BITCOIN IN 10 MINUTES

Alles wat je altijd al wilde weten over Bitcoin

Brought to you by Relai

WAT IS BITCOIN?

Bitcoin, ,s werelds succesvolste cryptogeld, is wereldwijd in het nieuws. Velen willen profiteren van het succes, anderen zijn onverschillig of zelfs sceptisch. De digitale munt heeft talloze discussies losgemaakt over geld, investeren en technologie. Sommigen zien Bitcoin als een puur speculatiemiddel of veroordelen het als een zeepbel, terwijl anderen spreken van vernieuwing, een monetaire revolutie of zelfs verlossing van het huidige monetaire systeem.

Verschillende landen, waaronder China, zien Bitcoin als een bedreiging en hebben de oorlog verklaard aan het cryptogeld. Andere regeringen, zoals die van El Salvador, hebben Bitcoin ingevoerd als officieel betaalmiddel in de hoop op economische groei.

Maar wat is Bitcoin? Is het geld? Digitaal goud? Een rage voor computerwetenschappers en speculanten? Of iets heel anders? In de volgende paragrafen gaan we dieper in op deze vragen en nemen we de digitale munt onder de loep om de filosofie en functionaliteit achter Bitcoin beter te begrijpen. Daarvoor is het belangrijk om bij het begin te beginnen: met het verhaal over de oorsprong van Bitcoin.

HET VERHAAL VAN BITCOIN

Het begin van Bitcoin gaat terug tot het begin van de jaren negentig. In 1992 begon een groep computerwetenschappers in Californië een e-maillijst om ideeën uit te wisselen met gelijkgestemden over cryptografie, wiskunde, politiek en filosofie. Ze noemden zichzelf 'Cypherpunks' - een woordspeling op cyberpunk (persoon in de sciencefictionliteratuur die sceptisch staat tegenover de maatschappij - en terecht) en cipher (versleutelen).

De Cypherpunks

De Cypherpunks groeiden al snel uit tot een bont gezelschap. Ondanks hun verschillende achtergronden werden ze verenigd door de overtuiging dat het internet binnenkort een van de meest betwiste strijdperken voor menselijke vrijheid zou worden.

Om zich te beschermen tegen de dreiging van controle, toezicht en censuur op het internet, en een vrij en open internet te behouden, gebruikten de Cypherpunks een krachtig wapen: cryptografie, het versleutelen van informatie.
In hun manifest van 1993 stelden ze: „Cypherpunks schrijven [computer] code. We weten dat iemand software moet schrijven om de privacy te verdedigen, en [...] we gaan het schrijven."

Maar cryptografie alleen zou niet genoeg zijn voor een vrij internet. Want, en daar waren de Cypherpunks van overtuigd, het internet kan niet echt vrij zijn als het geen eigen geld heeft. Geld dat onafhankelijk is van landen, centrale banken en bedrijven; cryptogeld zo eerlijk en gedecentraliseerd als het internet zelf.

Monetaire Experimenten

Maar de ontwikkeling van onafhankelijk, digitaal geld stelde de Cypherpunks voor technische uitdagingen. Al in 1990 had cryptoloog David Chaum eCash ontwikkeld, het eerste cryptogeld, wat niet gedecentrali-

seerd was maar dankzij cryptografie anonimiteit garandeerde. eCash kon zich echter op lange termijn niet handhaven tegenover andere online betaalsystemen. Het bedrijf achter het project moest na 8 jaar faillissement aanvragen en eCash verdween.

Andere pogingen volgden, waarvan E-Gold eruit sprong. E-Gold was cryptogeld gedekt door goud wat voor iedereen beschikbaar was. Opgericht tijdens het dotcomtijdperk in 1996, sloeg het bedrijf aan bij zijn gelijken en verwerkte op zijn hoogtepunt meer dan twee miljard Amerikaanse dollars aan transacties per jaar.

Maar E-gold werd gecontroleerd door een centrale instelling en was dus kwetsbaar voor aanvallen. Er volgden al snel juridische problemen en de Amerikaanse regering ondernam gerechtelijke stappen tegen E-Gold. In 2008 werd E-Gold door een Amerikaanse rechtbank schuldig bevonden aan het witwassen van geld en schendingen van de Patriot Act. Alle bezittingen werden bevroren en E-Gold moest zijn activiteiten staken.

Deze mislukte pogingen hebben de Cypherpunks twee dingen laten zien. Ten eerste werden zowel eCash als E-gold gedekt door onderpand. Dit onderpand was een zwakke plek gebleken, omdat het door landen in beslag kon worden genomen. Daarom zou een vrij cryptogeld geen centrale aanvalspunten moeten hebben zoals een geregistreerd bedrijf, een bankrekening of een gecentraliseerde serverlocatie. En ten tweede hebben overheden en toezichthouders geen belang bij onafhankelijk digitaal geld.

Voor de Cypherpunks bleef de basisvraag, waarvoor nog geen oplossing was gevonden: hoe kan onafhankelijk digitaal geld werken zonder een centrale partij die de boeken bijhoudt en ervoor zorgt dat geld niet dubbel wordt uitgegeven? Want als het mogelijk zou zijn om het probleem van dubbele uitgaven op te lossen zonder afhankelijk te zijn van een centrale partij, dan zou het misschien mogelijk zijn om vrij digitaal geld te creëren dat verweven is met het internet.

Een mysterieuze geboorte

Daarom begonnen de Cypherpunks te discussiëren over ontwerpen van cryptogeld zonder centrale partij en onderpand. Twee van de belangrijkste concepten waren b-money (1998) en BitGold (2005). Deze theoretische ideeën, die nooit in praktijk werden gebracht, leken qua ontwerp al sterk op Bitcoin. Er werd gedacht aan asymmetrische cryptografie voor encryptie en Proof-of-Work (bewijs van werk) voor het aanmaken van extra digitale munten, zoals ook bij Bitcoin het geval is. In zijn Whitepaper bevestigde de uitvinder van Bitcoin ook dat hij op de hoogte was van b-money en BitGold.

Omdat b-money en BitGold echter vertrouwden op een stemsysteem voor consensus (de overeenstem-

ming over wie welke monetaire eenheden op dit moment bezit), waren ze kwetsbaar voor kwaadaardige aanvallen die dergelijke verkiezingen konden manipuleren en zo het eigendom konden verstoren.

Voor dit laatste probleem, dat de creatie van nieuw internetgeld nog steeds in de weg stond, werd op vrijdag 31 oktober 2008 een oplossing gepresenteerd. Op die dag werd de Bitcoin Whitepaper, waarin Satoshi Nakamoto zijn concept voor een gedecentraliseerd betalingsnetwerk uitlegt, naar de Cypherpunks gemaild. Twee maanden later, op 3 januari 2009, ging het Bitcoin-netwerk live.

De eerste reacties op het nieuwe netwerk waren gematigd. Enkele enthousiastelingen begonnen het netwerk te testen en meldden fouten. In het begin was het echter vooral Satoshi Nakamoto zelf die het netwerk draaiende hield. Maar langzaam verspreidde het nieuws van het nieuwe internetgeld zich naar computer- en techfora en groeide de belangstelling voor het netwerk. Na een jaar telde het Bitcoin-netwerk al enkele gebruikers. Bitcoin zelf had echter nog geen waarde.

Wie is Satoshi Nakamoto?

Zowel de Bitcoin Whitepaper als de e-mailcommunicatie van de uitvinder van de Bitcoin waren ondertekend met de naam Satoshi Nakamoto. De ware identiteit van de Bitcoin-uitvinder blijft echter tot op heden onbekend, omdat zijn naam een alias lijkt te zijn. Om gelijkgestemden en later de gemeenschap van Bitcoin-ontwikkelaars aan te spreken, gebruikte Nakamoto minstens drie verschillende e-mailadressen, die hij grondig versleutelde om de ware identiteit van de afzender te verbergen.

Verschillende mensen hebben al beweerd Satoshi Nakamoto te zijn. Maar tot op heden is ieder van hen er niet in geslaagd dit te bewijzen. Want het ultieme bewijs, namelijk het versturen van Bitcoin vanaf een van de Bitcoinadressen die hoogstwaarschijnlijk aan Satoshi toebehoren, is nog door niemand geleverd.

Bovendien is de groep van degenen die „persoonlijk“ met Satoshi Nakamoto hebben gecommuniceerd via het internet erg klein. Satoshi Nakamoto schreef zijn laatste bericht aan de Bitcoin-gemeenschap op 12 december 2010, maar dit was geen afscheidsbericht – Satoshi stopte daarna gewoon plots met communiceren. Zijn terugtrekking was echter alleen naar de bredere gemeenschap. Nakamoto bleef een kleine groep hoofdontwikkelaars om zich heen verzamelen en informeerde hen over de verdere ontwikkeling van het Bitcoin-netwerk. Maar in april 2011 stuurde hij ook aan deze groep een laatste bericht. Net zo mysterieus als Nakamoto in 2008 verscheen, verdween hij drie jaar later weer.

Bitcoin‘s “Pizza Dag”

Maar hoe kreeg Bitcoin eigenlijk waarde? In het begin kon Bitcoin worden gemined en heen en weer gestuurd tussen leden van het netwerk, maar de digitale eenheden hadden geen waarde. Ook was de groep die Bitcoin kende, laat staan kon versturen en ontvangen, nog erg klein.

Dit veranderde op 22 mei 2010, toen er een ongewoon verzoek verscheen op het internetforum bitcointalk.org. Een 28-jarige man genaamd Laszlo Hanyecz uit Florida bood 10.000 Bitcoin aan degene die twee pizza‘s bij hem thuis zou laten bezorgen. Een Californische student nam het aanbod aan en liet twee grote pizza‘s ter waarde van 41 dollar bij hem thuis bezorgen. In ruil daarvoor stuurde Hanyecz hem de 10.000 Bitcoin.

Sinds die dag wordt 22 mei jaarlijks door Bitcoiners gevierd als Bitcoin „Pizza Day“. De dag werd populair omdat het drie dingen illustreert:

- Bitcoins hebben waarde
- Bitcoins zijn geschikt als ruil- en betaalmiddel
- Bitcoin als valuta is onderhevig aan deflatie. Het aantal extra Bitcoin dat in omloop wordt gebracht neemt gestaag af, waardoor de waarde kan stijgen.

De twee pizza‘s zijn de geschiedenisboeken ingegaan als de duurste ter wereld. Als je hun kosten berekent met de Bitcoinprijs van december 2021 is er een ongelooflijke 460 miljoen dollar voor betaald. Dat is veel geld, maar de ontvanger van de 10.000 Bitcoin heeft ze ook al uitgegeven. In een interview verklaarde hij dat hij de Bitcoin niet lang daarna had verkocht om een roadtrip te betalen – bij de huidige Bitcoinprijs waarschijnlijk ook de duurste roadtrip in de menselijke geschiedenis.

De Bitcoin „Pizza Dag“ illustreert ook op indrukwekkende manier waarom „hodling“ – afgeleid van „to hold“ (vasthouden) – zo populair is onder Bitcoiners. Hodling‘ betekent dat de bezitter zijn Bitcoins gedurende langere tijd bewaart met de bedoeling ze (mogelijk) nooit te verkopen. Immers, wie wil zijn Bitcoin vandaag uitgeven als hij in de komende jaren twee, drie of zelfs tien keer zoveel waard kan zijn?

HOE WERKT BITCOIN?

Nadat we de geschiedenis van Bitcoin hebben leren kennen, duiken we nu in de werking ervan. Het doel is te begrijpen hoe het Bitcoin-netwerk werkt, welke problemen het oplost en wat de praktische voordelen ervan zijn.

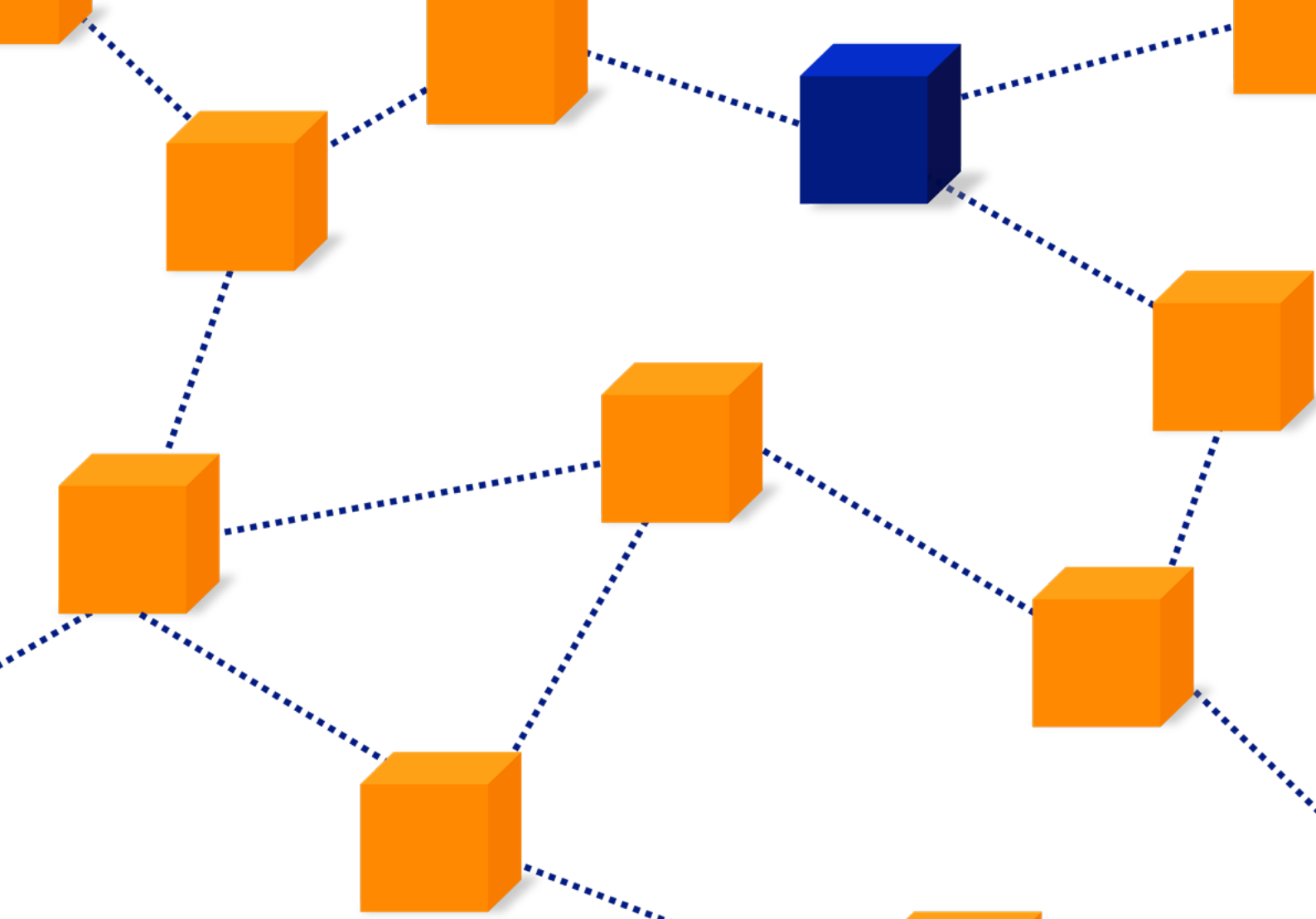
De bedoeling van Bitcoin is een gedecentraliseerd netwerk te zijn. Geen enkele deelnemer aan het netwerk mag het netwerk alleen besturen – de beslissingsbevoegdheid en het toezicht zijn verdeeld over alle deelnemers. Dit is belangrijk omdat geen enkel individu, geen enkele regering en geen enkel bedrijf het netwerk zelfstandig kan veranderen. Veranderingen zijn alleen collectief mogelijk.

Bitcoin werkt zo dat elke deelnemer aan het netwerk altijd een identieke kopie heeft van het actueelste kasboek – daardoor weet iedereen altijd wie welke Bitcoins bezit. Niemand kan dus beweren dat hij meer Bitcoin bezit dan hij daadwerkelijk heeft, omdat elke netwerkdeelnemer deze bewering kan toetsen aan zijn kopie van het kasboek en kan bewijzen dat deze onjuist is.

Voordat Bitcoin werd gelanceerd, stonden decentrale netwerken voor twee grote uitdagingen. Ten eerste, hoe kan ervoor worden gezorgd dat alle deelnemers de laatste updates krijgen over veranderingen in eigendom – dat wil zeggen, de informatie over welke Bitcoins zijn overgedragen en aan wie. En ten tweede, hoe kunnen deelnemers met absolute zekerheid verifiëren of de informatie die ze ontvangen correct is.

De Blockchain (Nederlands: blokketen)

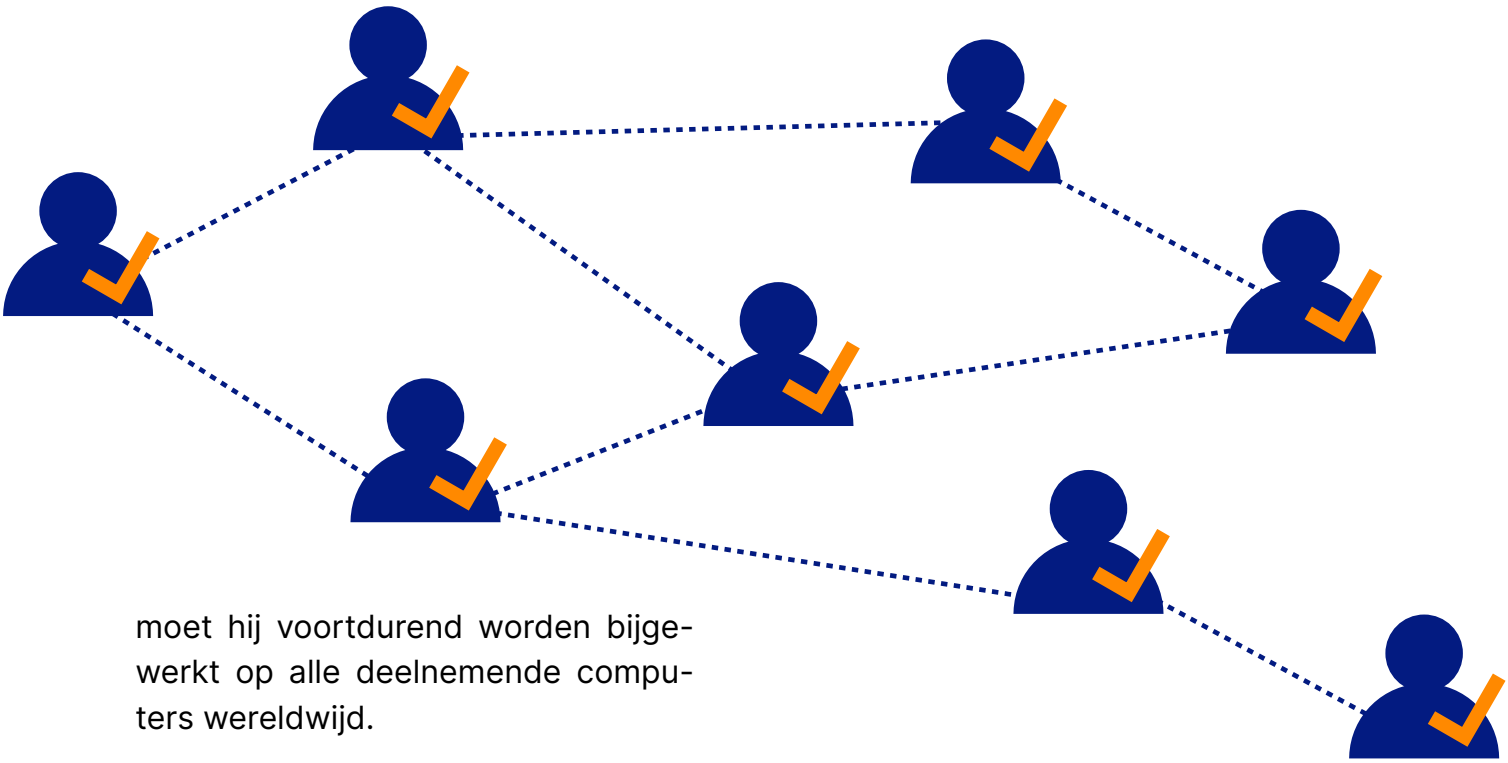
Deze moeilijkheden zijn overwonnen dankzij de uitvinding van de blockchain. Een blockchain slaat informatie en gegevens op in chronologische volgorde. In het geval van Bitcoin worden alle transacties sinds het ontstaan van Bitcoin in chronologische volgorde opgeslagen in tienduizenden blokken, die samen de Bitcoin-blockchain vormen. Elke netwerkdeelnemer die wil weten wie welke Bitcoin bezit, kan de transactiegeschiedenis op de Bitcoin-blockchain nagaan en precies bepalen wie hoeveel Bitcoins op dit moment bezit. Als iemand dus een Bitcoin wil versturen, kan iedereen nagaan of deze



Bitcoin daadwerkelijk aan de persoon in kwestie toebehoort.

Tot zover is dit mechanisme niets nieuws, aangezien banken een soortgelijk proces gebruiken. Als een klant een euro wil uitgeven, kijkt de bank in de transactiegeschiedenis of de euro nog aan de klant toebehoort of al is uitgegeven (naar iemand anders gestuurd). Het unieke kenmerk van een blockchain is echter dat deze informatie niet wordt opgeslagen op een centrale bankserver, maar op de computers van alle netwerkdeelnemers (zogenaamde volledige nodes) en dus wereldwijd in tienduizenden kopieën bestaat. Dit is ook de reden waarom Bitcoin niet zomaar kan worden gewist – daarvoor zou men de blockchainkopie van alle deelnemende computers wereldwijd tegelijkertijd moeten wissen.

De uitdaging voor blockchain is echter dat elke netwerkdeelnemer met absolute zekerheid moet kunnen vaststellen dat zijn kopie van de blockchain correct is en dat er geen foutieve of frauduleuze transactie in zijn kopie van het kasboek terechtkomt. Omdat elke 10 minuten nieuwe blokken met nieuwe transacties aan de blockchain worden toegevoegd, groeit de blockchain voortdurend en



moet hij voortdurend worden bijgewerkt op alle deelnemende computers wereldwijd.

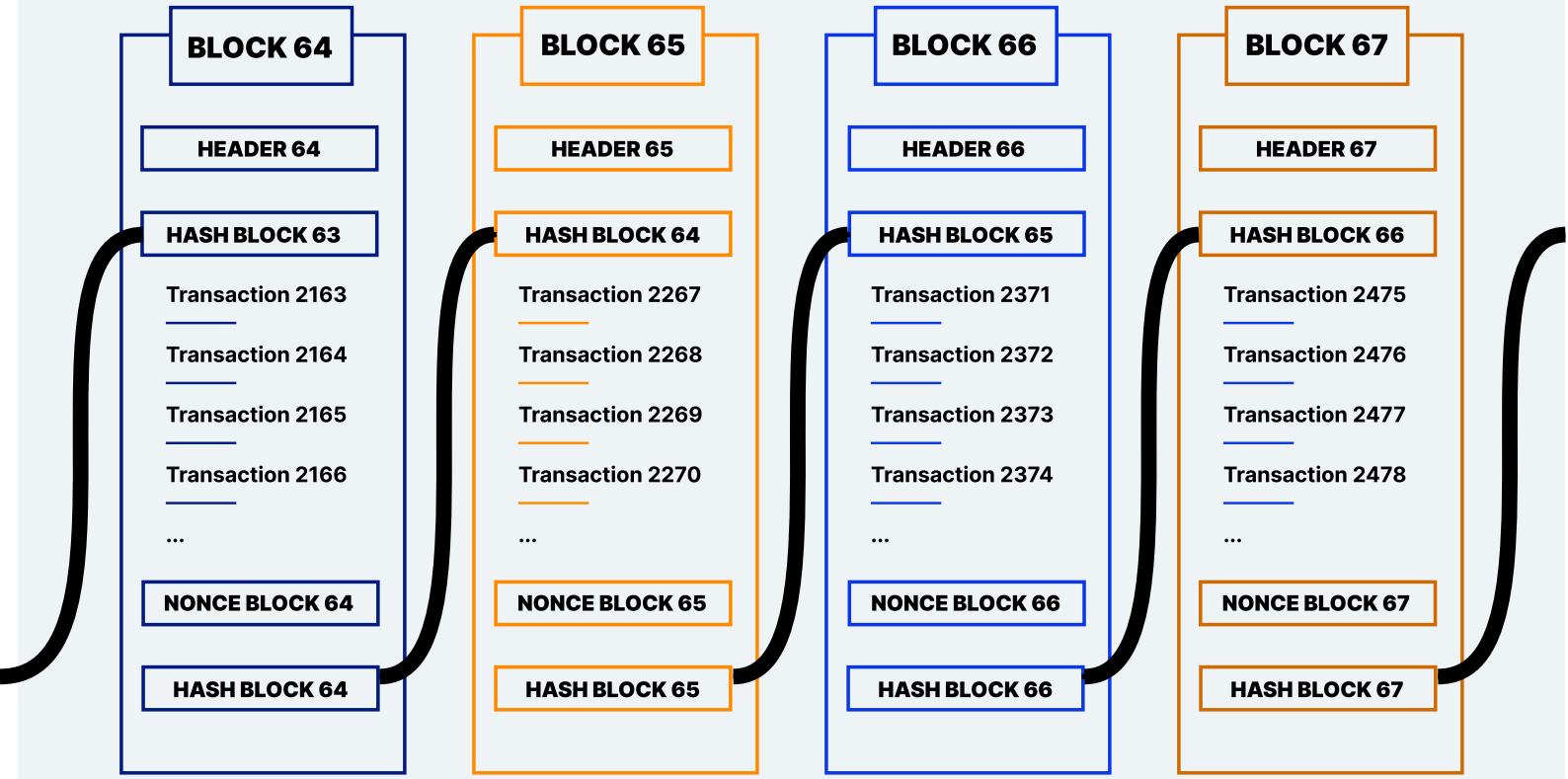
Deze nieuw toegevoegde blokken moeten door iedereen verifieerbaar zijn. De verificatie gebeurt aan de hand van onveranderlijke regels die zijn vastgelegd in de computercode van het Bitcoin-netwerk. Deze regels bepalen precies welke transacties zijn toegestaan en welke niet. Iedere gebruiker die de kopie van de blockchain downloadt, kan dus nagaan of alle transacties voldoen aan de gegeven regels. Als een transactie de regels overtreedt, d.w.z. als ze onjuist of frauduleus is, wordt ze door de netwerkdeelnemers (volledige nodes) verworpen en niet opgenomen in de blockchain.

Proof-of-Work (bewijs van werk) Mining

Bovendien heeft het Bitcoin-netwerk een mechanisme om het toevoegen van nieuwe blokken te beperken. Als iedereen nieuwe transacties en blokken aan de blockchain zou kunnen toevoegen, zou het netwerk in chaos belanden, omdat de blockchain zichzelf wereldwijd niet snel genoeg overal naar dezelfde staat zou kunnen bijwerken.

Om dit te voorkomen werkt Bitcoin met een Proof-of-Work mechanisme. Wil iemand het recht verdienen om een nieuw blok aan de blockchain toe te voegen, dan moet hij een bewijs van werk leveren. Een eenvoudige illustratie van dit proces is een groep mensen die zoekt naar naalden in een hooiberg. Wie als eerste een naald vindt, mag een nieuw blok aan de blockchain toevoegen. Bovendien wordt de vinder beloond met nieuwe Bitcoin-eenheden en de transactiekosten die dit blok bevat. Zodra het blok is bevestigd, begint dit proces opnieuw.

In werkelijkheid voeren miners een wiskundige hashfunctie (SHA-256 hashalgoritme) uit in de zoektocht naar specifieke getallen. Het hashnummer van het vorige blok, de



Het resultaat van de hashfunctie van het vorige blok, alle transacties van het huidige blok en een Nonce (willekeurig getal) worden in een wiskundige functie gestopt. De Nonce wordt veranderd totdat het resultaat van de hashfunctie genoeg voorloopnullen heeft. Dit proces wordt mining genoemd.

transacties van het huidige blok en een willekeurig getal (zogenaamde ‚nonce') worden samen gehasht. Het willekeurige getal wordt gewijzigd totdat de hashfunctie een resultaat met een minimum aantal voorloopnullen oplevert. Bijvoorbeeld, blok #700000, gecreëerd op 11 september 2021, had het geldige hashnummer: 0000000000000590fc0f3eba193a27853422 0b2b37e9849e1a770ca959.

Het zoeken naar dit nummer, ook wel mining genoemd, heeft twee belangrijke functies: Ten eerste verbindt het de blokken met elkaar op een wiskundig-cryptografische manier, zodat iedereen gemakkelijk de juiste volgorde kan controleren. Tegelijkertijd maakt het Proof-of-Work mechanisme het vrijwel onmogelijk om deze volgorde te veranderen. Ten tweede vertraagt dit mechanisme de toevoeging van nieuwe blokken, zodat gemiddeld slechts om de 10 minuten een nieuw blok aan de blockchain wordt toegevoegd. Zo krijgen alle netwerkdeelnemers wereldwijd genoeg tijd om de blockchain bij te werken naar dezelfde meest recente staat.

Kortom, miners houden het Bitcoinnetwerk draaiende. Dankzij hen worden nieuwe transacties verwerkt en toegevoegd aan de blockchain. De volledige nodes houden kopieën van het kasboek bij, zorgen ervoor dat de regels worden nageleefd, en zor-

gen ervoor dat er geen frauduleuze transacties in de blockchain terechtkomen.

21 miljoen Bitcoin

Hoewel er voortdurend meer blokken worden toegevoegd aan de Bitcoin-blockchain en miners voor dit werk worden beloond met nieuwe Bitcoins, is het totale aantal Bitcoin beperkt tot 21 miljoen. Er zullen nooit meer dan 21 miljoen Bitcoins zijn. Maar deze 21 miljoen munten waren niet vanaf het begin in omloop. Ze worden vrijgegeven door de Bitcoin-code volgens een strikt uitgifteschema.

Toen Bitcoin werd gelanceerd, gaf de code ongeveer elke 10 minuten 50 nieuwe Bitcoin vrij aan miners. Vier jaar na de lancering is het aantal Bitcoins dat per tien minuten wordt vrijgegeven gehalveerd. Dit proces heet „halveren" en beschrijft het feit dat de blokbeloning voor miners elke 4 jaar met de helft afneemt. Momenteel zijn er al 19 miljoen Bitcoin in omloop. De resterende Bitcoin zullen geminеd worden tot het jaar 2140. Daarna zullen miners alleen nog gecompenseerd worden via transactiekosten.

De strikt beperkte hoeveelheid Bitcoin-eenheden is een van de fundamentele eigenschappen van cryptogeld en maakt Bitcoin tot een uiterst schaars goed. Deze absolute digitale schaarste is ook een belangrijke voorwaarde voor de functie van Bitcoin als opslag van waarde over lange perioden en is de reden waarom Bitcoin vaak digitaal goud of goud 2.0 wordt genoemd.

Het resultaat: Digitaal eigendom

Als men alle kenmerken van het Bitcoin-netwerk samen bekijkt, ziet men het belang van deze uitvinding. Voor het eerst in de geschiedenis bestaat er een digitaal goed dat slechts in een strikt beperkt aantal beschikbaar is. Bitcoins kunnen niet worden gekopieerd of gedupliceerd.

Dankzij deze prestatie wordt Bitcoin vaak aangeduid als digitaal eigendom. Want net zoals elk stukje grond op deze aarde uniek is en maar één keer bestaat, is ook elke Bitcoin-eenheid uniek en bestaat deze maar één keer in de digitale ruimte.

En deze Bitcoin-eenheden kunnen echt eigendom zijn. Alleen de persoon die in het bezit is van de bijbehorende privésleutel, een combinatie van cijfers en letters van 64 tekens, kan de bijbehorende Bitcoin verplaatsen. Met andere woorden, zonder deze privésleutel kan de Bitcoin niet worden gestolen, in beslag genomen of geblokkeerd. Hierdoor heeft de eigenaar absolute controle over zijn financiële middelen, ongeacht of hij miljonair, politiek vluchteling of vervolgde schuldeiser is. Voor het eerst sinds de uitvinding van de computer is het mogelijk om echt digitale bezittingen te hebben.

WAAROM BITCOIN?

Maar waarom al die hype rondom Bitcoin? De mogelijkheid om echt een digitaal bezit te hebben kan revolutionair zijn. Maar waarom zou iemand eigenlijk Bitcoin willen bezitten?

Het beste van twee werelden

In voorgaande eeuwen werden edele metalen en later contant geld in de vorm van munten en bankbiljetten gebruikt als betaalmiddel. Deze hadden het voordeel dat ze onafhankelijk van derden konden worden bewaard en uitgegeven. Het gezegde "cash is printed freedom" („contant geld is gedrukte vrijheid") vat dit goed samen. Het nadeel van edele metalen en contant geld is echter dat ze moeilijk te gebruiken zijn in de digitale wereld van het internet. Sinds de opkomst van het online winkelen zijn debet- en kredietkaarten dan ook ingeburgerd bij de algehele bevolking.

Maar nu de meeste mensen digitaal geld op bankrekeningen gebruiken in plaats van contant geld, nemen de bijbehorende tegenpartijrisico's toe. Als een financiële instelling bijvoorbeeld failliet gaat, kan het spaargeld van de klanten verloren gaan. Of, zoals in 2013 in Cyprus gebeurde, als het opnemen van contant geld sterk wordt beperkt, er vermogenscontroles worden ingesteld en gedwongen onteigening op spaarrekeningen plaatsvindt, dan hebben mensen geen controle meer over hun geld. Of, zoals nu het geval is in veel westerse landen, als bankklanten geen geld mogen sturen naar familieleden omdat ze in Cuba of Iran wonen, zijn ze afhankelijk van een derde partij om al hun transacties goed te keuren.

Met de overgang van papiergeld naar digitaal geld, opgeslagen op bankrekeningen, hebben we uiteindelijk geen controle meer over ons eigen geld. Tot nu toe was dit nadeel echter de prijs die we moesten betalen

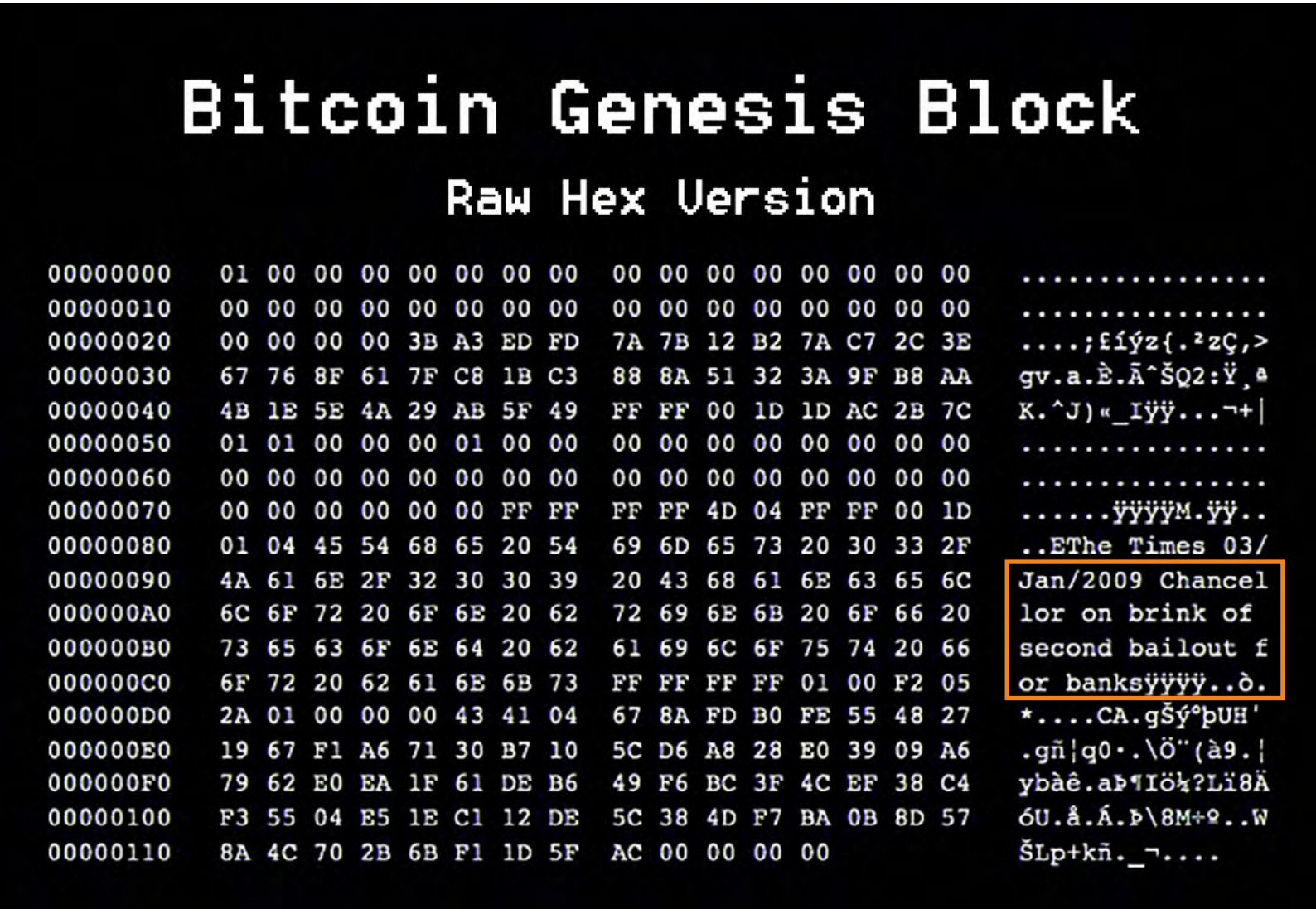
om deel te nemen aan een gedigitaliseerd leven.

Bitcoin biedt een oplossing voor dit dilemma. Als digitaal geld is het bij uitstek geschikt voor gebruik in de digitale wereld. Tegelijkertijd kan Bitcoin worden opgeslagen als digitaal eigendom zonder afhankelijk te zijn van derden (banken) voor de bewaring. Bitcoin-bezitters kunnen hun munten – in de vorm van de privésleutels – dus bewaren onder hun matras of waar ze dat het veiligst vinden.

'Perfect Timing'

Bitcoin ontstond tijdens de wereldwijde financiële crisis van 2008/09. Op het eerste blok van de Bitcoin blockchain – ook wel het Genesis blok genoemd – liet Satoshi Nakamoto een sterke boodschap achter. Hij citeerde een krantenkop van The Times: "Chancellor on brink of second bailout for banks" („Kanselier op het randje van tweede reddingsactie voor banken").

Met deze actie drukte Satoshi de staatskritische filosofie van de Cypherpunks uit. In de financiële crisis van 2008 brachten de centrale banken enorme hoeveelheden nieuw geld in omloop om de banken te redden. Maar uiteindelijk betaalden de spaarders daarvoor, want hun spaargeld verloor aan waarde door een overvloed aan geld. Dit feit bevestigde nogmaals het wantrouwen van de



Cypherpunks tegenover de staat en de centrale banken en versterkte hun overtuiging dat onafhankelijk geld dringend nodig was.

Dezelfde procedure, alleen op grotere schaal, is herhaald sinds het uitbreken van de Covid-19 pandemie. Alleen al in 2020 werd de Amerikaanse geldhoeveelheid met 50 procent uitgebreid, en ook in andere landen – waaronder Zwitserland – draait de digitale drukpers onophoudelijk. Een direct gevolg hiervan is recordlage rente – in Zwitserland zelfs negatieve rente – en sterke vermogensinflatie.

Bescherming tegen Valuta Devaluatie

Bitcoin is daarom op het beste moment gelanceerd. Zelden was de geldkwestie relevanter en waren de vraagtekens groter dan vandaag. Met zijn beperkte voorraad van 21 miljoen vormt Bitcoin een aangenaam contrast met de eindeloos groeiende balansen van de centrale banken. Zijn beperkte voorraad biedt bescherming tegen de verwatering van zijn kapitaal, zoals de afgelopen decennia bij alle valuta wereldwijd is vastgesteld.

Door zijn specifieke opzet is Bitcoin ontworpen om het behoud van koopkracht over lange perioden te garanderen. Aangezien Bitcoin schaars is, zou het zelfs beter moeten zijn in deze taak dan goud dat een netto-instroom heeft van 1-2% per jaar. Bovendien zijn de kosten voor opslag en transport van Bitcoin ook aanzienlijk lager dan die van goud, waardoor ook het waardebehoud op termijn beter is.

Eigendomsbescherming

Een ander probleem dat Bitcoin ondervangt is de bescherming van eigendom. Terwijl goud of contant geld meestal tegen hoge kosten veilig moet worden opgeslagen om het te beschermen tegen diefstal, kan Bitcoin vrijwel kosteloos worden opgeslagen en vervoerd. Zelfs aanzienlijke bedragen kunnen overal ter wereld naartoe worden meegenomen met een code van twaalf of vierentwintig woorden. Eenmaal uit het hoofd geleerd en fysiek vernietigd, kan deze code door niemand worden gestolen, waardoor de Bitcoin achter de code veilig is en de eigenaar ze desgewenst mee het graf in kan nemen.

BITCOIN KOPEN

Er zijn twee manieren om aan Bitcoin te komen. Ofwel je verdient Bitcoin als miner, of je koopt Bitcoin van een ander. Aangezien mining met thuisapparatuur tegenwoordig bijna onmogelijk is geworden blijft er voor nieuwkomers alleen nog de mogelijkheid over om Bitcoin te kopen.

Cryptobeurzen & makelaars

De eenvoudigste manier om Bitcoin te kopen is via een cryptobeurs of een makelaar. Deze werken vergelijkbaar met handelsplatforms voor aandelen. Na het openen van een persoonlijke rekening kunt u Zwitserse franken, euro's of Amerikaanse dollars overmaken via een bankoverschrijving of creditcard. Zodra het geld is aangekomen op de persoonlijke rekening bij de handelsbeurs, kan er dag en nacht met een paar klikken Bitcoin worden gekocht tegen de huidige marktprijs. In Europa is het mogelijk om Bitcoin te kopen zonder registratie, verificatie of eerst geld te storten met de populaire Bitcoin-only investeringsapp Relai.

Peer-to-peer

Als alternatief voor cryptobeurzen kan Bitcoin ook rechtstreeks van andere eigenaren worden gekocht via peer-to-peer platforms zonder tussenkomst van een beurs. Dit zorgt voor meer anonimiteit, omdat er geen persoonlijke gegevens bekend hoeven te worden gemaakt.

Bitcoin geldautomaten

Er is ook de mogelijkheid om Bitcoin op te nemen via geldautomaten. Deze zijn al beschikbaar in veel landen, waaronder Zwitserland, Duitsland en Oostenrijk. Bij Bitcoin-automaten kan de Bitcoin anoniem worden opgenomen met contant geld of een creditcard. Een account of een bestaande cryptoportemonnee is niet nodig.

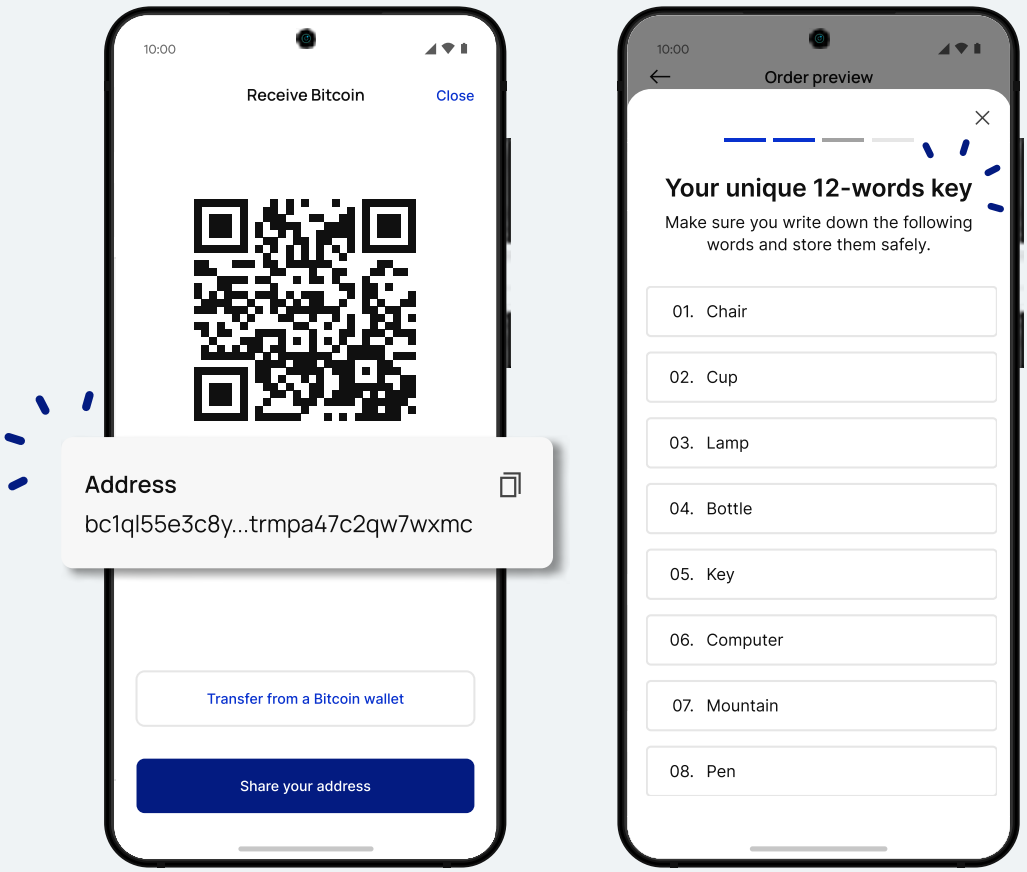
Bitcoin veilig bewaren

Na het aanschaffen van Bitcoin is de vraag hoe ze veilig gehanteerd en bewaard kunnen worden. Voor Bitcoin en cryptogeld geldt het uitgangspunt: „niet uw sleutels, niet uw munten“ („not your keys, not your coins“). Om Bitcoin echt te bezitten moet je in het bezit zijn van de bijbehorende privésleutels. Deze enigszins technische uitdrukking betekent dat je pas echt controle hebt over je Bitcoin als je ze opslaat in een persoonlijke digitale portemonnee waarvan je zelf de privésleutels hebt.

Zolang de Bitcoins bij een cryptobeurs zijn opgeslagen staan ze onder controle van de beurs. Als de beurs wordt gehackt, failliet gaat of frauduleus is, kan de Bitcoin voor altijd verloren gaan.

Zelfbewaring

In tegenstelling tot een bankrekening biedt Bitcoin je de mogelijkheid om je monetaire eenheden op te slaan in een persoonlijke portemonnee. Hierdoor kun je je eigen bank zijn en dat heeft het voordeel dat je absolute controle hebt over je Bitcoin. Daar staan ook verantwoordelijkheden tegenover. De privésleutel, vaak in de vorm van twaalf of vierentwintig woorden, moet door de eigenaar van de betreffende Bitcoin zelf op een veilige manier worden bewaard. Een onjuiste of nalatige behandeling kan leiden tot onherstelbaar verlies van Bitcoins.



Portemonnees: Digitale portemonnees

Digitale portemonnees helpen om de Bitcoin, of beter gezegd de privésleutels, veilig op te slaan. De Bitcoin zelf worden altijd opgeslagen op de blockchain en kunnen niet worden overgedragen naar een portemonnee. Alleen de toegangssleutels tot de Bitcoin kunnen worden opgeslagen in een portemonnee.

Portemonnees zijn dus in het leven geroepen om de privésleutels veilig en eenvoudig op te slaan. Bovendien kunnen ze met een paar klikken Bitcoin verzenden en ontvangen. Portemonnees zijn dus een handig hulpmiddel voor het omgaan met Bitcoin.

Software Portemonnee

De meest voorkomende portemonnees zijn software portemonnees. Software portemonnees kunnen worden gebruikt als computer applicaties of als smartphone apps. Bij het instellen worden de privésleutels van de portemonnee opgesomd in de vorm van twaalf of vierentwintig woorden (de zogenaamde „seed phrase“). Deze woorden zijn synoniem voor de Bitcoin in die portemonnee. Wie deze woorden kent, heeft controle over de munten. Daarom moeten de woorden analoog worden bewaard, bijvoorbeeld op papier, en in het geheim veilig worden opgeslagen. Mocht de computer of smartphone ooit verloren gaan of gestolen worden, dan kan de portemonnee met deze woorden altijd hersteld worden. Omdat papier verloren kan gaan wordt het aanbevolen de woorden te bewaren op een plaat van metaal.

Software portemonnees hebben het voordeel dat ze snel kunnen worden ingesteld en gemakkelijk te gebruiken zijn. Echter, omdat software portemonnees computerprogramma‘s zijn die op een apparaat zijn geïnstalleerd en rechtstreeks met het internet zijn verbonden, bestaat er altijd een risico op aanvallen van hackers.

Hardware Portemonnee

Om je Bitcoin echt goed te beschermen dan is het beter om een hardware portemonnee te gebruiken. Deze kleine apparaten bewaren de toegangscodes voor de Bitcoin op een USB-stick-achtig apparaatje dat alleen op de computer wordt aangesloten als het nodig is. Het apparaatje is zo ontworpen dat zelfs een met kwaadaardige software geïnfecteerde computer geen toegang heeft tot de codes.

Bij het opzetten van een hardware portemonnee worden twaalf of vierentwintig woorden (seed phrase) gegenereerd, die veilig analoog moeten worden bewaard. Als de hardware portemonnee ooit verloren gaat kan hij met behulp van deze woorden worden hersteld. Voorbeelden van hardware portemonnees zijn BitBox en Trezor.

Made in Switzerland

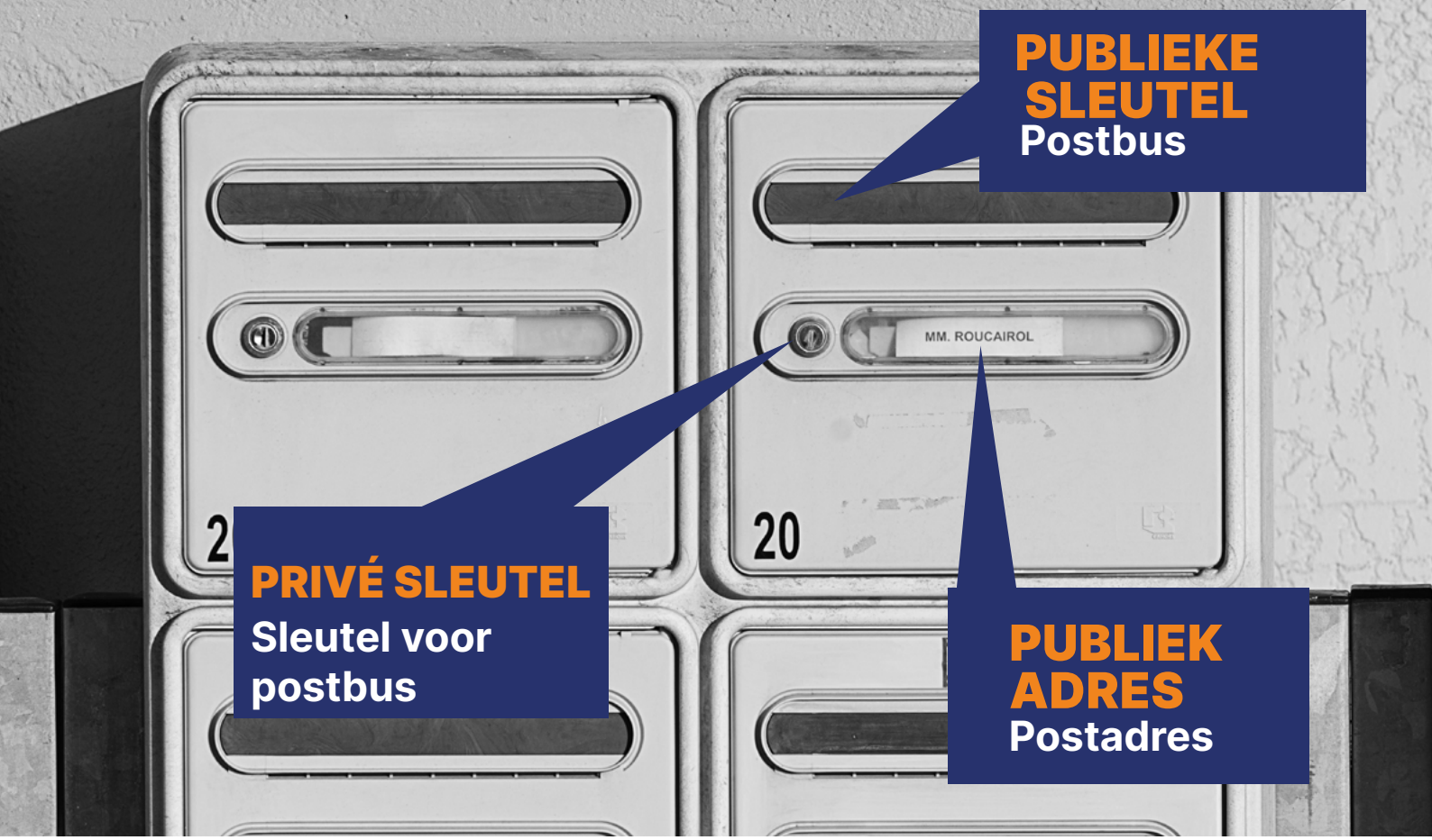
EUROPE'S EASIEST BITCOIN APP

Relai

Download on the App Store

GET IT ON Google Play

Buy bitcoin in 1 minute from as little as 10 EUR/CHF without verification.



Bitcoin verzenden en ontvangen

Het versturen en ontvangen van Bitcoin is zeer eenvoudig. Elke Bitcoin-portemonnee heeft een openbaar adres dat wordt gegenereerd uit de zogenaamde openbare sleutel. Dit dient als ontvangstadres, vergelijkbaar met een IBAN. Iedereen die dit adres heeft kan Bitcoin sturen naar de bijbehorende portemonnee. Het adres wordt vaak weergegeven als een QR-code wat de afhandeling verder vereenvoudigt.

Als je Bitcoin naar iemand wilt sturen kan je het Bitcoin-adres van de ontvanger in je portemonnee invoeren onder ‚verzenden' of de bijbehorende QR-code scannen. De transactiekosten worden automatisch afgetrokken van de portemonnee van de verzender. De hoogte van de transactiekosten hangt af van de belasting van het netwerk en kan je hier opzoeken. Het duurt gemiddeld 10 minuten voordat de Bitcoin is overgemaakt naar de ontvanger. Het kan echter ook langer duren, dit is afhankelijk van de transactiekosten die je bereid bent te betalen.

Betalen met Bitcoin

Toen Bitcoin werd gecreëerd, hoopte men dat Bitcoin ooit zou kunnen worden gebruikt om alledaagse goederen te betalen. En in theorie is dit vandaag de dag mogelijk. Sommige non-profitorganisaties en een groeiend aantal bedrijven accepteren Bitcoin als betaalmiddel. Maar omdat transacties via het Bitcoin-netwerk meerdere euro's kunnen kosten en minstens 10 minuten duren, heeft dit alleen zin voor grotere bedragen. Om Bitcoin goedkoop en snel te versturen is een alternatieve oplossing nodig.

Lightning netwerk - sneller en goedkoper

Daarom werd er een extra laag gebouwd bovenop het Bitcoin-netwerk. Dit netwerk, genaamd Lightning, maakt het mogelijk om binnen enkele seconden met Bitcoin te betalen tegen minimale kosten. In landen als El Salvador wordt het Lightning-netwerk al actief en succesvol gebruikt.

Het betalen van alledaagse goederen met Bitcoin zal in de toekomst dan ook grotendeels via het Lightning-netwerk plaatsvinden. De ontwikkelingen op dit gebied draaien op volle toeren. Zo introduceerde Twitter kortgeleden een ‚tip'-functie die gebruik maakt van het Lightning-netwerk. Verder biedt de app Strike wereldwijde betalingen in verschillende valuta's aan zonder kosten via het Lightning-netwerk. Het is dan ook te verwachten dat in de toekomst alleen grotere bedragen direct via het Bitcoin-netwerk zullen worden verrekend, terwijl alle andere transacties via het Lightning-netwerk zullen lopen.

Omdat vooral kleinere bedragen via het Lightning-netwerk worden verrekend, worden Satoshis, of kortweg Sats, gebruikt als rekeneenheid in plaats van Bitcoin. 1 Bitcoin is gelijk aan 100.000.000 Satoshis. Om het Lightning-netwerk te gebruiken, moet een Lightning-portemonnee worden aangemaakt.

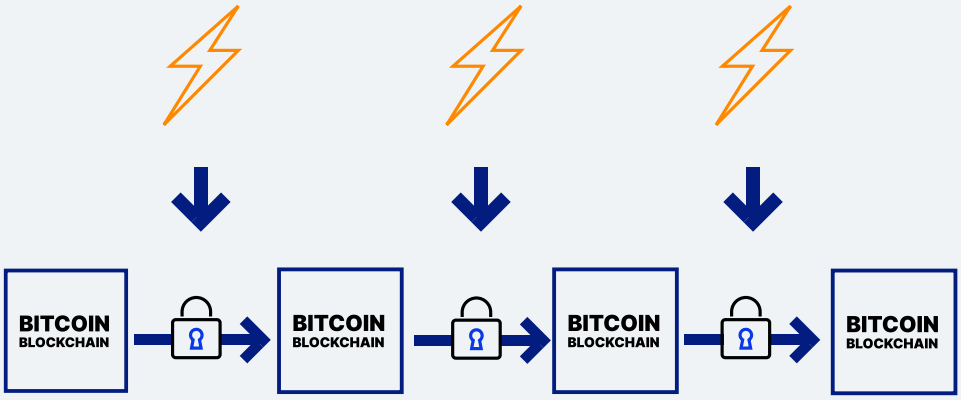
EEN BLIK IN DE TOEKOMST

In de ruim tien jaar van zijn bestaan heeft de Bitcoin vele hoogte- en dieptepunten gekend. De cryptovaluta werd verschillende keren doodverklaard of raakte in de vergetelheid bij het grote publiek na zware prijsverliezen. Toch heeft Bitcoin zich het afgelopen decennium onverbiddelijk over de wereld verspreid.

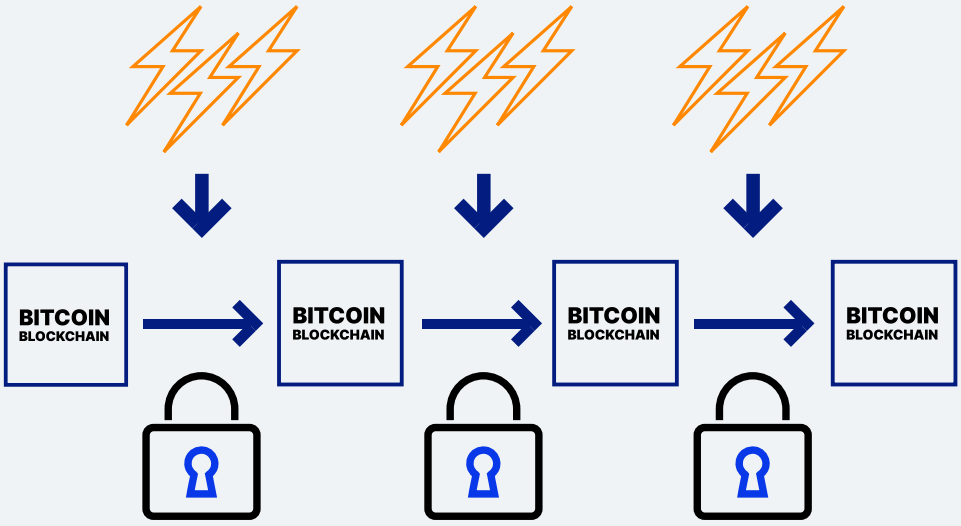
Bitcoin en Energie

Een van de eerste zorgen die vaak worden geuit over de ontwikkeling van Bitcoin is het energieverbruik van het Bitcoin-netwerk. Bitcoin mining verbruikt wereldwijd al een aanzienlijke hoeveelheid elektriciteit. En dit verbruik zal in de toekomst waarschijnlijk toenemen als meer mensen aan Bitcoin mining gaan doen.

Hoe minder energie in de vorm van rekenkracht wordt gebruikt om de Bitcoin blockchain te bouwen, des te makkelijker het is om deze later te veranderen.



Hoe meer energie in de vorm van rekenkracht wordt gebruikt om de Bitcoin blockchain te maken, des te moeilijker het is om hem later te veranderen.



Als we het hebben over Bitcoin en energie, is het belangrijk om te begrijpen dat de hoeveelheid energie die het Bitcoin-netwerk binnenstroomt cruciaal is voor de veiligheid van het netwerk. Hoe meer energie het netwerk binnenstroomt, hoe veiliger het is. Om de Bitcoin-blockchain aan te passen, moet namelijk dezelfde hoeveelheid rekenkracht – en dus energie – worden gebruikt als voor het maken van de blockchain. Maar met miljoenen computers wereldwijd die rekenkracht leveren aan het Bitcoin-netwerk, is het bijna onmogelijk voor een individu, organisatie of staat om ooit genoeg rekenkracht te verzamelen om zelfs de kleinste veranderingen in de blockchain aan te brengen. Daarom is rekenkracht en het daarmee samenhangende energieverbruik een belangrijk veiligheidskenmerk van het Bitcoin-netwerk.

Verder hebben Bitcoin-miningcomputers het voordeel dat ze zich overal ter wereld kunnen bevinden. Omdat miners zo goedkoop mogelijke elektriciteit nodig hebben om winstgevend te zijn, vestigen ze zich vaak op plaatsen waar veel overschotten, en dus goedkope energie, zijn. Op langere termijn zal dit waarschijnlijk zijn op plaatsen waar veel duurzame

energie is, omdat dit de goedkoopste elektriciteit oplevert.

Volgens de Bitcoin Mining Council gebruiken Bitcoin-miners momenteel ongeveer 56% hernieuwbare energie en de trend neemt toe. Veel Bitcoin-experts geloven dat Bitcoin mining in de toekomst tot 100% hernieuwbare energie zal gebruiken.

Tot dat het geval is, komt het energieverbruik van Bitcoin echter neer op de vraag of veilig en onvervalsbaar geld en waardeopslag deze energie-uitgaven waard zijn – of niet.

El Salvador - Bitcoin als de Nationale Munt

Een paar jaar geleden hielden visionairs het al voor mogelijk dat Bitcoin ooit als wettig betaalmiddel zou worden erkend door nationale staten. In de zomer van 2021 was het zover: El Salvador was het eerste land ter wereld dat Bitcoin invoerde als wettig betaalmiddel. In winkels, restaurants en bij allerlei dienstverleners kan niet alleen met Amerikaanse dollars worden betaald, maar ook met Bitcoin. Daartoe kregen de burgers een aangepaste Bitcoin-portemonnee, waarmee binnen enkele seconden en tegen minimale kosten kan worden betaald via het Lightning-netwerk.

Andere landen zoals Oekraïne, Brazilië en Panama bespreken momenteel soortgelijke wetsontwerpen. Als andere landen het voorbeeld van El Salvador zouden volgen, zou dit aan de ene kant de vraag naar Bitcoin verder doen toenemen en aan de andere kant de geloofwaardigheid van Bitcoin als ‚geld' versterken. De acceptatie van Bitcoin als wettig betaalmiddel in steeds meer landen betekent dus een beslissende fase in het wereldwijde adoptieproces van Bitcoin.

Wetten en voorschriften

Deze ontwikkelingen hebben ertoe geleid dat staten, centrale banken en bedrijven zich intensief met cryptogeld moeten bezighouden. Verschillende staten, waaronder Zwitserland, hebben regelgeving en richtlijnen uitgevaardigd over cryptogeld. Deze stap wordt door veel marktdeelnemers toegejuicht, omdat het juridische zekerheid schept voor zowel cryptoprojecten als de betrokken beleggers.

Ook in de VS, waar tot nu toe een laisser-faire (op zijn beloop laten) aanpak werd gehanteerd, ligt regelgeving in het verschiet. De exacte vorm die deze nieuwe reguleringswetten in de VS zullen aannemen, wordt nauwlettend gevolgd door de wereldwijde cryptogemeenschap, omdat ze een grote impact zullen hebben op de hele cryptosector.

Andere cryptovaluta

Bitcoin is lang niet het enige cryptogeld van dit moment. Er zijn nu meer dan 16.000 verschillende cryptovalu-

ta en activa. Deze munten en tokens hebben verschillende kenmerken en functionaliteiten en zijn niet allemaal ontworpen als ‚valuta' of geld. Sommige lijken meer op aandelen, in die zin dat hun waarde het succes van een cryptoproject weerspiegelt. Andere zijn vereist om gebruik te maken van een bepaalde dienst. En weer andere – zogenaamde meme tokens – zijn er vooral voor de grap.

Om verliezen te voorkomen, is het daarom raadzaam om de betreffende munt en het project erachter nader te bekijken voordat je een investering doet.

Central Bank Digital Currencies (CBDC)

Cryptocurrencies zijn in transitie van een ongereguleerde Wild-West fase naar een gereguleerde cryptofinanciële wereld. Deze ontwikkeling heeft centrale banken niet onberoerd gelaten, en er zijn ideeën geopperd dat centrale banken hun eigen cryptogeld zouden moeten uitgeven. Deze „Central Bank Digital Currencies," of CBDC's, zouden volgens voorstanders de stabiliteit van een staatsmunt combineren met de voordelen van een op blockchain gebaseerde munt. Kortom, ze zouden als het ware digitaal geld creëren.

Afhankelijk van het ontwerp kan een CBDC echter fundamenteel verschillende vormen aannemen. Diverse landen zijn proefprojecten gestart met verschillende soorten CBDC's, en in enkele landen zijn al CBDC's gelanceerd. Er wordt echter met spanning afgewacht of en in welke vorm economisch sterke valutagebieden zoals de VS, de EU of China hun CBDC's zullen lanceren.

Geldconcurrentie

Onze samenleving is de laatste decennia zo gewend geraakt aan staatsgeld dat andere soorten geld voor velen tot voor kort nauwelijks voorstelbaar waren. Maar nog niet zo lang geleden maakte het deel uit van het dagelijks leven dat er verschillende soorten geld naast elkaar circuleerden. Er waren bankbiljetten van verschillende banken, munten van verschillende metalen en andere geldsoorten die als betaalmiddel konden worden gebruikt.

Met Bitcoin zijn niet-staatsvaluta nu weer beschikbaar als alternatief voor staatsvaluta. Tot nu toe hebben de meeste regeringen Bitcoin getolereerd. Tot op zekere hoogte is dit wellicht te danken aan het gedecentraliseerde karakter ervan, waardoor Bitcoin moeilijk aan te vallen is. Voor burgers betekent dit dat een digitaal alternatief voor staatsgeld nu beschikbaar is naast goud en zilver. De effecten van deze extra monetaire concurrentie zullen in de toekomst interessant worden.

BITCOIN, WAT NU?

Als je jezelf nu afvraagt wat je met al deze informatie moet doen, zal ik een voorstel doen. Het betreden van de wereld van Bitcoin kost niets, noch tijd noch geld. Maar je leert een technologie kennen die op het punt staat onze wereld en de toekomst te veranderen.

Dus: Maak een account aan op een crypto-beurs of download een portemonnee op je smartphone en koop Bitcoin voor 50 euro. Of laat een collega wat Bitcoin naar je portemonnee sturen. Maar zorg dat je Bitcoin in ieder geval een keer in handen krijgt.

Want mocht Bitcoin doorbreken en net zo alomtegenwoordig worden als het internet, dan weet je er niet alleen theoretisch iets van, maar heb je Bitcoin ook zelf gebruikt. Soms maakt dat het verschil, want zo krijg je een kijk op en een gevoel voor de technologie, waardoor je een voorsprong hebt op een meerderheid van de mensen.

OVER DE AUTEUR

Daniel Jungen is een econoom en financieel journalist met expertise in crypto-activa. Daniel is medeoprichter van InsightDeFi, een onderzoeksbureau gespecialiseerd in alles wat met crypto te maken heeft. Samen met zijn partners bij InsightDeFi publiceren ze een tweewekelijkse nieuwsbrief (Duits) over Bitcoin, DeFi en Crypto.

RELAI

Opgericht in Zwitserland door Julian Liniger en Adem Bilican nadat ze worstelden met het vinden van een veilige, probleemloze ruimte voor het kopen van bitcoin, maakt Relai bitcoin sparen en beleggen toegankelijk voor iedereen. De bitcoin-only app is ontworpen om eenvoudig en intuïtief te zijn, waardoor iedereen in Europa binnen enkele minuten bitcoin kan kopen en verkopen, zonder dat registratie, verificatie of stortingen nodig zijn. Onafhankelijk geauditeerd, en met meer dan 35 miljoen CHF aan bitcoin geïnvesteerd via haar platform, geeft Relai consumenten de kans om nieuwe manieren van sparen en investeren te benutten.

Voor meer informatie ga je naar Relai.app.

Dank aan @StackSatsNu die dit e-book van het Engels naar het Nederlands vertaalde. Gebruik code STACKSATSNU voor het kopen van Bitcoin met Relai en je kosten worden met 0.5% verlaagd.