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 najaar 2009 en heeft sindsdien een stormachtige ontwikkeling doorgemaakt.

Bitcoin is de naam voor zowel het protocol, de wijze waarop in Bitcoin financiele transacties worden uitgevoerd als de naam voor de eenheid. Meedoen kan iedereen door gratis software te downloaden en op de eigen pc te installeren en Bitcoin bij een handelshuis of exchange te kopen (zie 'Bronnen').

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

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

"Wrijvingsloze" transacties - Gebruikers van Bitcoin software kunnen naar elkaar Bitcoin overmaken tegen zeer lage kosten. De snelheid kan wisselen van enkele minuten tot een uur of meer, maar de verwerking gaat dag en nacht, 7 dagen per week door.

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 soft- ware is volledig *open source*.

Nooit was het zo makkelijk en goedkoop om in enkele minuten op eer zaterdag 1.000 euro naar een nicht in Nieuw Zeeland over te maken.

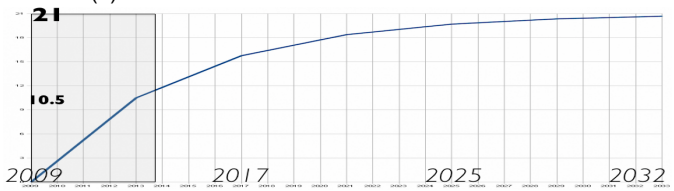
Of er nu ter waarde van een halve euro of een half miljoen euro bitcoins worden overgemaakt, de overmakings-**kosten** zijn in de orde van enkele eurocenten. Voor inwoners van Europa, die met het SEPA/IBAN bancair systeem tegen lage kosten geld kunnen overmaken is dit wellicht niet zo bijzonder, maar 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 lage kosten.

De waarde van Bitcoin

Bitcoins worden verkocht en gekocht , er is wereldwijd een levendige handel. Er dan ook sprake van koersvorming. De waarde van Bitcoin wordt uitgedrukt in traditioneel geld als de Euro of Dollar. Eind oktober 2013 was de koers ongeveer 140 euro per bitcoin.

De eerste Bitcoin transactie (2010?) was een pizza die verkocht werd voor 10.000 bitcoins. 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 waarde vermoedelijk nog wel enkele keren met een factor 10 toenemen. (grafiek in $)

"Mining" (delven) - Een van de meest fascinerende aspecten van Bitcoin is hoe nieuwe Bitcoins tot stand komen: deze worden elektronisch gedolven door wiskundige puzzels op te lossen, waarvoor veel rekenkracht nodig is. Deze puzzels bewaken op een slimme wijze het btc systeem tegen valsemunterij. Zware computers (ASIC's), die veel stroom gebruiken, dienen hiervoor te worden ingezet. Dit moeilijk uit te leggen mechanisme waarborgt in elk geva tegelijk (a) een geleidelijke uitgifte volgens een voorgeschreven *steeds trager* verloop met 21milj als maximum, als in onderstaande curve en (b) met veel rekenkracht bewaakte transacties.



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 mil staan en pas in 2140 wordt de laatste, de 21 miljoenste, bitcoin gedolven.

Bitcoin is 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 niet eenvoudig uit te schakelen omdat dan honderduizenden pc's uitgeschakeld zouden moeten worden. Er is geen centrale instantie, geen baas of directeur. Beslissingen over de verdere ontwikkelingen worden in consensus door een collectief van vrijwillige programmeurs genomen.

Cash, dwz bezit = eigendom
Bitcoins hebben geen eigendomsbewijs: als een bitcoin in uw wallet zit, is die kennelijk van u. (Zoals baar geld in uw portemonnee in praktijk ook onbetwist van u is).
De dief van uw laptop met uw bitcoins kan er over beschikken (daarom altijd met wachtwoord beschermen).

Bitcoin transacties zijn **definitief**. Bank- en creditcard transacties zijn vaak 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).

Bitcoin is (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 bitcoin transactie en ook de *blockchain* bevat geen identieitsinformatie.. Dit is de reden dat Bitcoin ook gebruikt wordt voor minder zuivere aankopen als verdovende middelen (net als met kontant geld).
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 wel betalingen getraceerd 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 met uw 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 centrale logboek van alle transacties die in het Bitcoin netwerk zijn uitgevoerd. Elke Bitcoin gebruiker houdt een volledige kopie van deze blockchain op jaar computer (!). (nu enkele GB).

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.

Client - software om gebruik te maken van het Bitcoin netwerk. Bijv: MultiBit en BitcoinQT. Zie Bronnen.

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

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

Pyramide spel - is een frauduleus beleggings systematiek waarbij de inleg van nieuwkomende beleggers deels uitgekeerd wordt aan eerdere beleggers, om de indruk van een goed rendement te geven. Uiteindelijk gaat de organisator van het pyramidespel er met de inleg van de laatste inleggers vandoor. Sommigen beweren dat Bitcoin een pyramide spel is. Echter: er is geen centrale organisator en er wordt door niemand rendement beloofd. Ook wel 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, bubbles worden altijd gevoed door overdaad aan goedkoop krediet, daarvan is bij btc geen sprake.

"Het Bitcoin systeem is oneerlijk"

De early adopters, mensen die vroeg in het Bitcoin avontuur zijn ingestapt, verdienen naar alle waarschijnlijkheid een mooi (bitcoin) vermogen. Laatkomers betalen meer voor bitcoins. Dit wordt wel als 'oneerlijk' bestempeld, met name vanuit een (socialistisch) perspectief waarbij het aangaan van financieel risico geen reden tot beloning is.

Beleggingscategorie - Is Bitcoin een valuta, een grondstof, een verzamelobject, 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 Bitcoins 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.

Altcoins - er zijn al vele op bitcoin lijkende cryptocurrencies in omloop: Altcoin, 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.

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 zin (bijv 'kortj@kjeS zijN alt00S zieK'). 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: wie haar wallet bestand kwijt raakt, zonder goede backup van wallet bestand of private key / brain wallet, die is de bitcoins onherroepelijk kwijt. Bitcoins naar een verkeerd/niet-bestaand adres sturen leidt idem tot *onherroeplijk* verlies.

Libertarisme - een politieke stroming die een kleine overheid met bescheiden uitgaven en 'hard' geld voorstaat. Bitcoin lijkt erg aan te slaan bij veel libertariers.

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.

"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 het niet kunnen werken met Bitcoin.

Bitcoin en Politiek

De Dollar, de Euro en de Yen hebben grote problemen: in de respectieve economieën zijn overheden, particulieren en banken veel te veel 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 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 depostiehouders afromen in opdracht van de nooddruftige overheid (Cyprus, juni 2013) zijn met Bitcoin natuurlijk niet mogelijk.

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

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 café bij u in de buurt

Post, muziek, film en telefonie zijn enorm veranderd door de koms 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! Vorm geen mening zonder deze ervaring!