitcointransacties te creëren. Bitcoin is dus, zoals het tegenwoordig over het algemeen wordt gebruikt, niet volledig anoniem. Andere valuta, zoals Monero of ZCash, beweren veel dichter in de buurt van ware anonimiteit te komen. Verbeteringen aan Bitcoin, zoals conjoin en Layer 2, maken Bitcoin echter waarschijnlijk anoniemer in de toekomst.

‘Dit bericht, dat geld stuurt vanaf 1L7hHWfjL1dd7ZhQFgRv8ke1PTKA-Hoc9Tq, is verstuurd met de privésleutel die gebruikt is om dit adres te genereren... dus het bericht moet gestuurd zijn door degene die eigenaar is van het adres en daarmee ook eigenaar van het geld dat bij het adres hoort.’



TIP

Ik weet dat dit concept verwarrend kan zijn; het is moeilijk te bevatten. Daarom is hier een andere manier om erover te denken: de enige persoon die een versleuteld bericht met transactie-instructies voor dit adres, samen met de publieke sleutel die oorspronkelijk het adres creëerde, heeft kunnen sturen, is de persoon die de bijbehorende privésleutel beheert. Dat wil zeggen, de eigenaar van het adres en het geld dat ermee geassocieerd is. Het eigendom wordt dus geverifieerd en de transactie gevalideerd.

Dus dat is de crypto in cryptovaluta! Je kunt geld in de blockchain anoniem beheren door het gebruik van cryptografie, met paren van publieke sleutels en privésleutels en de bijbehorende adressen, door berichten cryptografisch te ondertekenen.

De basisonderdelen van cryptovaluta

De volgende paragrafen werpen een blik op hoe de basisonderdelen van cryptovaluta in elkaar passen.

Wat zit er in een wallet?

De *wallet* is waar alles begint wat betreft jouw cryptovaluta. Wanneer je een walletbestand creëert, genereert de walletsoftware een privésleutel. Die privésleutel wordt gebruikt om een publieke sleutel te creëren, en de publieke sleutel wordt gebruikt om een adres te creëren. Het adres heeft nog nooit eerder in de blockchain bestaan en bestaat er nog steeds niet in.

Zodra je een adres hebt, heb je een manier om cryptovaluta op te slaan. Je kunt het adres bijvoorbeeld geven aan iemand van wie je cryptovaluta koopt of aan een beurs, en zij kunnen de cryptovaluta naar dat adres sturen; in andere woorden, zij sturen een bericht naar de blockchain met daarin 'stuur x hoeveelheid crypto naar adres x '. Nu bestaat het adres in de blockchain en is er cryptovaluta aan verbonden.

Een walletprogramma is een berichtenprogramma dat je sleutels en adressen opslaat in een walletbestand. Het walletprogramma doet deze hoofdzakelijke dingen:

- » Het haalt data op uit de blockchain over je transacties en saldo.
- » Het stuurt berichten naar de blockchain om crypto van jouw adres naar andere adressen te sturen, zoals wanneer je een aankoop doet met je cryptovaluta.
- » Het creëert adressen die je kunt geven aan anderen als zij cryptovaluta naar jou moeten sturen.

Privésleutels creëren publieke sleutels

Op basis van de privésleutel in je wallet wordt een publieke sleutel gecreëerd die gebruikt wordt om de berichten die je naar de blockchain stuurt te ontcijferen. Privésleutels moeten geheim blijven; iedereen met toegang tot de privésleutel heeft toegang tot je geld in de blockchain.

Publieke sleutels creëren blockchainadressen

Publieke sleutels worden ook gebruikt om adressen te maken. De eerste keer dat een adres wordt gebruikt, stuurt iemands walletsoftware een bericht naar de blockchain met daarin 'stuur x hoeveelheid cryptovaluta naar adres x van adres y '. Tot op dit moment bestond het adres niet in de blockchain. Nadat de walletsoftware het bericht heeft verstuurd, is het adres echter in de blockchain en is er geld aan verbonden.



CRYPTOVALUTA DIE 'FORKEN'

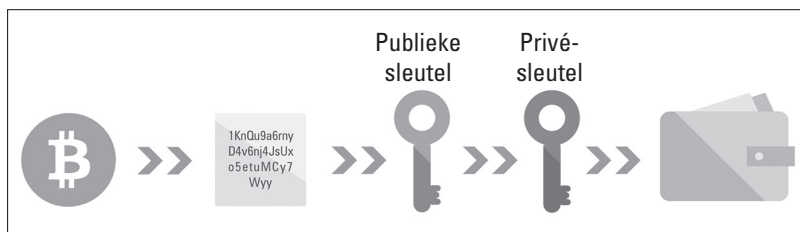
Bij een *fork* splitst één cryptovaluta in twee. Dat wil zeggen, de netwerknodes zijn het niet meer met elkaar eens en er wordt een kopie gemaakt van de cryptovalutasoftware. In de kopie wordt een verandering doorgevoerd en de twee verschillende softwareversies bouwen ieder een eigen blockchain. In januari 2015 werd bijvoorbeeld een kopie van de DASH-code, genaamd DNET (DarkNet), gemaakt. Zowel DASH en DNET vervolgden hun ontwikkeling als aparte cryptovaluta en DNET werd later hernoemd naar PIVX (Private Instant Verified Transaction).

De privésleutel beheert dit adres

De privésleutel die het adres beheert, is een uitermate cruciaal concept in cryptovaluta en mensen die toegang tot hun cryptovaluta verliezen, of van wie de cryptovaluta gestolen wordt, begrijpen dit niet (zie figuur 1.4). In dit boek gaan we niet in detail over het beschermen van privésleutels, maar zorg ervoor dat je je privésleutels beveiligd! Raak ze niet kwijt en laat andere mensen ze niet achterhalen.

FIGUUR 1.4:

De cryptovaluta horende bij een adres in de blockchain; het adres is afgeleid van de publieke sleutel, die hoort bij een privésleutel... die veilig in een wallet wordt bewaard.



Waar komt crypto vandaan? De cryptomijnen (soms)

Dus waar komt cryptovaluta vandaan? Cryptovaluta kan *gemined* worden (de minst voorkomende vorm, maar wel degene waar je vanzelfsprekend het meeste in geïnteresseerd bent gezien je interesse voor dit boek), of het kan *pre-mined* zijn.

Zeggen dat een cryptovaluta *pre-mined* of *nonmineable* is, betekent eenvoudigweg dat de cryptovaluta al bestaat. De blockchain is een ledger (digitaal grootboek) met daarin informatie over transacties. Toen de blockchain gecreëerd werd, bevatte de ledger al een record van alle cryptovaluta die de oprichters beoogd hadden. Er wordt niet meer aan toegevoegd; het zit allemaal al in de blockchain.

Het is zelfs zo dat, hoewel we veel horen over het minen van cryptovaluta, de meerderheid van de valuta (op het moment van schrijven meer dan 2000 verschillende soorten) *pre-mined* zijn: ongeveer 74 van de top 100-cryptovaluta zijn *nonmineable* en algeheel gezien kan zo'n 70 procent van de cryptovaluta niet gemined worden.

Een voorbeeld van een *pre-mined* valuta is XRP, vaak Ripple genoemd, dat op het moment de op één na grootste cryptovaluta is (wat betreft beurswaarde tenminste, dat is de waarde van alle cryptovaluta in omloop). XRP is opgeslagen binnen de RippleNet-blockchain.

Toen de Ripple-blockchain opgericht werd, waren er al 100 miljard XRP opgenomen in de blockchain, al was het meeste ervan niet verstrekt. De oprichters van Ripple hielden zelf 20 procent en zelfs nu is bijna 60 procent van de valuta niet in omloop.

Een ander voorbeeld is Stellar, een betaalnetwerk dat oorspronkelijk bekostigd werd door betaaldienst Stripe, dat op het moment van schrijven de nummer vier grootste cryptovaluta was. Stellar heeft een totale voorraad van meer dan 100 miljard lumens, waarvan 2 procent aan Stripe werd toebedeeld voor hun investering.

Dus nee, niet alle cryptovaluta kunnen gemined worden (de meeste zelfs niet). Maar goed, dat is niet waarom je dit boek leest, toch?

Het goede nieuws is dat je op het moment zo'n 600 cryptovaluta wel kunt minen (al zul je het overgrote deel nooit willen minen). Lees hoofdstuk 8 om te besluiten welke je wilt minen.