BITCOIN, een introductie

Bitcoin is virtueel contant (cash) geld, dat enkel in digitale vorm bestaat op het internet. Bitcoin wordt niet uitgegeven door een land of bank, iedereen met een pc, laptop of smartphone kan meedoen. Bitcoin bestaat sinds 3 januari 2009 en maakt sindsdien een stormachtige ontwikkeling door.

Bitcoin is de naam voor zowel het technisch protocol, de wijze waarop in Bitcoin financiele transacties worden uitgevoerd als de naam voor de betaal-eenheid, afgekort btc.

Bitcoin is zowel revolutionair als geniaal. **Geniaal** omdat in een relatief klein software programma de functies van (a) internet geld-transacties (zoals credit card betalingen), (b) beveiliging van opslag en transacties en (c) de uitgifte van nieuwe Bitcoin 'munten' worden verzorgd. En dit op geheel nieuwe wijze, zonder controlerende instanties.

Bitcoin is **revolutionair** omdat voor het eerst in de moderne tijd geld door alle mensen op de wereld op een veilige manier gebruikt en beheerd kan worden zonder noodzakelijke bemoeienis van overheid of andere instantie. En Bitcoin is zo opgezet dat er op den duur geen inflatie kán plaatsvinden: het aantal Bitcoin is namelijk gemaximeerd.

"Wrijvingsloze" transacties - Gebruikers van Bitcoin software kunnen naar elkaar Bitcoin overmaken tegen zeer lage kosten. Transacties duren meestal maar enkele seconden, de verwerking gaat dag en nacht, 7 dagen per week door.

Bitcoin functioneert verbluffend goed als **internet-geld**. Tienduizenden webshops accepteren bitcoin als betaling voor hun artikelen. Ook PersianShoes.com, een schoenen-webshop uit Iran. Bitcoin transacties zijn **definitief**. Bank- en creditcard transacties zijn terug te draaien (te 'storneren'). Dat is prettig voor de consument bij een online aankoop waarbij de webshop een waardeloos product levert. Voor de internet winkelier zijn deze storneringen zeer onwelkom, vooral omdat er ook misbruik van wordt gemaakt. Bitcoin maakt het de **webshop** houders mogelijk voor kleine of niet te retourneren aankopen enkel Bitcoin te accepteren. Daarnaast bespaart de webwinkelier zich de 3%-7% creditcard kosten (vooral in de vele landen waarin iDeal achtige betalingssystemen niet beschikbaar zijn).

Zonder grenzen – Nooit was het zo makkelijk en goedkoop om in enkele minuten op een zaterdag direct 1.000 euro aan btc naar een nicht in Nieuw Zeeland over te maken.

Of er nu ter waarde van een halve euro of een half miljoen euro bitcoins worden overgemaakt, de overmakings-kosten zijn in de orde van enkele eurocenten. Voor inwoners van Europa, die met het SEPA/IBAN bancair systeem tegen lage kosten geld kunnen overmaken is dit wellicht niet zo bijzonder, maar buiten Europa kosten basis interbancaire overmakingen al gauw 25 tot 40 euro. Indiase IT-ers werkzaam in het Westen kunnen met bitcoin geld naar de familie overbrengen tegen zeer lage kosten.

Winkels – In Delft en Amsterdam kan je al je koffie of biertje afrekenen met Bitcoin. Dit gaat via je Smartphone. In Berlijn is er een hele 'Bitcoin wijk' van cafe's en winkels waar je met bitcoin kan betalen. Wereldwijd zijn er tien duizenden internet shops en winkels en horecagelegenheden die btc accepteren.

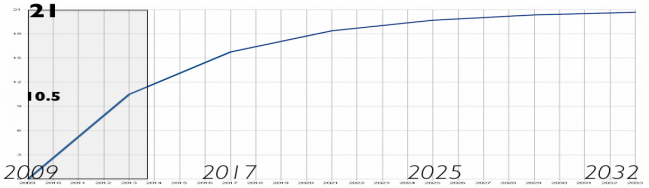
De waarde/koers van Bitcoin

Bitcoin heeft als elke valuta ook een Euro-koers. Eind oktober 2013 was de koers ongeveer 140 euro per bitcoin.

De eerste aankoop van een fysiek product met Bitcoin was een pizza die verkocht werd voor 10.000 bitcoins, in mei 2010. Tegen de huidige koers een miljoen euro! Ruwweg is de bitcoin elk jaar 10x in (euro)waarde gestegen. Of en hoe lang dit doorgaat kan niemand zeggen, maar als Bitcoin een blijvende rol gaat spelen, zal de koers vermoedelijk nog wel enkele keren met een factor 10 toenemen.

"Mining" (delven) – Het beschermen van het Bitcoin systeem tegen valsemunterij en het controleren van de transacties op misbruik (valsemunterij) gebeurt in feite door het oplossen van wiskundige puzzels. Hiervoor worden computers met veel rekenkracht (zgn ASIC's) ingezet. Bij het oplossen van de puzzels worden automatisch nieuwe Bitcoins gegenereerd, die toebedeeld worden aan de eigenaren van deze zware computers, als beloning voor de controle-werkzaamheden. Dit proces wordt 'mining' genoemd, genoemde operators de 'miners'.

De uitgave van bitcoins was halverwege gevorderd in november 2012, toen de teller op 10.5 milj stond. In 2028 zal de teller op 20 milj staan en pas in 2140 wordt de laatste, de 21 miljoenste, bitcoin gedolven. Uitgifte volgens onderstaande afbouwende curve, momenteel 25btc per 10 minuten.



Bijna al het moderne geld is onderhevig aan inflatie. Bitcoin is (uiteindelijk) **deflatoir** in die zin dat de hoeveelheid uiteindelijk beperkt is tot 21 milj en de creatie van nieuwe coins volgens een vast, afnemend tempo gebeurt. Het lijkt daardoor behalve een goed (internet) betaalmiddel ook een goede Store Of Value voor (een deel van) het spaargeld. Bitcoin wordt vanwege deze eigenschappen wel "digitaal goud" genoemd.

Iedereen kan meedoen door gratis software te downloaden en op de eigen pc of smartphone te installeren. Vervolgens Bitcoin bij een handelshuis of exchange kopen (zie 'Bronnen') of, nog mooier, diensten of producten aanbieden tegen Bitcoin.

Bijzondere Eigenschappen

Decentraal – Er is nergens op aarde 'de centrale bitcoin server' te vinden, want die bestaat niet. Elke Bitcoin gebruiker die bitcoin software op haar computer geïnstalleerd heeft, is onderdeel van het netwerk. (engels: Peer to Peer (P2P) network, dwz gelijke-tot-gelijke). Het Bitcoin netwerk is daardoor robuust: het is niet eenvoudig uit te schakelen door bijv. een centrale server uit de lucht te halen. Dus ook uiterst storing-ongevoelig.
Er is ook geen centrale instantie, eigenaar, geen baas of directeur, noch helpdesk. Beslissingen over de verdere ontwikkelingen worden in consensus door een collectief van vrijwillige programmeurs genomen.

Digitaal Cash – Bitcoins hebben geen eigendomsbewijs: als een bitcoin in jouw wallet zit, is die kennelijk van jou. (Zoals contant geld in jouw porte-monnee in praktijk ook onbetwist van jou is). De dief van uw laptop met jouw bitcoins kan er over beschikken (daarom altijd met wachtwoord beschermen).

Pseudo-Anoniem – Transacties in Bitcoin worden gekenmerkt door het zgn *adres* van de ontvanger (begunstigde) en de afzender (betaler). De identiteit (naam, woonplaats e.d.) van de beide partijen is op geen enkele wijze onderdeel van de vastgelegde bitcoin transactie. Dit is de reden dat Bitcoin ook gebruikt wordt voor minder zuivere aankopen als verdovende middelen (net als met contant geld). Ook witwassen is van gewoon geld is met Btitcoin mogelijk.
Bitcoin is niet 100% anoniem, omdat vervolg-transacties met elkaar in verband gebracht kunnen worden, dus als de identiteit achter 1 adres eenmaal bekend is, kunnen betalingen wél aan elkaar gerelateerd worden.

Termen

Adres - Een bitcoin adres wordt gevormd door een reeks letters en cijfers, 27 tot 34 posities lang, met het cijfer 1 aan het begin. Een 'adres' is te vergelijken met een bankrekening-nummer. De meeste mensen hebben maar 1 of enkele bankrekeningen, bij Bitcoin kan je zo veel adressen voor jezelf aanmaken als je wilt: 1 voor transacties met familie, 1 voor aankopen enz. Je kan zelfs per individuele transactie een nieuw nummer hanteren. Voorbeeld:

`1e78Ugas23jH238J09ePkalHw9eb3nSd`

Wallet - de digitale portemonnee: effectief het bestand op je pc of smartphone, of online, met je bitcoins; het bevat een private key.

Transactie - een hoeveelheid bitcoins wordt van wallet A naar wallet B overgemaakt. De verzender heeft een *public address* nodig van de wallet van de ontvanger.

Blockchain - het publieke grootboek van alle transacties die in het Bitcoin netwerk zijn uitgevoerd. Elke Bitcoin gebruiker houdt een volledige kopie van deze blockchain op haar computer. (nu enkele GB). De blockchain is op blockchain.info online in te zien. De transacties worden anoniem vastgelegd in de blockhain.

Cryptografie - versleuteling van digitale informatie. zonder private key is de informatie niet te ontcijferen. Cryptografie is een wezenskenmerk van Bitcoin en andere cryptocurrencies.

Double Spending - de grootste uitdaging is de voorkoming van digitale valsemunterij, het meer dan 1 keer uitgeven van dezelfde bitcoin. Dit is bij btc geniaal opgelost, zonder centrale controle/autoriteit, met de zgn 'proof of work' methode, uitgevoerd door miners.

Client - software om gebruik te maken van het Bitcoin netwerk. Bijv: MultiBit en BitcoinQT. Zie bitcoin.org/clients.

Public address - bitcoin adres waarop men bitcoins ontvangt. Ook de afzender wordt gekenmerkt door een 'public address'. (vergelijkbaar met bankrekening nummers).

Private key - de kern van een wallet: de code waarmee btc uitgaven gedaan kunnen worden. Aan 1 private key kunnen ontelbare *public addresses* worden gekoppeld.

21 Miljoen - het aantal Bitcoin dat maximaal geproduceerd zal worden. Een misverstand is dat door deze limiet nooit een economie volledig op Bitcoin zou kunnen draaien. Dit klopt niet, want 1 Bitcoin kan heel veel waard zijn en tegelijk schier eindeloos opgedeeld worden. Misschien koop je in de toekomst een auto voor een mili-Bitcoin.

Beleggingscategorie - Is Bitcoin een valuta, een grondstof, een verzamel-object, een aandeel, een elektronisch edelmetaal? Het lijkt van ieder van deze categorieën wel enkele eigenschappen te bezitten, maar is toch zó afwijkend dat het een eigen beleggings- categorie vormt.

Belastingen - Omdat Bitcoin transacties pseudo-anoniem zijn, zijn deze in beginsel aan het oog van de overheid onttrokken. Belastingen op transacties (denk aan btw) zijn enkel mogelijk bij vrijwillige opgave van de belastingplichtige of via een andere registratie.

Alt Coins - er zijn al vele op bitcoin lijkende cryptocurrencies in omloop: Litecoin, Primecoin, Feathercoin e.d. Echter, Bitcoin heeft een flinke voorsprong in het zgn netwerk-effect: het is vele malen groter dan deze alternatieven en dát is reden op zich om te verwachten dat dit zo blijft.

Satoshi Nakamoto - de naam van de bedenker en programmeur van Bitcoin. Naar wordt aangenomen een pseudoniem van een groep deskundigen op academisch niveau. Van hem is sinds 2010 niets meer vernomen.

Volatiliteit - Bitcoin's prijs fluctueert erg, dit noemen we een sterke volatiliteit; gedurende perioden met verhoogde media aandacht stijgt de prijs met 10-tallen % per maand, om daarna weer te dalen. De verwachting is dat met de groei van de omvang van de btc economie, de volatiliteit zal afnemen.

Brain Wallet - makkelijker te onthouden wijze van private key in de vorm van bijv een reeks woorden (bijv 'fiets terts ader Lent'). Biedt fascinerende mogelijkheid om met enkel kennis van deze zin toegang tot eigen bitcoins te hebben. (Het wallet bestand kan dan in feite worden verwijderd. Zin vergeten? bitcoin verloren!).

Paper Wallet - de kern van een wallet is de *private key*. Deze kan ook afgedrukt worden en bewaard in kluis of elders opgeborgen.

Risico - Bitcoins zijn risicovol: een verloren wallet, zonder goede backup van wallet bestand of private key / brain wallet, betekent bitcoins onherroepelijk kwijt. Bitcoins naar een verkeerd/niet-bestaand adres sturen leidt idem tot onherroeplijk verlies. Er is geen service nummer te bellen...

Libertarisme - een politieke stroming die een kleine overheid met bescheiden uitgaven en 'hard' geld voorstaat. VS oud-senator Ron Paul is de bekendste. Bitcoin lijkt erg aan te slaan bij veel libertariërs.

Market Cap - markt kapitalisatie, de totale waarde van alle bitcoins tegen de huidige koers. In oktober 2013: 11 miljoen bitcoin à 140 euro = plm 1.5 miljard euro.

"Oneerlijk!" - Zij die vroeg in het Bitcoin avontuur instappen, verdienen mogelijk een mooi (bitcoin) vermogen. (Volgens velen is het nog steeds 'vroeg'). Laatkomers zullen dat voordeel niet hebben. Dit wordt wel als 'oneerlijk' bestempeld, met name vanuit een perspectief waarbij het aangaan van financieel risico geen reden tot beloning is. Ter vergelijk: zij die bijv. vroeg Apple aandelen kochten hebben ook goed geboerd.

"Pyramide spel!" - Sommigen beweren dat Bitcoin een pyramidespel is. Dit is niet juist: er is namelijk geen centrale organisator en er wordt door niemand rendement beloofd. Zie wikipedia voor uitleg van pyramidespel en het verwante Ponzi-scheme.

"Zeepbel!" (bubble) - De enorme prijsontwikkeling van btc lijkt wel op een huizenprijzen-zeepbel, de dot-com aandelen hype of de tulpen-manie uit de 17e eeuw. Echter, zeepbellen worden altijd gevoed door overdaad aan goedkoop krediet, daarvan is bij btc geen sprake.

"Zonder internet geen Bitcoin!" - dat klopt: als internet niet functioneert kan je niks met Bitcoin. Telebankieren werkt dan overigens ook niet en tevens handel en industrie komen tot een stilstand. Er is dan dus een groter maatschappelijk probleem dan geen toegang tot je Bitcoin hebben.

Politiek en Monetaire zaken

De Dollar, de Euro en de Yen hebben grote problemen: in de respectieve economieën zijn overheden, particulieren en banken (te) hoge schulden aangegaan. We spreken dan ook van krediet-crises. Volgens velen gaat het oplossen van deze crises met grote ellende gepaard, onder andere met geldontwaarding: geld zal worden 'bijgedrukt' waardoor schulden makkelijker af te betalen zijn. Echter spaarders en gepensioneerden zien de koopkracht van hun (rente)inkomsten dan dalen.

Bitcoin, met zijn harde limiet van 21milj, knaagt dan ook aan de macht van traditionele instellingen als banken en centrale banken en er is bij de toenemende adoptie van Bitcoin nog veel weerstand te verwachten. Echter, de opzet van Bitcoin maakt het technisch dwarsbomen van Bitcoin in elk geval lastig.

Bitcoin is **positief geld**: het bitcoin systeem zelf kent geen schuld/krediet systematiek en 'rood staan' kan niet. Sparen in bitcoin geeft 1 zekerheid: door de limiet van 21 miljoen bitcoin, is de ontwaarding wegens inflatie gelimiteerd (en na 2140 zelfs onmogelijk).

Ook 'bail-ins', waarbij banken een deel van het spaargeld van deposito-houders afromen in opdracht van de nooddruftige overheid (Cyprus, juni 2013) zijn met Bitcoin natuurlijk niet mogelijk.

Vertrouwen - Bitcoin is erop gebaseerd dat je niemand, zeker geen regering of bank, hoeft te vertrouwen. Wél dien je te vertrouwen op de (crypto- grafische) wiskunde die ten grondslag ligt aan het Bitcoin protocol en het collectieve groepsproces van de programmeurs. Bitcoin software is volledig *open source*.

Bronnen (NE=nederlands, EN=engels)

- www.bitonic.nl - NE bitcoins uit voorraad kopen per iDeal en verkopen
- www.bitcoin.de - EN bitcoins verhandelen per SEPA overmakingen
- www.bitcoin.org - EN bitcoin programma (client) downloaden. Multibit aanbevolen voor 1e kennismaking.
- www.blockchain.info - NE veel informatie en live zicht op de blockchain
- www.blockchain.com/wallet - NE online wallet voor kleinere bitcoin bedragen, voor wie niet het gedoe van software installatie en veiligheid wil.
- www.localbitcoins.com – EN koop bitcoins in een café bij je in de buurt

Post, muziek, film en telefonie zijn enorm veranderd door de komst van resp. email, mp3, youtube en skype. Geld is het laatste bastion, dat was nog niet "ver-internet". Díe revolutie is nu met o.a. Bitcoin aan de gang.
Aanbeveling: Lees online over Bitcoin, koop voor 10, 50 of 100 euro aan Bitcoin en leer het kennen. Enkel er mee spelen geeft het idee van het revolutionaire karakter.