

Profielwerkstuk Informatica Bitcoins



Profielwerkstuk door S.

8082 woorden

22 maart 2015

★ 5,8

52 keer beoordeeld

Vak

Informatica

Wat zijn cryptocurrencies?

Cryptocurrency is een nieuwe gedecentraliseerde vorm van geld. Dit houdt in dat er geen persoon of organisatie is die de waarde van de 'coin' kan beïnvloeden. Het gebruikt cryptografie voor beveiliging en het voorkomen van 'Double Spending', het 2 keer uitgeven van dezelfde coin. In zijn simpelste vorm is het niet meer dan een digitale vorm van geld.

Echter is het, tegengesteld tot een FIAT valuta, inflatie-proof, niet wit te wassen, helemaal privé, zonder belasting, goed voor de zaken en niet te vergeten: de ervaring van het minen. [1]

FIAT valuta

Vroeger werd de waarde van geld bepaald door het aantal goud of zilver dat verwerkt was in het betaalmiddel. Je zou het je kunnen voorstellen als de waarde van het metaal in de euromunt. Dat was dan ook meteen de waarde van de munt.

Een FIAT valuta is eigenlijk een munt die geen intrinsieke waarde heeft, die gebruikt wordt als betaalmiddel. Dit betaalmiddel ontstond toen men erachter kwam dat de bedragen die werden betaald, niet langer te betalen waren als men bleef kijken naar de waarde van de metalen.

De letterlijke definities zijn:

- Een muntsoort die wordt herkend en geaccepteerd door een regering.
- Een munteenheid die kan variëren in waarde.
- Een munteenheid zonder intrinsieke waarde, die de eerste regel volgt.

[1]

Inflatie proof

Cryptocurrency zijn niet helemaal inflatieproof, de waarde wordt namelijk bepaald door vraag en aanbod. Zodra de vraag stijgt, stijgt de waarde. Zodra het aanbod stijgt, daalt de waarde, en andersom. Het werkt net als goud, de waarde wordt namelijk bepaald door de moeilijkheidsgraad van het verkrijgen van een 'coin'. De moeilijkheidsgraad van het verkrijgen van een 'coin' gaat omhoog zodra er meer 'coins' vrijkomen. Daarbij gaat ook het aantal 'coins' dat wordt vrijgegeven per gemiddeld block omlaag. Hierdoor blijven deze valuta redelijk stabiel.

Cryptocurrency hebben echter wel een 'dak', dit 'dak' zorgt ervoor dat er een maximum aantal 'coins' aanwezig kan zijn (21 miljoen Btc). Nadat dit bereikt is, kunnen er niet meer Bitcoins in circulatie voorkomen.

Veel critici vinden dat een valuta geen dak mag hebben, het zou er voor zorgen dat er een minimum waarde is die je moet spenderen. Echter gaan Bitcoins, tegenover reguliere valuta, door tot 8 decimalen. Hierdoor kun je zeer kleine getallen maken. Ze kunnen zelfs nog verder dan 8 decimalen, zou dat nodig blijken.

Inflatie is niet veel meer dan een stijging van prijzen over tijd. Dit heeft te maken met vraag en aanbod. Het aantal Bitcoins dat maximaal kan bestaan is 21 miljoen. De enige manier waarop Bitcoin kan dalen in waarde is wanneer de vraag naar Bitcoins zou verdwijnen. Het punt is, dat de waarde van Bitcoin niet beïnvloed kan worden door 1 persoon of regering, omdat er geen manier is om het aantal coins te vermeerderen nadat de 21 miljoen Bitcoin zijn bereikt.

Maar voor dit scenario hebben we 1 ding nodig, en dat is een hele wereld (of op zijn minst een groot gedeelte) die gebruik maakt van Bitcoin. Wanneer de vraag stagneert, blijft de waarde stabiel. [8]

Niet wit te wassen & 'Double Spending'

De enige manier om aan cryptocurrency te komen, is door het te kopen, of te minen. Je kunt dus ook geen Bitcoins genereren, zonder ze legitiem te minen. Zodra er Bitcoins vrijkomen, worden deze opgeslagen door het Bitcoin netwerk. Iedere coin heeft dus zijn eigen nummer. Bestaat het nummer al. Of staat deze al op iemands account. Of is het nummer gewoon niet geverifieerd. Dan heb je ook geen nieuwe coin. Hierdoor zijn ze niet wit te wassen.

Het 'double spending' probleem ligt iets dieper. In principe is alles dat digitaal is, te kopiëren en te plakken. Dit is ook het geval bij cryptocurrency. Hier hebben ze een oplossing voor gevonden.

Zodra iemand een transactie maakt, wordt er door een heleboel computers ten eerste gekeken naar de geschiedenis van deze persoon. Ten eerste hoeveel Bitcoins er ooit op zijn account zijn gezet.

Daarna wordt er gekeken naar hoeveel er is uitgegeven op dit account. En daarna naar of er inderdaad nog genoeg Bitcoins zijn om de transactie überhaupt te kunnen maken. Hierna wordt de transactie verwerkt. En dus Bitcoins toegevoegd op het account van de ontvanger. Wanneer de ontvanger dan een aankoop doet, begint het proces weer overnieuw.

Helemaal privé

Wanneer je een transactie verwerkt met een FIAT valuta, heb je eerst een aantal dingen nodig.

Als je geld wilt overmaken van een bankrekening naar de andere, dan moet je de naam van de andere persoon hebben, maar ook het rekeningnummer. Wanneer je iets overmaakt via Paypal heb je al een e-mail adres nodig. Dit hoeft ook niet iedereen te weten. Of als je iets met IDEal betaalt, of gebruik maakt van je pinpas. Krijgt de verkoper te zien wie en welk rekeningnummer iets gekocht heeft. Dat maakt veel mensen niet uit, maar er is enorm veel te doen met die informatie.

Om een voorbeeld te noemen. Een Amerikaanse supermarkt keten genaamd 'Target', wist al dat een meisje zwanger was voordat de vader van het meisje dit wist. Dit had te maken met een aantal aankopen dat dit meisje had gedaan. Door het aankooppatroon van het meisje te analyseren wist Target dus al voor de vader dat dit meisje zwanger was. [12]

Maar hetzelfde zie je terug wanneer je een aankoop doet bij www.bol.com. Wanneer ze op Bol.com zien dat jij veel aankopen binnen de categorie 'games' doet. Dan zullen ze jou reclame geven voor games gerelateerde onderwerpen.

Maar deze informatie word ondertussen ook doorverkocht aan banken, of andere bedrijven. Om dit te stoppen hebben de makers van Bitcoin een systeem bedacht waarin je het nummer van de ander zijn '*online portemonnee*' nodig hebt. Aangezien je geen informatie nodig hebt zoals namen, postcodes, bankrekeningen of e-mailadressen. Heb je meer privacy in tegenstelling tot reguliere betalingssystemen.

Zonder belasting & goed voor de zaken

Er kan geen belasting geïnd worden op een transacties die je maakt met Bitcoin. Deze kan er ook nooit komen, zelfs niet op het moment dat een regering Bitcoin accepteert als betaalmiddel. Dit komt omdat Bitcoin van een Peer-2-Peer systeem gebruikmaakt. Een systeem waarin een heleboel computers of servers een netwerk vormen, die de hele tijd informatie naar elkaar uploaden en downloaden.

Als een regering nu een belasting wilt invoeren op de Bitcoin, dan moeten ze dus alle computers binnen het netwerk aanpassen. Maar omdat Bitcoin een gedecentraliseerd netwerk is. Heeft dus niemand macht hierover.

Maar bovendien zorgt dit ervoor dat de Bitcoin goed is voor de zaken. Je betaling wordt verwerkt binnen 3 minuten, ook kan de koper niet terug zodra de betaling is gemaakt. Dit hoeft natuurlijk niet altijd goed te zijn. Maar er zijn tegenwoordig een heleboel systemen geplaatst waarop je bijvoorbeeld een koper kan 'raten', je geeft hem als het waren een cijfer. Hierdoor kan de gemeenschap zien of hij daadwerkelijk dingen verkoopt, of dat hij een neppert is. Hierdoor kun je dus snel en gemakkelijk betaling verwerken. Maar ook nog eens meer winst behalen.

Je kunt je natuurlijk afvragen of het wel goed is dat er geen belasting geïnd kan worden. Namelijk zorgt de belasting ervoor dat een samenleving in stand kan worden gehouden. Denk maar eens aan leraren, wegen, politie of de regering. En daarom is het ook een beetje een 'double edged sword', op het moment dat iedereen over zou gaan op Bitcoin, zouden de winkeliers hetzelfde kunnen blijven vragen voor hun producten. Alleen houden ze dan de 21% belasting.

Maar wat gebeurt er dan met de maatschappij. Er moeten namelijk een heleboel veranderingen komen als wij met Bitcoin willen gaan betalen.

De geschiedenis van Bitcoin

2008

In 2008 zat de wereld midden in een financiële crisis, er was een grote recessie. Mensen begonnen te twijfelen over valuta's van regeringen, over hun betrouwbaarheid en stabiliteit. De inflatie zorgde ervoor dat huishoudens het lastiger kregen. Allemaal door een factor die ze zelf niet in de hand hadden: de banken/regeringen. De mensen die leden onder deze inflatie en de mensen die het niet vonden kunnen dat de waarde van hun zwaarverdiende geld werd bepaald door een bank/regering waar ze zelf geen invloed op hadden wilden verandering. Je hoorde mensen klagen hoe het niet eerlijk was dat hun geld in waarde daalde terwijl ze er niks mee deden. Het was de perfecte situatie voor de opkomst van de Bitcoin!

Al vanaf het begin van het internet zijn er pogingen gedaan om een internetvaluta te creëren, maar ze konden allemaal geen oplossing vinden tegen het 'double spending' probleem. Dit probleem houdt in dat een "coin" gewoon een stukje data is, dat je het dan simpelweg kan kopiëren en er opnieuw mee kan gebruiken. [3] Hetzelfde idee als een briefje van €50 kopiëren in een printer en er dan mee betalen.

De makers van Bitcoin bedachten daarom een nieuw systeem: 'de block chain'. Bij deze techniek wordt elke Bitcointransactie gecheckt door een groot netwerk van computers verspreid over de hele wereld. Hierdoor kan er niet vals worden gespeeld binnen het systeem en kunnen mensen niet zomaar coins creëren, hierdoor werd de Bitcoin een eerlijkere valuta. [3]

In augustus 2008 werd Bitcoin.org opgericht. Dit is in feite de homepage van de Bitcoin. Het is het originele domein van de eerste Bitcoin-website. Het is bedoeld voor iedereen die met Bitcoins te maken heeft en er is veel informatie over Bitcoins te vinden. Bitcoin.org heeft geen officiële eigenaar. Maar de site wordt wel beheerd door een aantal communityleden en kern-ontwikkelaars van Bitcoin, ze hebben ook het domein van de site. De code van de website is 'opensource' (online beschikbaar) en gebruikers kunnen hem aanpassen als ze iets willen toevoegen of veranderen, en naar de ontwikkelaars sturen die de website er naar zullen veranderen als het hun bevalt, maar het kan ook dat dit idee wordt afgewezen door de beheerders van een site. [7]

In November 2008 werd er op het internet een artikel over Bitcoins gepubliceerd onder de naam van Satoshi Nakamoto. Het artikel heette: A Peer-to-Peer Electronic Cash System. Er stonden gedetailleerde instructies in over hoe Bitcoins werkten. In het artikel werd Bitcoin genoemd als "een systeem voor elektronische transacties zonder te moeten vertrouwen op vertrouwen". [3]

2009

In januari 2009 werd de eerste open-source Bitcoin-client geïntroduceerd en begonnen de uitgaven van de eerste Bitcoins, hiermee steeg de interesse in Bitcoins ineens enorm. Deze eerste Bitcoins werden gemined door Satoshi Nakamoto uit het zogenaamde 'Genesis Block', dit block had een beloning van 50 Bitcoins. De waarde van de eerste Bitcoins werd bepaald door mensen op Bitcoin forums. [3]

Lazslo Hanjecz, een programmeur uit Florida, maakte de eerste echte bestelling met Bitcoins, hij bestelde twee pizza's bij het pizzabedrijf Papa John's voor 10.000 Bitcoins (BTC). Deze transactie gebeurde wel indirect: Hanjecz stuurde de 10.000 BTC naar een vrijwilliger uit Engeland, die toen via creditcard de pizza's bestelde voor Hanjecz. [3] [4]

2010

Op 6 augustus 2010 werd er een groot zwak punt in Bitcoins ontdekt. De transacties werden niet goed gecontroleerd, voordat ze werden opgenomen in de 'block chain' of 'transactie log'. Hierdoor konden gebruikers de beveiliging omzeilen en zo een onbeperkt aantal Bitcoins genereren. Op 15 augustus werd de kwetsbaarheid misbruikt en werden er door twee Bitcoingebruikers 184 miljard Bitcoins gegenereerd in een transactie, deze Bitcoins werden toegestuurd aan twee adressen in het Bitcoinnetwerk.

Maar gelukkig werd deze bug binnen een paar uur ontdekt en gewist van de transactie log nadat de bug was verholpen.

Dit was een grote beveiligingsfout in de geschiedenis van de Bitcoin. [3] [4]

In november steeg de economische waarde van alle Bitcoins samen boven de 1 miljoen USD. [3]

2011

In februari 2011 kreeg 1 Bitcoin dezelfde waarde als 1 dollar. [4]

In juni begon Wikileaks Bitcoins te accepteren voor donaties. Wikileaks is gebaseerd op anonieme overdracht van informatie. De site is bedoeld zodat klokkenluiders van belangrijke overheidsinstellingen geheime informatie de wereld in kunnen brengen. Aangezien ze hier anonieme documenten lekken en misverstanden uit de wereld helpen is de anonimiteit van de klokkenluiders hier dus heel belangrijk.

Hierom passen Bitcoins ook goed bij Wikileaks, aangezien Bitcoins niet zijn te traceren blijft de identiteit van de ontvanger en verzender anoniem. [3] [9] [10]

Tevens werd er in juni een artikel uitgeven over Silk Road, dit was een website waarop mensen illegale goederen konden kopen. De site werkte via het principe van darknet. Een darknet is een directe privé verbinding tussen twee computers. Bij deze verbindingen worden de IP-adressen niet onthuld en blijft de identiteit van de gebruikers dus geheim. Hierdoor is er geen vrees voor een instantie die de gebruiker kan traceren. Silk Road accepteerde Bitcoins voor betalingen aangezien deze transacties ook anoniem zijn en om deze reden konden mensen 'veilig' illegale producten zoals drugs bestellen. [3] [14] [15]

Toen gebeurde er iets onverwachts dat niet goed uitwerkte voor de Bitcoin: de data van de gebruikers van Mt. Gox * was gelekt. Deze data bevatte de e-mailadressen, gebruikersnamen en wachtwoorden van zo'n 60.000 gebruikers. Sommige van deze gebruikers hadden hetzelfde wachtwoord en gebruikersnaam op MyBitcoin (een populaire online Bitcoin portemonnee). Van deze +- 600 gebruikers werden alle Bitcoins gestolen. Hierdoor daalde het vertrouwen in Bitcoins sterk en dus daalde de waarde met zo'n 50%. [3]

* Mt. Gox was een populaire online Bitcoin transactie 'bank' in Tokyo, gebruikers konden hier Bitcoins verkopen voor

ander geld en andersom. [13]

In 2011 ontstonden er ook twee andere cryptocurrency naast Bitcoin. Dit waren: Litecoin en Namecoin. Deze nieuwe soorten cryptocurrency waren gebaseerd op het idee en de code van Bitcoin maar hadden kleine aanpassingen (deze zullen verder worden beschreven in 'Hoe mine je Bitcoins?'). De bedoeling van de makers van deze coins was een cryptocurrency creëren die beter was als de 'oude' Bitcoin. Er zouden nog vele nieuwe cryptocurrency volgen, maar wel allemaal met dezelfde gedachtegang als waar het allemaal mee begon: Een gedecentraliseerde soort geld die erg flexibel en toepasbaar, waarbij het makkelijk is om wereldwijd betalingen te doen zonder veel vertraging. [17] [18]

2012

In oktober 2012 concludeerde de Europese bank dit over Bitcoins: "Virtual currencies could have a negative impact on the reputation of central banks if their use grows considerably. This risk should be considered when assessing the overall risk situation of central banks."

De Europese bank zag dus de dreiging van cryptocurrencies in. Want deze hebben geen banken nodig om te functioneren, bij het ruilen van cryptocurrencies gaat het namelijk direct van persoon naar persoon zonder de bank als tussenpersoon die weer weer winst uit kan halen.

In november was de eerste 'halveringsdag' van de Bitcoin. Eens in de vier jaar wordt de prijs die je krijgt van het minen van een block gehalveerd. Dit is om de waarde van Bitcoins te waarborgen, er komen namelijk steeds meer Bitcoins bij, en elke dag komen er meer miners en gaan we sneller door de blocks heen. Dus als je de toevoer ervan wat kleiner maakt blijft het aantal Bitcoins dat wordt gemined wordt per tijdseenheid toch redelijk constant. [3]

2013

De waarde van de Bitcoin steeg steeds verder, mede doordat steeds meer firma's Bitcoins begonnen te accepteren als betaalmiddel. Zo was er een taxifirma die Bitcoins accepteerde en ook konden er auto's en muziek albums van gekocht worden. De waarde van een Bitcoin werd hierdoor gelijk aan dat van 100 gram zilver. [3]

In oktober sloot de FBI Silk Road. Ook werd het eerste Bitcoin bankapparaat geopend in Vancouver, Canada, hiermee kon je Bitcoins verkopen voor cash en andersom. Het idee erachter was mede dat je nu makkelijk geld kon opnemen, ook als je in een ander land zit, zonder de overschrijvingskosten. [3]

De Bitcoin kwam boven de waarde van €1000. [3]

En in december 2013 besloot de bank van China dat het Bitcoin-transacties niet meer zou accepteren, toch stopte dit de Bitcoin handel in China niet. [3]

Samenvattend is er veel gebeurd met en rondom Bitcoin in de afgelopen 6 jaar. Het is van een concept tegen de toenmalige visie van geld in, naar een vrij wijd geaccepteerde valuta gegaan. [24] Het is een inspiratie geweest voor vele anderen cryptocurrency die waarschijnlijk nog een flinke verandering in de wereldeconomie gaan brengen. En misschien zelfs het hele economische systeem gaan veranderen. Zo zou over een paar decennia de functie van de bank zoals we die nu kennen volledig weg gevallen zijn en plaats hebben gemaakt voor cryptocurrency, die natuurlijk ook veel beter past in een technologisch tijdperk.

Een ding is in ieder geval zeker: we gaan nog veel van Bitcoin horen!

Hoe werkt Bitcoin?

Nu we de basisprincipes van Bitcoin uitgelegd hebben is het tijd om deze in een groter plaatje te brengen.

Hiervoor ga ik een voorbeeld gebruiken van Piet.

Piet wilt graag een laptop kopen, maar hij heeft besloten dat hij genoeg heeft van de euro, en graag met Bitcoins wilt betalen. Dus hij gaat naar een website, en besteld een nieuwe laptop. Op het moment dat hij heeft betaald, wordt zijn betaling in een block chain verwerkt. De informatie die wordt verwerkt is aardig wat.

1. Er wordt gekeken naar de eerdere transacties waar Piet aan mee gedaan heeft.
2. Daarna wordt er gekeken of na al deze transacties Piet nog genoeg Btc over heeft.
3. Als er genoeg over is worden de Bitcoins gestuurd naar een andere Bitcoin portemonnee.
4. De Bitcoins worden bij het voormalige aantal Bitcoins opgeteld bij de ontvanger.

Deze 4 stappen worden over een hele pool (een hele grote groep met miners) gedaan, dit houdt in dat er eigenlijk geen fouten worden gemaakt. Dit komt namelijk doordat de hashes worden vergeleken met elkaar. En op basis daarvan worden ze vergeleken, en dus de fouten eruit gehaald.

Maar deze transactie is slechts een klein onderdeel van het block, in dit block zitten namelijk nog duizenden andere transacties. Wanneer je nu naar bitcoins mined, ben je eigenlijk 2 dingen tegelijk aan het doen, je verwerkt al de transacties, maar je bent ook naar de code aan het zoeken om het block te openen. Voor elke code die jij met het netwerk deelt, krijg je meestal een heel klein bedrag terug, het gaat hier meestal om een X aantal nanobitcoin. Maar als jij de gelukkige bent die de juiste code weet te generen (hier heb je zelf geen invloed op). Dan krijg je 25 Bitcoins (op het moment), er wordt hier meestal wel iets van 1-5% aan belasting voor de pool vanaf gehouden, maar dan zijn ze evengoed nog steeds veel waard. Er is dus wel degelijk sprake van een soort belasting, Maar deze is er alleen bij het minen, dit vooral om de pool levende te houden. Deze belasting stopt dus ook wanneer het maximum aantal Bitcoins bereikt is.

Deze Bitcoins worden dan toegevoegd aan jouw portemonnee, en dus wordt ook deze transactie verwerkt in het volgende block. En zo blijft dit proces zich eigenlijk herhalen.

Hoe mine je Bitcoins?

Voordat je Bitcoins kunt gaan minen, moet je eerst een aantal dingen hebben gedaan.

Je moet namelijk:

1. Een apparaat hebben dat kan minen.
2. Een pool kiezen en hier een account op aanmaken
3. Een 'werker' creëren.
4. Het apparaat in werkende stellen/bouwen.
5. Het apparaat configureren.

Stap 1: Een apparaat kiezen dat kan minen

Een apparaat kiezen dat kan minen is niet gemakkelijk, eerst moet je namelijk iets weten van de verschillende soorten apparaten.

Je hebt in totaal 3 verschillende manieren om te minen.

- Met je CPU (Central processing unit), je processor.
- Met je GPU (Graphics processing unit), je video-kaart.
- Met een ASIC miner (application-specific integrated circuit). Dit zijn apparaten specifiek gemaakt voor bepaalde doeleinden.

Met je CPU minen

In het begin van Bitcoin kon je nog met je CPU minen. Nu gaat dat echter niet meer, de CPU bleek inefficiënt tegenover de GPU of ASICs. Hierdoor hebben ze de optie om met je CPU te minen uit de meeste programma's gehaald. Dit is dus ook niet meer mogelijk.

Met je GPU minen

Grafische kaarten bleken echter heel efficiënt te zijn voor het minen van Bitcoin, ze worden dan voor 99% belast en worden heel warm. Vaak worden er aparte PC's gebouwd voor het minen naar Bitcoin. Hier werden dan tot wel 6 GPU's in gezet. Dit is enorm duur tegenover het geld dat ze uiteindelijk opleveren. Maar het was wel de beste optie toen er nog geen ASIC miners waren. Tijdens het minen zal je GPU van slijtage en de hitte kapot gaan, en

waarschijnlijk heb je aan het eind van de levenstijd van de GPU het bedrag van de aankoop nog niet terugverdiend. Echter is het wel een oplossing voor mensen die hobbymatig willen minen.

De GPU's van het merk AMD zijn hier veel efficiënter in dan het rivaliserende merk NVIDIA. Dit heeft te maken met de architectuur van AMD kaarten, deze maken namelijk gebruik van meerdere kleinere processoren die simpelere processen uitvoert, al de processoren worden aan het werk gezet. Aangezien deze niet heel moeilijke taken krijgen is dit efficiënter dan de manier die NVIDIA heeft. Deze heeft namelijk een kleiner aantal SHADERS maar met hogere snelheden, voor games en het creëren van film is dit ideaal. Echter is het dat niet voor minen.

Maar hier is met de meest recente kaarten van NVIDIA verandering in gekomen. De nieuwste kaarten (GTX-9xx series) gebruiken namelijk maar 60-70% van de stroom die zij eerst gebruikten, waardoor deze kaarten weer rendabel zijn voor hobbyisten. [23]

Per model videokaart kun je van 500 Mh/s tot 2 Gh/s naar Bitcoin minen.

ASIC minen

Je kunt ook minen met apparaten die hier speciaal voor gemaakt zijn, deze heten ASIC (application-specific integrated circuit) miners. Deze zijn nog efficiënter dan GPU's, gaan langer mee wanneer ze goed gekoeld worden, maar nemen wel extra ruimte in beslag, waarnaast ook de ruimte zelf in temperatuur zal toenemen.

De ASIC miner is daarnaast ook moeilijker in te stellen. Je moet gebruik maken van voorkennis die je misschien nog niet hebt, natuurlijk kun je dit opzoeken op het internet. Maar het is een stuk gemakkelijker met de kennis.

ASIC miners zijn dus speciaal gebouwd voor het minen van Bitcoin, maar in relatie tot de prijs van een videokaarten zijn deze goedkoop voor de kracht die eruit komt. Waar je bij een videokaart dus van 500 Mhash/s tot 2Gh/s rangeren ze bij een ASIC miner van 2Gh/s tot 12 Th/s

Bij deze apparaten is het zo dat des te meer je erin investeert, des te meer winst je zal maken. Inhoudelijk betekent dat dat je met apparaten van 2Gh/s waarschijnlijk verlies zal maken, en met een apparaat van 12 Th/s je heel veel winst zal maken. Dit komt omdat de moeilijkheidsgraad van het minen hoog ligt. En je dus zoveel mogelijk shares wilt maken naar het netwerk toe. Des te sneller dat jij dat doet, des te meer geld je verdiend.

Dit klinkt natuurlijk alsof het niet eerlijk is, en dat is het ook niet. Vroeger waren de zwakkere apparaten nog rendabel. Dit komt omdat de difficulty toen nog niet zo hoog lag als dat hij nu is. De difficulty zorgt er namelijk voor dat de moeilijkheidsgraad van de hash hoger ligt. Dit zorgt er op zijn beurt dus weer voor dat de miner meer moeite

moet doen, met hetzelfde aantal stroom. Dus duurt het langer.

Het dus niet evenredig.

Maar het gaat hier ook over stroom gebruik. Waar een videokaart maar maximaal 220 watt gebruikt. Moet hier wel nog een pc omheen gebouwd worden, dit kan betekenen dat je met een erg kleine snelheid mined, terwijl je toch ook de andere componenten in een pc moet aansturen. Hierdoor zul je snel aan 500-700 watt zitten. Dit is natuurlijk een stuk minder efficiënt.

Bij een ASIC miner gaat alle energie naar het minen van Bitcoin en het koel houden van het systeem. Hierdoor is de efficiëntie hoger. Daartegenover staat wel dat de energie die je daadwerkelijk betaald een stuk hoger kan zijn dan die van een PC. Dit kan wel oplopen tot 6000 watt per uur. Dat is natuurlijk erg duur. Maar dit verdienen je dan ook gemakkelijk terug. [16]

Stap 2: Het kiezen van een pool en een account maken

Om zo effectief mogelijk Bitcoins te minen werk je meestal in groepen samen met andere miners. Als je namelijk alleen mined is de kans op het kraken van een block vrij klein, je hebt dan als het ware wel de volledige beloning aan Bitcoins die in het block zit maar de kansen zijn gewoon een stuk kleiner. Om deze reden hebben mensen 'pools' bedacht. Dit zijn servers waarop mensen samen door de rekencapaciteit van hun computers samen te voegen een block proberen op te lossen. Als zo'n block opgelost is wordt de beloning verdeeld onder de computers die hieraan gemined hebben. Ze worden verdeeld kijkende naar hoeveel een pc aan een block gerekend heeft.

Om dit principe beter te kunnen begrijpen kun je het vergelijken met een goudzoeker die zijn vrienden vraagt om samen goud te gaan zoeken. Die groep mensen is de pool. Ze graven een dag naar goud en aan het eind van de dag wordt het goud verdeeld. Iedere keer dat ze hun zeef door de grond halen en al de modder eruit schudden kun je vergelijken met een 'share'. Iemand die sneller werkt maakt dus meer shares per uur. De waarschijnlijkheid om een Bitcoin te vinden in een share is dus hetzelfde als de waarschijnlijkheid om een stuk goud te vinden in een zeef.

Je kunt kijken hoeveel shares je hebt gehad binnen de statistieken van de pool, als deze worden vrijgegeven tenminste. Meestal ziet dit er dan zo uit:

Maar deze kun je ook terugvinden in je miner. Deze komt echter niet overeen met die op de site gegeven is. Dit komt omdat het alleen het aantal shares zijn sinds je het programma hebt opgestart.

Bij het kiezen van een pool komen een aantal dingen aan de orde:

Hoe wordt je uitbetaald?

Er bestaan vele manieren die pools gebruiken om hun gebruikers uit te betalen. Er zijn een aantal manieren die vaak gebruikt worden, en een aantal die niet vaak gebruikt worden. De meest gebruikte manieren van gebruikers uitbetalen zijn: PPS, PPLNS, DGM, Prop, Score en ELIGIUS.

Om te beginnen, een share is een ongelooflijk groot getal of aantal letters. Dat wordt omgezet in een codering van letters, cijfers en speciale tekens. Deze zijn zo opgezet dat als je ook maar 1 ervan verandert. Je een totaal ander getal krijgt.

PPS (Pay Per Share): Deze manier van uitbetalen verdeelt de beloning van een opgelost block onder de miners kijkend naar hoeveel shares ze hebben gemaakt (hoeveel rekenkracht ze bij hebben gedragen aan het oplossen van het block). In deze soorten pools wordt voor elke share die je maakt een bedrag aan je gegeven. Als iemand dus een miner heeft met een rekenkracht van 20GH/s krijgt hij twintig keer zoveel uitbetaald in een uur als iemand met een miner met 1GH/s.

De waarde van 1 share is de beloning van een opgelost block (in BTC) * de waarschijnlijkheid dat je met een share een block oplost.

Het gevaarlijke hieraan is wel dat wanneer je constant langzame blocks tegenkomt, je als eigenaar van de pool failliet gaat doordat je balans waarvan de gebruikers hun Bitcoins afhaken leeg gaat. Om deze reden bestaan er tegenwoordig ook lang niet meer zoveel PPS pools als voorheen.

PPLNS (Pay Per Last N Shares):

DGM (Double Geometric Method): Deze methode beloont, net zoals PPS, de miners ook per hoeveel shares ze hebben gemaakt. Deze methode heeft alleen een slimme oplossing bedacht tegen de grote variatie van de minesnelheid: als een block gemiddeld gezien snel wordt opgelost, de eigenaar dit bedrag niet volledig uitbetaald aan de miners. Zodat wanneer het een keer lang duurt om een block op te lossen, hij die coins die hij nog achter de hand had van het snelle block kan gebruiken om aan de miners te verdelen.

Prop: Hierbij verdienen miners shares totdat er een block op is gelost, en dan worden ze pas uitbetaald. De beloning hier is de beloning van een opgelost block (in BTC)

Multipoolmining:

Dan bestaat er nog een totaal andere manier van minen: multipoolmining.

Het belangrijkste verschil met anderen manieren van minen is dat deze vorm niet op een cryptocurrency alleen gefixeerd is. De pool checkt constant welke cryptocurrency het meest profitabel is om te minen en daar switcht het naar over met behulp van een zogenaamde 'coin switcher'. En om ervoor te zorgen dat niet erg veel verschillende wallets hoeft aan te maken voor elke cryptocurrency worden de verkregen coins meestal direct geruild voor een cryptocurrency waarin de gehele pool in uitbetaald wordt.

Om dit principe duidelijk te krijgen kunnen we het beste even terug gaan naar het voorbeeld van de goudzoekers. Stel dat er zo weinig goud in de grond is dat het niet meer winstgevend is om er naar te gaan zoeken. Maar iets verderop zit wel nog redelijk wat zilver in de grond, dus is het winstgevender om daar naar te gaan zoeken. Nog iets verderop zit een hele hoop koper in de grond en het blijkt het meest profitabel om daar naar te gaan zoeken. Dus de goudzoekers worden tijdelijk koperzoekers.

Maar omdat ze het liefst toch goud willen hebben ruilen ze dit aan het eind van de dag weer om voor goud.

Wat er dan gebeurd met het koper en zilver? Deze worden opgeslagen in grote warenhuizen, en verkocht zodra ze meer waard zijn. En dus ook weer verkocht aan andere warenhuizen, die weer de gok nemen. Dat het ooit meer waard zal zijn.

Hoe vaak vinden zij een block?

Wanneer een pool vaker een block kraakt, dan is het vaak winstgevender om met deze pool mee te gaan minen. Hoe vaak een pool een block kraakt, hangt van verschillende dingen af. Onder andere het algoritme van de pool (De manier waarop deze geprogrammeerd is), de stabiliteit van de pool, hoeveel mensen/werkers er mee minen en natuurlijk hoeveel geluk deze pool heeft.

Bitcoin maakt over het algemeen gebruik van het HashCash algoritme

Maar deze informatie moet je als miner natuurlijk wel opzetten tegenover de hoeveelheid die je betaald krijgt, zelfs als je geen Bitcoins vind. Wanneer jij in een succesvolle pool mined, maar vervolgens nauwelijks inkomsten genereert. Dan kun je zelf de afweging maken tegenover een pool die niet zo succesvol is, maar wel veel inkomsten genereert.

Je kunt het beste dus beginnen door een maandje in elke pool te minen. Natuurlijk heeft niemand zoveel tijd in handen, maar een weekje per pool is goed genoeg. Hierna kun je deze vergelijken met elkaar en beslissen welke pool voor jou het beste is.

Er zullen bijvoorbeeld pools zijn waarbij de minimale waarde die je verdiend redelijk laag is, maar dat er af en toe een gigantische uitschieter tussen zit. Of je gaat voor een pool die altijd redelijk goed verdiend, maar minder uitschieters

heeft. Het is maar net wat je zelf wilt.

Geven zij statistieken?

Er zijn verschillende pools, maar niet elke pool heeft dezelfde structuur. De ene geeft namelijk wel statistieken, en de ander niet. Je kan je natuurlijk afvragen hoe belangrijk statistieken voor jou zijn. maar deze geven wel behoorlijk wat inzicht in wat jij maandelijks mined of verdient. Met deze info kun je natuurlijk je miner verbeteren. Of je setup verbeteren. Verschillende maatregelen nemen als je erachter komt dat je niets hebt verdient. Of besluiten dat het minen het toch niet waard is.

Statistieken zijn er dus voor jou om te kijken hoe de tussenstand is.

Er zijn letterlijk duizenden pools. De grote pools, zoals Discuss Fish, Ghash.io, BTCguild en Slush's pool. Geven allemaal statistieken. Maar dit zijn slechts enkele voorbeelden.

Statistieken kunnen er bijvoorbeeld zo uitzien:

Hoe stabiel is de pool?

Wanneer je gaat minen naar bitcoins wil je er wel van uit kunnen gaan dat je kan blijven minen, en dus niet dat je miner nog aanstaat en opeens stopt met minen. Om dit tegen te gaan kan je 2 dingen doen. Je kan een stabiele pool kiezen, of van een pool switcher gebruikt maken.

Een pool switcher is een programma dat automatisch van pool verandert zodra de eerste pool niet meer winstgevend genoeg is, of zelfs inactief word. Dit zorgt ervoor dat je mining operatie altijd 'up and running' blijft. En dus zal je winst gemaximaliseerd worden.

Je moet er dus voor zorgen dat je altijd door kan blijven gaan met minen.

Kan je ook merged minen?

Merged Mining houdt in dat je met 2 miners naar dezelfde hash werkt. Hierbij verzeker je je hash als het waren. Je word er ook extra voor uitbetaald, aangezien je de kans op frauderen verkleint binnen een transactie in een block.

Dit is voor velen een belangrijke feature.

Stap 3: Een 'werker' creëren

Een 'werker' is de naam van jouw miner, deze werker is eigenlijk niets behalve de verbinding tussen de pool en jouw miner.

Hij zorgt ervoor dat jouw miner alle pakketjes krijgt waar hij daarna mee kan rekenen, en dat je al jouw hashes worden doorgegeven aan de pool.

Om een werker te creëren moet je naar de website gaan van je pool. Helaas verschilt deze per pool.

In je startup file van je miner wil je je naam van je werker en je wachtwoord van je werker zetten. Je start straks je miner met deze startup file.

Na '-o' komt de link naar je pool te staan, achter '-u' zet je dan je werker inlognaam, (Deze zal op de website van je pool ook beschreven staan) naast '-p' staat dan tenslotte het wachtwoord van de werker. Soms is het wachtwoord echter niet nodig, ook dit staat weer op de website van jouw pool.

Stap 4: Het apparaat in werkende stellen/bouwen

Als je mined op je pc, dan is het eigenlijk heel gemakkelijk. Je download je miner (BFGminer of CudaMiner) En maakt dan een startup file aan.

die startup file gaat er ongeveer zo uitzien:

Daarna sla je deze op als een .bat bestand

Deze kun je daarna uitvoeren, daarna werkt je miner.

Het kan zijn dat je handmatig apparaten moet toevoegen.

Dit kun je doen door eerst op je toetsenbord op M+ te drukken, en dan auto te typen. Daarna druk je weer op enter. Als je allesgoed hebt gedaan, begint hij vanzelf met minen.

Je kunt met deze programma's trouwens ook USB-ASIC miners gebruiken.

Dit gaat echter wel anders als je met een ASIC-Miner gaat minen. Dit verschilt namelijk per apparaat en dus moet je vooral in de handleiding kijken over hoe je deze moet bouwen. Het zou eigenlijk geen problemen mogen opleveren, aangezien alles eigenlijk al klaar is, misschien dat er een paar schroefjes in moeten, maar dat is het dan ook.

Vergeet vooral niet dat het apparaat voldoende koele lucht nodig heeft, een extra ventilator inbouwen is dus geen slecht idee, deze helpt met de aanvoer van koele lucht. Deze zijn ook belangrijk bij USB miners.

Stap 5: Het apparaat configureren

Als je een ASIC-miner bezit zul je deze moeten configureren, dit zal je hoogstwaarschijnlijk doen door in te loggen op zijn ip adres, deze kun je invoeren in je browser, om daarna naar de settings te gaan. Hier zul je de gegevens van je werker & pool in kunnen voeren.

Je wachtwoord, inlognaam en de link naar de pool.

Je moet daarna je miner opnieuw opstarten, en dan zou hij moeten gaan minen.

Hoe ruil je Bitcoins?

Er zijn meerdere manieren om Bitcoins te ruilen.

Van persoon naar persoon

Er zijn een aantal sites waarop je dit kunt doen. Zo heb je onder andere: Coinbase en LocalBitcoins in de VS, en

BitBargain en Bittylicious in Engeland. Hierop Bitcoins naar geld omzetten werkt als volgt: Eerst maak je een account aan en identificeer je jezelf via je persoonsgegevens. Dit is van belang omdat het als het ware een bank is. Dan geef je op de site aan dat je een bepaald aantal Bitcoins wilt verkopen. Een koper kan hier op reageren en dan kunnen de Bitcoins via de site geruild worden.

Dit gaat natuurlijk wel ten koste van je anonimiteit. Maar hier kies je zelf voor. Op zichzelf zijn Bitcoin transacties altijd anoniem. Maar hier moet je zelf voor beslissen. Het heeft dan wel als voordeel dat de koper zich veiliger voelt. Aangezien ze niet met een username praten maar met een echte naam. Dit geeft een gevoel van vertrouwen. Maar hiervoor heb je dus wel anonimiteit op.

Via een online markt

Hierbij maak je ook weer een account aan op een speciale site. Je kunt dan je Bitcoins op je account zetten. Je maakt een bod van hoeveel Bitcoins (of andere cryptocurrency) je wilt verkopen en voor hoeveel geld. Als iemand akkoord gaat met dat bod wordt het geld van de andere op jou account gezet.

Je moet daarna het geld van je account verplaatsen naar je rekening op je bank.

Peer-to-peer ruilmarkten

Dit zijn sites zoals Purse.io. Op dit soort sites zijn er twee groepen mensen: er zijn mensen die iets willen kopen op een site die geen Bitcoins accepteert (bijvoorbeeld Amazon.com), en een groep mensen die graag Bitcoins wilt kopen voor geld (meestal via een creditcard).

Stel dat Piet Bitcoins wil verkopen, dan zet hij een product dat hij graag wil bestellen op de site. Bob, die Bitcoins wilt kopen kan dat reageren op deze aankoop voor Piet. Ze maken dan een deal via de site: Bob bestelt met zijn creditcard het product voor Piet en laat het bij Piet bezorgen. Als het product is aangekomen laat Piet dit aan de site weten en wordt het bedrag dat de bestelling koste in euro's naar Bitcoins omgezet, en overgemaakt naar Bob's account.

Hier zit meestal ook een kleine rente voor de site bij in begrepen.

Dit is een redelijk snelle manier om via je creditcard Bitcoins te verkrijgen.

Een manier om Bitcoins om te ruilen naar ander geld is voor de speciale banken gefixeerd op cryptocurrency. [22]

Wederom heb je hiervoor een stukje belastingloze transactie op. Maar hier ga je zelf mee akkoord. Denk eraan dat Bitcoin transacties altijd kosteloos zijn. Maar dit is meer een vergunning zodat jij aan de markt mag deelnemen.

Onze Bitcoinminer

Wij hebben ook een eigen bitcoinminer gebouwd om te ervaren hoe het minen precies werkt, wat je ervoor moet doen, welke onderdelen je moet hebben en natuurlijk of het winstgevend is.

Het leek ons een goed idee om van een Raspberry Pi (een minicomputer) onze miner te maken. Alle benodigde onderdelen waren:

Raspberry Pi MiniComputer (met het groene printplaatje op de foto's)

Dit is de computer nodig voor het minen.

Adafruit 16x2 LCD

Op deze display kan je nuttige informatie laten verschijnen, bijvoorbeeld hoeveel hashes je mined of andere zaken.

Adafruit LCD plate

Dit is het plaatje waar de display op vast gemaakt moet worden.

2 USB Bitcoin Miners

Deze miners worden aangesloten op een USB poort en vergroten de rekenkracht van het minen.

Usb Hub

Deze heb is nodig om beiden USB miners aan te sluiten.

Onze resultaten

Aangezien we de USB miners niet ontvangen hebben, zijn we gaan minen met de grafische kaart van Loek's computer.

Dit zijn de specs van de computer

- I5-4670K 4.5 GHz
- 2 x Nvidia gtx 770 sli mode
- 8 gb ram
- 120 Gb ssd
- 1 TB hdd

Dit is dus een enorm snelle computer, maar ondanks dat feit hebben we in 5 uur tijd maar een heel klein aantal Bitcoins kunnen minen.

Dit stond na het minen op ons bankaccount, 0.00000162 Bitcoins, nog geen cent omgerekend naar euro's.

Is er winst te behalen?

Om deze vraag in het kort te beantwoorden; ja! Maar er komt wel een heleboel bij kijken.

Ten eerste is het niet meer rendabel om met je pc of een ander zwak apparaat te minen. Dit heeft 1 hele simpele reden. Je pc is niet snel of sterk genoeg om de handelingen uit te voeren die vereist zijn voor het snel en goed minen van bitcoins of andere cryptocurrency. Daarnaast kost de stroom om je pc of apparaat operationeel te houden meer geld dan dat je zult verdienen. Oftewel je verliest zelfs geld op deze manier.

een voorbeeld hiervan is onze bitcoin miner. met een simpele rekensom kwamen wij erachter hoeveel verlies we draaiden. $(\text{Wattage} \times \text{Hours Used Per Day}) \div 1000 = \text{Daily Kilowatt-hour (kWh)}$

$$24 \times 16 / 1000 = 0.384 \text{ KW/Day}$$

$$0.384 \times 30 = 11.52 \text{ KW/Month}$$

$$11.52 \times 0.23 = \text{€ } 2.64 \text{ per maand}$$

Daartegenover verdienen we natuurlijk ook een klein bedrag.

Dit ligt echter iets ingewikkelder. De waarde van Bitcoin is net zoals een wisselkoers, hij kan dus op elk moment stijgen, maar ook dalen.

wij minen met ongeveer 4 Giga Hashes/s (4 miljoen hashes per seconde).

Dit houdt in dat wij ongeveer 5 cent verdienen per dag.

30 dagen in een maand dus $30 \times 5 = 150$ wij verdienen dus €1,50 per maand. Min de stroomkosten: $2.64 - 1.50 = 1.14$

We hebben per maand dus ongeveer 1.14 euro verlies.

Maar niet getreurd, We kunnen ook winst maken met het minen van Bitcoins. Helaas is dit een geval van, des te meer je investeert, des te meer je verdient. Je kunt bijvoorbeeld een miner kopen van 600,- euro, en nog steeds verlies draaien.

Het is zelfs bijna zo dat de apparaten van 2000 euro nauwelijks meer winst maken voor Bitcoins.

Maar hier hebben ze iets op verzonnen. Je kunt nu bijvoorbeeld minen naar een andere coin, bijvoorbeeld litecoin. En deze daarna ruilen voor bitcoin. Dit is dan weer wel rendabel. Dit komt omdat de moeilijkheidsgraad van deze litecoins momenteel nog zo laag ligt, dat ze gemakkelijk en snel te minen zijn. En dus kun je met een goede installatie veel van deze coins vergaren. Wanneer je deze daarna ruilt voor bitcoins, maak je wel weer een percentage winst. Het gaat dus zoveel sneller dat het rendabel word.

Maar je kunt natuurlijk ook een gigantisch bedrag investeren in miners. (Alles boven 10.000 euro). Deze hebben heel erg veel stroom nodig. Maar ze zijn erg snel met maar liefst 12 Th/s. Met deze verdien je dan zo'n 6000 euro extra op

jaarbasis.

Helaas is de prijs om te beginnen en daartegenover de winst die je maakt dus niet linear. Dit komt eigenlijk door een aantal dingen.

- De miner is al ouder en eigenlijk niet meer voldoende.
- De moeilijkheidsgraad gaat omhoog, en de miner is niet meer snel genoeg.
- Maar ook 'vraag & aanbod' speelt een rol, niet alleen in de waarde van Bitcoins, maar ook in het investeerbedrag van de miner.

Al met al is het dus riskant om te minen naar Bitcoin, het kan dus ook goed zijn dat je het ene moment, heel veel winst maakt, en het andere eigenlijk helemaal niets.

Wat zijn de voordelen en nadelen van Bitcoin?

Voordelen

- Gedecentraliseerd

Bitcoins zijn volledig gedecentraliseerd, er is namelijk niemand die de macht heeft over Bitcoins. Er is niemand die zelf of met een aantal mensen iets kan veranderen in Bitcoins. Mocht er iets willen veranderen dan moet dit bij elke gebruiker van Bitcoins gebeuren en dit maakt het praktisch onmogelijk.

- Snel

Wanneer je normaal een overschrijving wilt doen vanuit jou bankaccount naar een ander, of zelfs naar het buitenland, kan dit vaak een paar dagen duren. Zeker als je wilt dat dit in het weekend gebeurt. Een overschrijving vanuit jou Bitcoin wallet naar een andere wallet duurt daarentegen maar een paar minuten.

- Veilig

Aangezien Bitcoins gebruik maken van het blockchain principe is het vrijwel onmogelijk om iets te veranderen aan bitcointransacties. Het minen en overmaken is een stabiele handeling.

- Bevordert internationale handel

Omdat het zo snel is, is het natuurlijk erg voordelig in de handel. Tevens heb je met FIAT valuta's allerlei heffingen die je erbij krijgt, hierdoor betaal je uiteindelijk meer als dat iets kost. Dit probleem heb je met Bitcoins niet.

- Nauwelijks commissies

Over FIAT valuta's betaal je BTW aan de regering, maar aangezien je bij Bitcoins geweent BTW kan innen blijven die 21% gewoon voor jezelf. Er worden wel een klein aantal procenten van overschrijvingen of andere handelingen afgehouden, zoals ook de commissie die betaald dient te worden bij sommige mining pools. Maar dit is allemaal nog altijd een stuk lager als de BTW.

Nadelen

- Gebaseerd op vertrouwen

In feite is elke valuta gebaseerd op vertrouwen. Als bijvoorbeeld niemand de euro meer zou gebruiken zou deze ook geen waarde meer hebben. Maar euro's worden erg veel gebruikt door een groot deel van de bevolking, zonder deze kun je in Europa vrij weinig. Bitcoins zijn daarentegen tegenwoordig nog veel instabieler, zo was te zien dat toen wanneer er een fout in de blockchain ontdekt werd, de waarde van de Bitcoin ineens enorm daalde. Je kunt geen maatschappij draaiende houden op een valuta die zo onvoorspelbaar en instabiel is.

- Heeft de status van een ruilwaar

Bitcoins worden door de staat niet geaccepteerd als regulier geld zoals de euro. Het heeft daarentegen de status van een ruilwaar, hetzelfde als goud. Zolang Bitcoins niet volledig worden ondersteund door de staat is het natuurlijk minder stabiel en heeft het andere nadelen.

- Bij scams geen geld terug

Zo krijg je bij scams geen geld terug omdat Bitcoins als ruilwaar worden gezien. Mocht er dus iets gebeuren zoals een hack waarbij je al je Bitcoins verliest. Krijg je deze niet terug.

- Nog moeilijk om te beginnen

Er staat hier een hele hoop informatie over Bitcoins en andere cryptocurrencies, maar toch hebben we nog lang niet alles kunnen bespreken. Het is nu eenmaal een ingewikkeld onderwerp en lang niet iedereen zal het begrijpen. Ook voor ons was het lastig om erachter te komen hoe alles werkte. Bitcoins moeten dus een normaler fenomeen worden waar iedereen alles over weet.

- Er gaat geen belasting naar de staat

Het klinkt natuurlijk wel leuk dat je geen belasting meer hoeft te betalen met Bitcoins. Maar als een deel van de mensen switcht naar Bitcoins, heeft de overheid dus ook minder inkomsten. Wat weer leidt tot minder geld voor infrastructuur, gezondheidszorg, veiligheid en nog veel meer dingen. Dit is natuurlijk erg nadelig voor ons allemaal.

- Vereist nieuwe maatschappij

Om deze reden is als er wordt gewisseld naar cryptocurrencies, er een heel nieuwe soort maatschappij moet komen. Eentje die misschien meer gericht is op eigen initiatief in plaats van de overkoepelende macht van een overheid.

Conclusie

Bitcoins zijn een geweldige currency waar enorm veel nieuwe ontwikkelingen mee kunnen worden gecreëerd. Omdat de transacties zo makkelijk, snel en veilig zijn bevordert het tevens de internationale handel. Niemand weet wat je koopt en je behoudt je anonimiteit bij elke transactie.

Er wordt minder geld van je weggesluisd omdat je geen belasting hoeft te betalen. Maar dit is ook meteen een van de grootste problemen van Bitcoins. De overheid wilt de Bitcoin niet als echt geld accepteren, mede omdat zeer geen belasting van innen. Daarom worden ze nog steeds gezien als een ruilwaar wat het vertrouwen en de stabiliteit van Bitcoins niet echt verbeterd.

Maar er zijn momenteel nog teveel problemen die voorkomen bij Bitcoins of cryptocurrencies. Het instapniveau is nog te hoog. Het is nog te moeilijk voor de gemiddelde mens. Zoals je ziet is er nog ongelooflijk veel research nodig om hier ook maar een globale 'understanding' van te krijgen. Omdat het zo ingewikkeld is is het voor mensen ook moeilijk om er genoeg vertrouwen in te hebben.

Daarbij is het zo dat Bitcoin nog niet in onze cultuur zit verwerkt. Dit maakt de te maken stap nog groter. Van kleins af aan wordt ons al geleerd hoe we met Euro's om moeten gaan. Dit zou een totale andere omgeving zijn.

Al met al komen wij dus tot de conclusie dat Bitcoin nog geen goede oplossing zou zijn voor de huidige economie. Dit komt dus mede door de hoge drempel, maar ook is het zo dat deze coin internationale handel gaat bevorderen. En dus zullen we moeten leren omgaan met culturen uit andere landen.

Wij denken persoonlijk dat de infrastructuur van Bitcoin nog moet veranderen. Alles gebeurt op het moment nog online, dit houdt dus ook in dat je altijd online moet zijn als je wilt betalen met Bitcoins. Natuurlijk is dit voor lang niet iedereen het geval.

Al met al komen wij dus tot de conclusie dat Bitcoin voor de nabije toekomst niet de oplossing is.

Of dit gaat veranderen voor de verre toekomst is nog maar de vraag.

Bronnen

	URL	Titel	Geraadpleegd op
[1]	http://www.techopedia.com/definition/27531/cryptocurrency	What is Cryptocurrency?	23-09-2014
[2]	http://nl.wikipedia.org/wiki/Cryptografie	Cryptografie	23-09-2014
[3]	http://www.tech365.nl/de-complete-geschiedenis-van-van-Bitcoin-infographic/	De complete geschiedenis van Bitcoin [Infographic]	23-09-2014
[4]	http://en.wikipedia.org/wiki/History_of_Bitcoin	History of Bitcoin	23-09-2014
[5]	http://balhiser.com/2011/07/Bitcoin-the-inflation-proof-e-currency-of-the-future-or-not/	Bitcoin: The Inflation-proof E-Currency of the Future, or Not	26-09-2014
[6]	https://Bitcoin.org/en/faq#what-determines-Bitcoins-price	What determines Bitcoin's price?	26-09-2014
[7]	https://Bitcoin.org/nl/	Bitcoin - opensource-2P2-geld	4-11-2014
[8]	https://en.Bitcoin.it/wiki/Myths#Bitcoin_can.27t_work_because_there_is_no_way_to_control_inflation	Myths - Bitcoin	5-11-2014
[9]	http://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/	WikiLeaks Asks For Anonymous Bitcoin Donations	5-11-2014
[10]	http://nl.wikipedia.org/wiki/WikiLeaks	Wikileaks	5-11-2014
[11]	http://en.wikipedia.org/wiki/Fiat_money#Money_creation_and_regulation	FIAT currency	6-11-2014
[12]	http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/	Forbes, target anecdote	6-11-2014
[13]	https://en.Bitcoin.it/wiki/Mt._Gox	Mt. Gox	19-11-2014
[14]	http://en.wikipedia.org/wiki/Darknet_%28file_sharing%29	Darknet (file sharing)	19-11-2014
[15]	http://en.wikipedia.org/wiki/Silk_Road_%28marketplace%29	Silk Road (marketplace)	19-11-2014
[16]	https://en.Bitcoin.it/wiki/Mining#Hardware	Mininghardware info	20-11-2014
[17]	http://en.wikipedia.org/wiki/Litecoin	Litecoin	20-11-2014
[18]	http://en.wikipedia.org/wiki/Namecoin	Namecoin	20-11-2014
[19]	https://en.Bitcoin.it/wiki/Comparison_of_mining_pools	Comparison of mining pools	28-11-2014
[20]	https://en.bitcoin.it/wiki/Pooled_mining	Pooled Mining	29-12-2014
[21]	http://en.wikipedia.org/wiki/Mining_pool	Mining Pools	29-12-2014
[22]	http://www.coindesk.com/information/sell-bitcoin/	How to sell Bitcoins	6-1-2015
[23]	https://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU#Why_are_AMD_GPUs_faster_than_Nvidia_GPUs.3F	Verklaring AMD>Nvidia voor minen	2-2-2015
[24]	http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html	Who Accepts Bitcoins As Payment?	2-2-2015