Cryptovaluta voor dummies 2e editie

SPIEKBRIEF

Houd je aan de volgende regels:

1. **Zet waar mogelijk 2FA aan.** 2FA is de afkorting van two-factor-authentication of authenticatie met een extra wijze van inloggen naast een normaal wachtwoord.
2. **Maak een kopie/foto/printje van je 2FA-code.** 2FA instellen is makkelijk: download een app zoals Google Authenticator op je telefoon en scan de **QR-code** of typ een speciale code in die je wordt getoond. Voor elke website moet je apart een item aanmaken in je Google Authenticator app. Als je je telefoon kwijtraakt, ben je je 2FA ook kwijt! Je kunt dit programma niet back-uppen. Wel kun je de QR-code en/of de code printen en ergens veilig bewaren. Als je dan een andere telefoon hebt, kun je dezelfde codes gebruiken!
3. **Gebruik een speciale hardware-wallet.** Een hardware-wallet is de veiligste manier om de sleutels tot je cryptovaluta te bewaren en ook nog redelijk makkelijk te kunnen bereiken.
4. **Laat je fondsen niet op een exchange staan.** Als je niet actief handelt met je fondsen, laat ze niet op een exchange staan. Een exchange kan gehackt worden! Je hardware-wallet niet.
5. **Schrijf je seed op papier en bewaar dit veilig.** Je krijgt bijna altijd 12 of 24 speciaal voor jou gegenereerde woorden. Deze woorden moet je echt goed bewaren. Bewaar deze nooit in een bestand op je computer, maar schrijf ze op een briefje en sla dit briefje veilig op. Ben je ooit je wallet-bestand kwijt? Dan kun je weer bij je fondsen door je 12 of 24 woorden in te voeren.
6. **Controleer altijd een publieke sleutel na kopiëren en plakken.** Een veelvoorkomende manier om cryptovaluta te stelen, is door het wijzigen van het gekopieerde en vervolgens geplakte adres. Bepaalde malware herkent zo'n adres en verandert dit in een eigen adres. Veel mensen zien niet in één oogopslag dat het adres veranderd is. Dit is makkelijk te voorkomen door altijd de eerste paar en laatste paar cijfers van een adres te checken voor je verstuurt.
7. **Zorg voor je nalatenschap.** Hierover nadenken is niet leuk, maar zorg voor je nabestaanden. Laat iemand niet per ongeluk papiertjes met seeds weggooien omdat hij of zij niet weet wat het zijn. Licht daarom je familie of mensen die je vertrouwt in over hoe je met je cryptovaluta omgaat. Denk een systeem uit waarmee in geval van nood zij bij je sleutels en je wachtwoordmanager kunnen.
8. **Update je computer.** Zorg ervoor dat je altijd de laatste versie van je besturingssysteem op je computer hebt staan en update als er updates zijn. Heel veel mensen klikken updates weg. Dat moet je niet doen.
9. **Dek delen van je id's af bij KYC's.** Als je meedoet aan **ICO's** of als je lid wilt worden bij bepaalde exchanges, dan kan het zijn dat je identiteitsbewijzen moet overleggen. Zorg er altijd voor dat het duidelijk is dat het een kopie is en dek je bsn-nummer af. Zie ook informatie van de Rijksoverheid door te zoeken naar 'Hoe voorkom ik fraude met een kopie van mijn identiteitsbewijs?' (Zie ook https://laatjeniethackmaken.nl/)

Inhoud in vogelvlucht

1

De geschiedenis van geld en de komst van bitcoin

IN DIT DEEL . . .

Als je de geschiedenis van geld kent, dan weet je ook waarom bitcoin en cryptovaluta interessant zijn, misschien zelfs wel belangrijk voor de wereldeconomie. We kijken naar bitcoin en de werking daarvan. Met deze basis gaan we naar het 'maken' van andere cryptovaluta.

IN DIT HOOFDSTUK

Hoofdstuk 1
Het begin: geld

Waar begin je met een boek over cryptovaluta? Bij snel geld verdienen en verliezen? Bij de **bitcoin** of de werking van een **blockchain**? Met een opsomming van alle in het oog springende cryptovaluta en tokens van de afgelopen jaren?

Dat kan allemaal, maar dan mis je een belangrijk onderdeel, namelijk waar cryptovaluta vandaan komen en dat is in de basis: geld. Als je weet hoe geld tot stand kwam, is ook veel duidelijker waarom cryptovaluta in het algemeen en bitcoin in het bijzonder zo interessant zijn.

Een beknopte geschiedenis van geld

Als je denkt dit allemaal al te weten, lees er toch even rap doorheen. Niet in de laatste plaats omdat enkele eigenschappen van geld heel bijzonder zijn en het is jammer als je die niet scherp hebt.

Die tumultueuze geschiedenis van geld laat het bestaansrecht van cryptovaluta zien en in het bijzonder dat van bitcoin. Het systeem zorgde voor de mogelijkheid digitale schaarste te creëren, waardoor de munt waarde kreeg en – in tegenstelling tot vrijwel alle andere digitale zaken – niet onbeperkt vermeerderd kan worden. Het loste direct een ander probleem op: hoe verplaats je waarde via internet?

Je kunt natuurlijk je zinnen gezet hebben op een heel andere cryptomunt en misschien vind je bitcoin al hopeloos ouderwets, maar zonder bitcoin was die munt of token waar je zo dol op bent er ook niet geweest. En die ouwe bitcoin heeft wel een eigenschap die geen enkele andere munt heeft, namelijk geen eigenaar.

Ruilhandel en de eeuwige misvatting

Eerst neem ik je mee naar vroeger. Naar een tijd waarin de mens in plaats van geld aan ruilhandel deed om elkaar te betalen. Althans, dat is de meest gehoorde 'oplossing' voor het afhandelen van transacties in het verre verleden. Om uit te vinden dat dit helemaal niet zo logisch is, kun je een snel gedachte-experiment uitvoeren.


VOORBEELD

Je hebt één kip en je wilt eigenlijk een koe. Die kip is niet voldoende voor die koe. Dan moet er of meer kip bij of minder koe. Een levende koe is niet deelbaar en tien kippen fokken duurt ook wel even. Oh ja, je hebt dan ook een haan nodig. Je kunt natuurlijk besluiten de kippen na te leveren en dan heb je een schuld.

Al met al: dit is een lastig probleem. In oude samenlevingen viel dat mee: de grootte van de gemeenschap was goed te overzien, en iedereen wist wel dat Harm een ploeg van Isaac had geleend en dat Yasmina goed is in het maken van kleding en Esma in het bakken van brood. Iedereen sloeg de boekhouding als het ware in het publieke geheugen op. Op den duur kwamen daar echte boekhoudingen bij. Nu hadden we in ieder geval een overzicht van wat iedereen aan anderen schuldig was. In eerste instantie was er helemaal geen geld, alleen maar schuld. In sommige samenlevingen werd schuld zelfs eens in de zoveel tijd door de heerser vereffend, zodat iedereen weer met een schone lei kon beginnen. Je ziet: er is nog geen stuiver aan te pas gekomen.

De komst van geld

Zo'n systeem van schuldvereffening werkt prima op kleine schaal en in tijden van rust. Het wordt lastiger als je over langere afstand of in grotere groepen dit soort dingen wilt bijhouden. Al snel zit je met een complex probleem. Het is handiger om schulden direct te vereffenen en daarvoor zijn heel veel systemen bedacht in de loop van de millennia. Van het elkaar betalen met schelpen, kralen en glimmende metalen tot het gebruik van grote ronde stenen die eigenlijk niet te verplaatsen waren, maar waarvan iedereen wist wie ze bezat. Soms werden zelfs alcohol en sigaretten als betaalmiddelen ingezet. Je ziet: al deze zaken hebben bepaalde problemen waardoor ze slecht als geld functioneren over langere tijd. Alcohol raakt op, schelpen slijten of gaan kapot en grote ronde stenen die ergens liggen zijn alleen maar waardevol als er nergens op de wereld andere grote ronde stenen zijn.

Voor een groter economisch stelsel is het belangrijk dat het middel dat we gebruiken voor de uitwisseling van waarde aan een paar eigenschappen voldoet. Ten eerste geven we het een naam: geld.

Geld voldoet aan de volgende eigenschappen:

- Geld is niet om op te eten
- Geld mag niet bederven
- Geld gebruik je voor niets anders, dat wil zeggen: geld is nooit onderdeel van andere spullen

Ook is het handig als geld aan de volgende eigenschappen voldoet, maar dit zijn geen ultieme voorwaarden:

- Geld is op te delen in kleinere eenheden (1 euro, 50 cent, 20 cent enzovoort)
- Geld is makkelijk te vervoeren (1 staaf goud is niet makkelijk te vervoeren, kleine stukjes of muntjes van goud wel)
- Geld behoudt zijn waarde (dit kun je als voorwaarde zien, maar is niet in alle gevallen nodig)
- Geld is lastig om te vernietigen

Als je de voorgaande alinea's even tot je door laat dringen, bedenk je waarschijnlijk dat er niet veel dingen goed als geld kunnen functioneren. Het is best lastig iets te vinden dat aan alle voorwaarden en eigenschappen voldoet. Maar de mens zou de mens niet zijn als daar nooit een oplossing voor kwam en die kwam in de vorm van edelmetalen. Goud, zilver en koper. Sommige munteenheden hebben het eeuwen volgehouden, zoals de florijn die voor het eerst in 1252 in Florence geslagen werd. De munt werd praktisch overal in Europa erkend, had een vaste waarde en werd op heel veel verschillende plekken gemaakt of gemunt. Zo'n munt moest dan aan dezelfde eigenschappen van de florijn voldoen. Hij moest bestaan uit 3,5368 gram goud. De waardevaste munt was een veilig toevluchtsoord om kapitaal in op te slaan en zorgde voor steeds groter wordende rijkdom in verschillende stadstaten in heel Europa.

Komst van de gouden standaard

We maken een grote sprong door de geschiedenis naar de gouden standaard, die in een groot aantal landen over de hele wereld vanaf 1814 werd ingevoerd. Nederland voerde vanaf 1850 een zilveren standaard en ging in 1875 over op een gouden standaard. De meest duidelijke vorm van een goudstandaard is een systeem waarbij goud ook als munteenheid wordt gebruikt. Bij de goudstandaard die in 1875 werd ingevoerd, ging het om een iets andere vorm, de goudenmuntenstandaard. Bankbiljetten werden volledig gedekt door goud en een houder van een biljet kon deze in principe inwisselen voor goud. Het muntgeld bestond uit andere metalen en was waard wat het metaal in kwestie waard was. Deze goudenmuntenstandaard werd in 1914 afgeschaft toen de Eerste Wereldoorlog uitbrak. Het afschaffen van de gouden standaard gaf landen in oorlog de mogelijkheid onbeperkt geld bij te drukken en zo de oorlog te financieren. Na de oorlog keerde een soort van gouden standaard terug. Tussen 1918 en 1936 was in Nederland nog maar 40 procent van alle bankbiljetten door goud gedekt en heette het 'goudkernstandaard'. Je kon je geld niet meer inwisselen tegen goud, behalve in speciale gevallen.

Na de Tweede Wereldoorlog was er nog een soort van goudstandaard, maar die liep via een vaste verhouding tot de Amerikaanse dollar, die op zijn beurt weer aan goud was gekoppeld. Dit liep via het systeem van Bretton Woods en hier kwam in 1971 een einde aan toen Amerika de dollar loskoppelde van goud om de Vietnamoorlog te bekostigen (lees: om geld bij te drukken).

Ik wil hier niet een verhandeling gaan houden over de verschillende economische denkrichtingen. Wij zitten in een tijd waarin inflatie als sturend middel gebruikt

wordt en mensen geld uit moeten geven omdat het anders minder waard wordt. Een andere denkrichting is dat dit niet handig is en dat geld altijd dezelfde waarde moet hebben. De bedenker van bitcoin komt uit die laatste school. We kunnen ook niet ontkennen dat ondanks de inflatie centrale banken nog steeds goud achter de hand houden, ook al gebruiken we de goudstandaard niet meer.

Waarom goud?

We komen bijna bij 'waarom cryptovaluta', maar eerst moeten we deze vraag nog beantwoorden: waarom goud? Je begrijpt inmiddels dat goud al eeuwen wordt gezien als belangrijke grondstof met een vrij vaste waarde per hoeveelheid en het is daarom een goede manier om rijkdom in op te slaan. Dit heet ook wel *store of value*.

Hoe kan het zijn, dat een stof die eigenlijk nergens goed voor is, behalve voor sieraden en sinds heel kort in bepaalde elektronica, toch een waarde vertegenwoordigt? Dit gaat allemaal terug op het lijstje van voorwaarden, dat waardeopslag moet zitten in iets dat niet mag bederven, dat je niet kunt opeten, dat je nergens anders voor kunt gebruiken en dat het waardevast is.

Waardevastheid is heel lastig te verkrijgen. Iets is waardevast als het aan alle eigenschappen uit het eerste lijstje voldoet en er ook nog de mogelijkheid is om te weten hoeveel je er in de toekomst nog van kunt verkrijgen.


VOORBEELD

Stel, stenen zijn bijzonder, want je woont op een eiland met alleen maar bomen en zand. Die stenen komen van een ander eiland dat alleen met een boot bereikbaar is. Op jouw eiland zonder stenen is een steen moeilijk te vermeerderen, omdat je alleen maar kleine bootjes hebt. Totdat iemand een grote boot weet te bouwen die veel meer kan vervoeren en verder kan varen en ineens heel veel stenen kan leveren. Ineens blijken stenen te bestaan in een vrijwel onuitputtelijke hoeveelheid. Daar gaat de waarde van je stenen.

Dit klinkt natuurlijk als een flauw voorbeeld, maar het is afgeleid van een voorbeeld rond het eiland Yap. Als je dit voorbeeld doortrekt naar andere grondstoffen, dan zie je al snel dat vrijwel niets meer in aanmerking komt voor een waardevaste investering. Goud is dat tot nu toe nog steeds. Dit komt doordat de bestaande voorraad maar heel langzaam groter wordt en doordat we weten dat er in de toekomst niet bijzonder veel meer van gevonden zal worden. Dit heet de verhouding voorraad-tot-stroom, een vrije vertaling/interpretatie van *stock to flow*-ratio.

Verhouding voorraad-tot-stroom

Je ziet al dat als je een grondstof hebt waarmee je snel veel meer van iets kunt maken, daardoor de waarde ook snel zal dalen. Om te berekenen of iets voor langere tijd zijn waarde zal behouden, is er de verhouding (ratio) voorraad-tot-stroom. Voorraad is daarbij de bestaande voorraad (alles dat is geproduceerd in het verleden minus alles dat inmiddels is vernietigd) en 'stroom' is wat er in de toekomst nog gemaakt zal worden. Hoe makkelijker je iets kunt vermeerderen, hoe lager de verhouding voorraad-tot-stroom (oftewel de ratio).

VOORBEELD

Je hebt 10 munten en je kunt heel makkelijk 20 munten bijmaken. Dan is de verhouding 0,5 oftewel: 10:20. Als je er maar 5 bij kunt maken, dan is de verhouding hoger: 10:5=2. Bij munteenheden geldt dus: hoe hoger de verhouding, hoe sterker de munt. In jargon heet dat een 'harde munt'. Iedereen die zich de tijd voor de euro nog kan herinneren, weet bijvoorbeeld nog dat de gulden en Duitse mark harde munten waren: ze hadden een lage inflatie en daardoor een hoge waarde ten opzichte van andere munten waar er meer van bijgeslagen en/of –gedrukt werden. Ze waren dus goed om voor langere tijd waarde in op te slaan als je zelf in een land leefde waar de munt snel in waarde daalde.

De waarde die iets heeft, is dus afhankelijk van deze verhouding. Als meer mensen een harde munt kiezen om hun tegoeden in op te slaan, wordt deze munt ook meer waard omdat er veel vraag naar is. Als je de maker van zo'n munt bent, is het heel verleidelijk om meer van zo'n munt te produceren. Als dat technisch niet mogelijk is, ben je ook geen bedreiging voor de waarde, omdat die niet ineens in kan storten omdat de maker er ineens heel veel van bij drukte. Je wilt dus iets dat moeilijk is om te maken en lastig is om te vernietigen.

Nu stop ik met het lesje geschiedenis van het geld. Sinds de laatste kredietcrisis zijn er veel dikke boeken verschenen over geld en hoe dat wel of niet moet functioneren. Een van mijn favorieten in dat rijtje is van antropoloog David Graeber, het boek *Schuld, de eerste 5000 jaar.* Maar er is natuurlijk veel meer interessants te lezen.

Harde munt in een wereld zonder schaarste

Je hebt net gelezen dat de waarde van geld niets te maken heeft met emotionele waarden, maar alles met afspraken. Die afspraken zijn: niet om op te eten, niet bederfelijk, niet voor iets anders geschikt dan waardeuitwisseling, op te delen in kleinere eenheden, lastig om te vernietigen, makkelijk over te dragen en niet makkelijk te vermeerderen.

In de digitale wereld is de afspraak 'niet makkelijk te vermeerderen' een van de moeilijkste zaken om na te komen. Denk maar aan de muziekindustrie die bijna ten onder ging aan kopieergedrag.

Onze digitale wereld heeft niet zo veel aan goud. Het past niet door koperen draden of glasvezelkabels. We moeten dan maar vertrouwen op derde partijen zoals banken en overheden. Die partijen bleken niet lang geleden verre van onfeilbaar voor het opslaan van waarde tijdens de kredietcrisis. Allemaal een eigen baar goud aanschaffen en in de kluis leggen is ook geen optie. Is er geen betere manier om digitale schaarste te creëren? Hoe zouden we dat voor elkaar moeten krijgen? En nog sterker: kun je beter zijn dan goud?

Digitaal beter dan goud

Waarom wil je beter zijn dan goud met je schaarste? Omdat goud schaars is op aarde, maar we hebben geen idee hoeveel goud er eigenlijk nog in de bodem zit. We hebben geen idee hoeveel goud we nog vinden als we grondstoffen gaan delven op meteoren en andere planeten. De voorraad-tot-stroomverhouding van goud zal er niet heel snel drastisch op achteruit gaan, maar we kunnen digitale systemen verzinnen die écht eindig zijn en waar je echt moeite voor moet doen om het digitale goed te bereiken. En daar is hij dan eindelijk: de bitcoin.

Het systeem van bitcoin is zo ingericht dat er maximaal 21 miljoen bitcoins gemaakt kunnen worden door een systeem van computers die daarvoor rekenkracht in moeten zetten. Dit systeem heet in jargon **mijnen** of delven. De analogie met het zoeken naar grondstoffen is duidelijk: het kost moeite om bitcoins te verkrijgen. Eerst ging het makkelijk, toen waren ze ook nog verre van een harde munt, want de voorraad-tot-stroomratio was heel laag. Dat mijnen van die bitcoins wordt steeds moeilijker en ook steeds duurder. Reken maar na: toen er 1000 bitcoins waren, konden er nog 20.999.000 gedolven of gemijnd worden. 1000:20999000=0,000047621. Op het moment van schrijven zijn er 17.282.713 bitcoins in omloop en kunnen er nog 3.717.287 gemijnd worden. Een verhouding van 4,65.

Waarin verschilt bitcoin nog meer van goud en zilver? Dat zit hem in het werkelijke bezit. Goud en zilver worden verhandeld, maar niet werkelijk verplaatst. Als je goud koopt, koop je een claim, zonder dat je werkelijk weet of je het hebt. Als je dit goud zou willen bezitten, moet je door heel wat hoepels van banken en overheden springen om het bij je thuis op de schoorsteenmantel te kunnen zetten. Als je bitcoins krijgt, dan zijn die echt onder jouw eigen beheer.

Het begin van een nieuwe geschiedenis

Bitcoin heeft al geschiedenis geschreven in de zoektocht naar een digitaal betaalmiddel dat functioneert als contant geld. Dit systeem is door een tot nu toe onbekende persoon met het pseudoniem Satoshi Nakamoto aan de wereld gegeven in de vorm van opensourcesoftware. Hij of zij wist(en) de eigenschappen van een schaars goed te simuleren in de digitale wereld. Daarmee heeft Satoshi Nakamoto een mogelijkheid gegeven aan mensen om in de digitale wereld direct en definitief een waardetransactie te doen, praktisch zonder vertraging en zonder dat het nodig is dat beide partijen dicht bij elkaar in de buurt zijn of dat de partijen elkaar kennen of vertrouwen. Een soort van contant geld in de digitale wereld zonder grenzen. Onze wereld.

Dit systeem is nu al vele duizenden keren gekopieerd in vele cryptovaluta. Bitcoin heeft ten opzichte van al die kopieën een bijzonder voordeel: bitcoin heeft geen leider en niemand bezit het bitcoin-netwerk of kan dit claimen of aansturen. Het bitcoin-netwerk is een verdeeld **peer-to-peer-netwerk** zonder een enkel punt waar het netwerk kan falen. Elke computer in het netwerk, ook wel **node** genoemd, heeft de beschikking over alle transacties die ooit zijn gedaan in dit systeem. Al die transacties zijn gecontroleerd met **digitale handtekeningen** en vastgelegd met digitale sleutels en een systeem dat *proof-of-work* heet.

Het maken van de nieuwe muntjes kost energie. De eerste keer dat een waarde werd toegekend aan bitcoin was door de energiekosten per bitcoin te berekenen, toen 0,0008 cent per bitcoin of 1309,03 bitcoin per dollar. Sommigen vinden de energievraag van het netwerk groot, maar de veiligheid van het netwerk speelt ook een rol. De vraag is waar je energie voor over hebt. Je tv of een superveilig netwerk?

De belangrijkste niet-technische eigenschap van het bitcoin-netwerk is dat het niet politiek is en geen eigenaren heeft. Iedereen mag meedoen, niemand moet meedoen. Het lot van het netwerk ligt in handen van de gebruikers. Door de werking van het systeem kan de toegang niet geblokkeerd worden door overheden of andere instanties. Het netwerk kijkt niet wie of wat iemand is en is in die zin neutraal. Daarmee is bitcoin een krachtig middel, omdat het monopolie van geldschepping ineens niet meer bij banken en overheden ligt. Niemand verplicht je om bitcoins te gebruiken.

Het gaat te ver om hier nog heel veel dieper op in te gaan in dit boek. Ik hoop dat je hierdoor beter begrijpt waarom bitcoin door velen als een interessant beleggingsobject gezien wordt en niet zozeer als handig online betaalmiddel. Daarvoor is het systeem te log, niet in de laatste plaats om de veiligheid te waarborgen. We zullen verderop in dit boek gaan zien dat het ook mogelijk is om systemen aan bitcoin te koppelen via zijketens of *side-chains*, zodat je wel miljoenen betalingen per seconde kunt verwerken en dat dit niet direct op het bitcoin-netwerk hoeft te gebeuren, zoals met de inmiddels goed functionerende tweede laag, het lightning-netwerk.

Wil je meer weten over de filosofie rond bitcoin en andere online betalingssystemen, lees dan *The Bitcoin Standard* van Saifedean Ammous en *Streaming Money* van Andreas Antonopoulos.