Daan Bouwsema

18-2-2019

KBG

AG6D

Informatica

De digitalisering van het Geld



# **Voorwoord**

Voor het schrijven van dit profielwerkstuk leek het mij leuk om twee onderwerpen te combineren: De digitalisering van de wereld en zoals de titel doet vermoeden geld. Als schoolvak zou dit dus kunnen passen bij economie en informatica. Mijn voorkeur ging echter uit naar informatica omdat ik inschatte dat er door de digitalisering een grotere rol voor informatica zal komen. Ik hoop veel te leren van het schrijven van dit profielwerkstuk en op een goede conclusie als afsluiting. Bovendien wil ik mijn vader bedanken voor het nalopen van de tekst op fouten.

Inhoudsopgave

[**Voorwoord 1**](#_Toc535754646)

[**Inleiding 3**](#_Toc535754647)

[**Hoofdstuk 1 4**](#_Toc535754648)

[Cijfers 4](#_Toc535754649)

[**Incidenten op cybergebied in Nederland 4**](#_Toc535754650)

[**Wereldwijde statistieken op cybergebied 5**](#_Toc535754651)

[**Cyberbeveiliging maatregelen 6**](#_Toc535754652)

[**Problemen cijfers? 7**](#_Toc535754653)

[Cybersecurity Versus Cybercrime, de methodes in de praktijk. 8](#_Toc535754654)

[**Toenemende opties cybercriminelen & gevolgen 8**](#_Toc535754655)

[**Hoofdstuk 2 10**](#_Toc535754656)

[Veiligheid cryptovaluta’s 10](#_Toc535754657)

[**Cryptovaluta bemachtigen 11**](#_Toc535754658)

[**Cryptovalutamining 11**](#_Toc535754659)

[Cryptovaluta vervanger huidige valuta’s? 12](#_Toc535754660)

[**Voordelen van cryptovaluta ten opzichte van normale valuta 12**](#_Toc535754661)

[**Nadelen van cryptovaluta ten opzichte van normale valuta 12**](#_Toc535754662)

[**Overheden en hun blik op cryptovaluta 12**](#_Toc535754663)

[**Hoofdstuk 3 14**](#_Toc535754664)

[Officiële verbindingen aan cryptovaluta 14](#_Toc535754665)

[**Interesse in cryptovaluta van banken 14**](#_Toc535754666)

[**Landen over cryptovaluta 14**](#_Toc535754667)

[Verantwoordelijkheden cryptovaluta 14](#_Toc535754668)

[Digitalisering van betalingsmogelijkheden 15](#_Toc535754669)

[**Mobiel bankieren apps 15**](#_Toc535754670)

[**Aansprakelijkheid internetbankieren 15**](#_Toc535754671)

[**De conclusie 17**](#_Toc535754672)

[**Wat zijn de gevolgen van het digitaliseren van het geld voor consumenten? 17**](#_Toc535754673)

[**Wat zijn de gevolgen van het digitaliseren van het geld voor banken? 17**](#_Toc535754674)

[**Wat zijn de gevolgen van het digitaliseren van het geld voor overheden? 18**](#_Toc535754675)

[**Hoe zit het met de veiligheid en privacy van het nieuwe geld? 18**](#_Toc535754676)

[**Hoe ziet de toekomst van ons geld eruit? 18**](#_Toc535754677)

[**Literatuuropgave 19**](#_Toc535754678)

[**Bijlagen 21**](#_Toc535754679)

[**Begrippenlijst 22**](#_Toc535754680)

[**Nawoord 23**](#_Toc535754681)

# **Inleiding**

De laatste paar jaar gaat het steeds vaker in het nieuws over de opkomst van het internetbankieren, de groeiende cryptovaluta en internetwinkels die miljarden producten verkopen over de hele wereld. Velen zien dit als de toekomst en verwachten dat je boodschappen via het internet kunnen worden besteld en dat alles via de handige apps van de banken kan worden betaald en geïnd. Op het internet is de laatste jaren ook veel groei gezien in de verschillende cryptovaluta die de banken buitenspel zetten, doordat dit allemaal via het internet gaat is het minder vertrouwd dan het oude contante geld als ruilmiddel voor producten. Een andere kant van de digitalisering van het geld is de veiligheid ervan en hoe we dat in de toekomst moeten gaan onderhouden en of er toezicht op moet komen van overheden wat de veiligheid zou kunnen verbeteren, maar ook zou kunnen verzwakken als alles via één partij moet worden gespeeld, waardoor de gevaarlijke kanten van het gebruik van Internet naar voren zouden kunnen komen.

Oftewel hoe kunnen we door alle digitalisering er nog voor zorgen dat de gegevens van klanten, bedrijven en banken goed beschermd blijven in de toekomst? Op deze vraag ga ik aan het eind van het werkstuk mijn mening/conclusie geven door de deelvragen die ik in dit werkstuk stel te beantwoorden.

Als motivering voor dit onderwerp heb ik dat het een steeds belangrijkere rol gaat spelen in de toekomst en kennis over deze onderwerpen kunnen later hun vruchten afwerpen.

De wijze van onderzoek wordt een schriftelijkwerkstuk met een prognostische conclusie.

# **Hoofdstuk 1: Online veiligheid**

**Deelvraag**: 1.Kun je met 100% zekerheid zeggen dat online transacties of gegevens van een klant nooit door onbevoegde derde partijen kan worden onderschept of herleid??

Tegenwoordig gaan geldtransacties, het versturen van belangrijke informatie en privéinformatie via het internet, in toenemende mate zelfs via de mobiele telefoon. Voordelen zijn natuurlijk de mobiliteit en vrijheid die je krijgt om informatie te delen met anderen of om een betaling te doen. In tegenstelling tot vroeger waar je naar de bank moest gaan voor transacties en voor het versturen van informatie je naar de desbetreffende persoon moest gaan. Met de groeiende digitalisering is de veiligheid van de eerdergenoemde handelingen echter niet erg gegroeid en in vergelijking met vroeger misschien zelfs wel afgenomen. Is er überhaupt een garantie voor een veiligheidsmethode in de digitale wereld waarbij je 100% zeker kunt zijn dat je gegevens of informatie alleen door jezelf en/of de partij waar je het naar toe stuurt kan worden gelezen?

## **Cijfers**

De afgelopen jaren is er veel geïnvesteerd in de beveiliging van het internet in het algemeen. Toch blijkt uit cijfers dat er vaak incidenten gebeuren op het gebied van Informatie en Communicatie Technologie (ICT) , wordt de online wereld veiliger of juist niet?

### **Incidenten op cybergebied in Nederland**

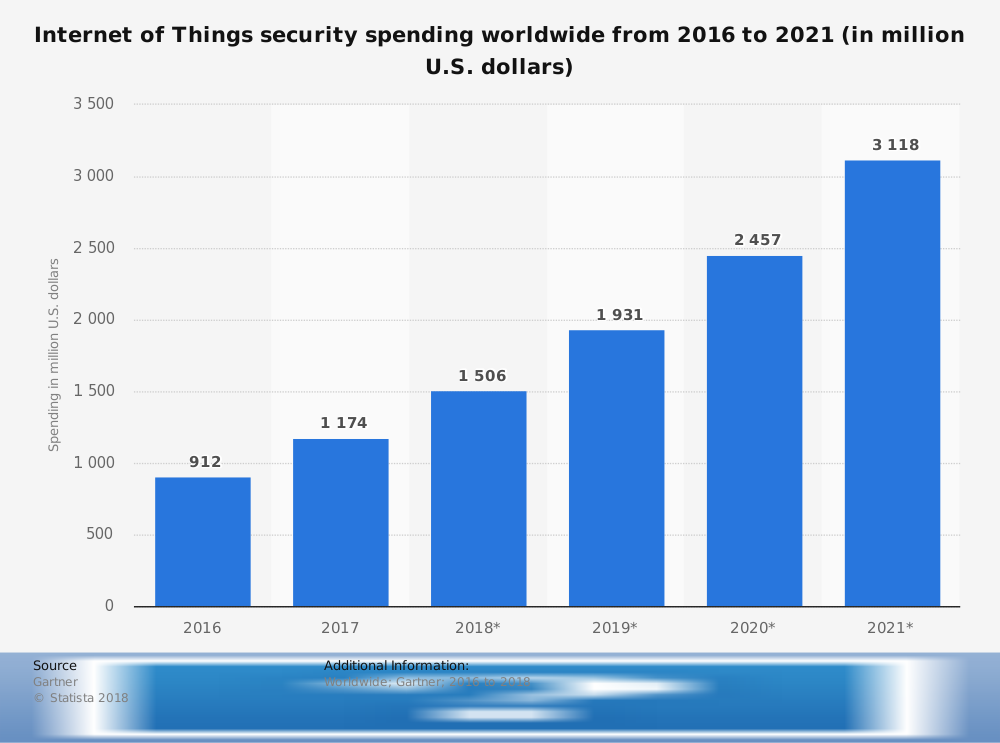
[[1]](#footnote-1))In Nederland is 1 op de 9 personen in 2017 slachtoffer geworden van een *cybercrime*. Een cybercrime is een delict (strafbaar feit) dat wordt gepleegd met behulp van ICT. Toch zijn dit niet alle incidenten die gebeuren met gegevens of informatie op het internet, vaak gaat het per ongeluk mis tijdens het gebruiken van systemen. [[2]](#footnote-2))Zo zijn er in 2017 10.009 datalekken gemeld bij de Autoriteit Persoonsgegevens (AP) , deze meldingen van datalekken door organisaties zijn sinds 2016 verplicht door de wet. Vaak zijn deze datalekken veroorzaakt door nalatigheid door de houder er van, maar er kan ook sprake zijn van doelbewust hacken om aan deze vertrouwde gegevens te komen, in 2017 was dat in 6% van de gevallen zo. Het aantal datalekmeldingen is vergeleken met 2016 verdubbeld in 2017 en de meeste meldingen kwamen uit de sectoren; Gezondheid en welzijn, en Financiële dienstverlening.

### **Wereldwijde statistieken op cybergebied**

Hiernaast in [[3]](#footnote-3)figuur 1 zie je op wereldwijde schaal het aantal biljoenen USA Dollars dat een land totaal aan kosten heeft gehad door cybercrime in 2017. Deze kosten worden gevormd door opbrengsten van verschillende soorten cybercriminaliteit waarvan onder andere *ransomware* en *dataleaks*. China spant in 2017 ruim de kroon met 66,3 biljoen dollar, gevolgd door Brazilië met 22.5 biljoen. Nederland staat op de zestiende plaats met 1,6 biljoen.

**Figuur 1;**

**Bron: Gartner,Statista.com**

[[4]](#footnote-4) In figuur 2 kun je de voorspelling zien van de totale uitgave aan cybersecurity op wereldwijd gebied. In de jaren 2016-2021 wordt er een stijging verwacht van 241% van de uitgaven.

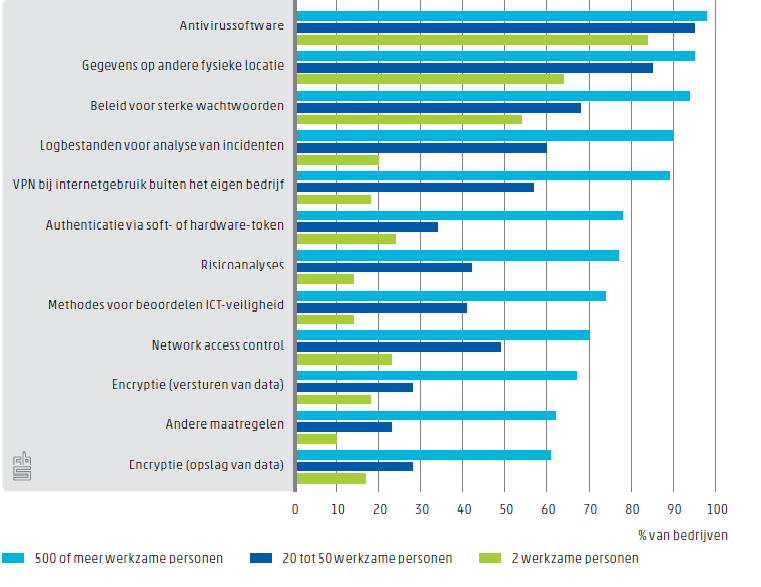
Figuur 2;

**Bron: Gartner, Statista.com**

### **Cyberbeveiliging maatregelen**

Om te zorgen dat er minder of geen incidenten meer gebeuren met data van bedrijven of personen, is er groeiende aandacht voor *cybersecurity,* het beveiligen van computers en internetnetwerken om zo vormen van cybercriminaliteit tegen te gaan.

[[5]](#footnote-5)De Nederlandse overheid heeft onlangs bekendgemaakt dat er eenmalig 30 miljoen extra naar de cybersecurity gaat in 2019. De koning heeft in de troonrede van dinsdag 18 september 2018 gezegd “Dat het nodig is de digitale infrastructuur van ons land te beveiligen. ” (Oranje-Nassau, 2018). Onderzoeksbureau Gartner heeft verondersteld dat over heel 2018 gezien er wereldwijd ongeveer 100 miljard euro aan investeringen zijn gedaan in de cybersecurity. Gartner verwacht dat in de komende jaren de investeringen in cybersecurity blijft stijgen, dit komt mede door strengere privacyregels in de EU waaraan bedrijven zullen moeten voldoen.

**Bedrijven**

Figuur 3; Soorten cybersecurity bedrijven NL

[[6]](#footnote-6)) Uit onderzoek van het CBS blijkt dat grotere bedrijven vaak betere maatregelen nemen in de ICT-beveiliging dan de kleinere bedrijven, ook kan er een onderscheid worden ontdekt in de sectoren qua beveiliging. De Informatie- en communicatiesector lopen samen op kop met de financiële sector. De desbetreffende sectoren zijn dan ook gevoeliger op het gebied van de ICT in vergelijking met de andere. In 63% van de grotere bedrijven wordt er gewerkt met intern cybersecuritypersoneel dat verantwoordelijk is voor de beveiliging van het hele bedrijf. Beveiligingsmanieren die ze gebruiken zijn uitgebreide encryptie technieken om zo informatie te versleutelen en het opstarten van eigen netwerksystemen binnen een bedrijf. Bij de kleinere bedrijven is de beveiliging vaak extern geregeld en minder complex, dit komt door de mindere financiële middelen. In figuur 3 kun je de verschillende soorten cybersecurity zien die worden toegepast bij bedrijven in Nederland. Enkele voorbeelden zijn antivirussoftware, beleid voor sterke wachtwoorden en authenticatie via soft- of hardware-token.

**Persoonlijk**

Er is door het CBS ook onderzoek gedaan naar cybersecurity bij personen. 46% van Nederlandse bevolking boven de 12 jaar zegt (online)- Clouddiensten te gebruiken voor het opslaan van privézaken. De computer loopt procentueel voor op de mobiele telefoon op het gebied van antivirusprogramma’s en firewall. Verder neemt de bekendheid van internetcookies toe in Nederland en ook waar deze cookies voor worden gebruikt.

Een belangrijk securitysysteem voor webpagina’s is het DNSSEC. Dit is een systeem dat ervoor zorgt dat een IP-adres een authentieke code krijgt waarmee het enkel naar de juiste domeinnaam kan worden geleid. Hiermee kan het dus niet dat als je naar een bepaalde site wil dat je naar een andere site wordt geleid die zich voordoet als die andere site. Dit werkt goed tegen de fraudedelicten phising en pharming. Ruim 60% van de Nederlandse sites gebruikt deze beveiliging.

### **Problemen cijfers?**

Veel van de bovenstaande cijfers worden zo nauwkeurig mogelijk berekend, maar toch zeggen vele deskundigen dat dit niet opgaat voor de praktijk. In de traditionele criminaliteit weet het slachtoffer vaak dat iemand de wet heeft overtreden, bij cybercriminaliteit is het heel goed mogelijk dat het slachtoffer zelf er niets van weet en er ook nooit zal achter komen dat iemand hem/haar bijvoorbeeld heeft gehackt of malware op de computer heeft binnengelaten. Deze wettelijke overtredingen zullen dus vaak niet gemeld worden simpelweg door het feit dat mensen het niet door hebben.

Doordat er sprake is van de digitalisering van de wereld zou je dus kunnen verwachten dat cybercrime aan het groeien is, toch kan dit niet worden bevestigd. De cijfers van de cybercrime lijken in de afgelopen jaren te zijn gestabiliseerd.

Op het gebied van de beveiliging en de criminaliteit in de ICT lijkt er dus geen echte winnaar aanwijsbaar te zijn van de afgelopen jaren. De cijfers die er zijn, zijn stabiel en lijken aardig in balans met elkaar. De beveiliging wordt steeds breder en complexer, maar dit geldt ook voor de aanvallen van de cybercriminelen.

## **Cybersecurity Versus Cybercrime, de methodes in de praktijk.**

Om de veiligheid en privacy van gegevens te waarborgen in de digitale wereld, worden er steeds nieuwere en betere veiligheidssystemen gemaakt die tegen de nieuwste soorten cyberaanvallen kunnen worden gebruikt.

### **Toenemende opties cybercriminelen & gevolgen**

Door de toenemende mate van digitalisering krijgen kwaadwillenden steeds meer mogelijkheden om achter informatie en gegevens te komen van personen en bedrijven. Denk aan de toenemende open netwerken, waardoor iemand gemakkelijk een kijkje kan nemen binnen jouw *device* (apparaat) en zo alles over jou te weten kan komen. Een andere manier om ergens binnen te komen is natuurlijk het omzeilen van de firewall van een systeem, oftewel het originele hacken. Door de jaren heen worden er steeds nieuwere hackmanieren bedacht die iemand kan gebruiken bij het begaan van cybercrimes.



Figuur 4 Internet of Things

Alles staat in verbinding met elkaar

Verder helpt het Internet of Things (**IoT**) mee aan de inbreekopties voor cybercriminelen. Als voorbeeld hiervan kun je de moderne koelkasten geven. De koelkast staat in verbinding met het netwerk binnen een huis. Een cybercrimineel zou dus theoretisch via de koelkast mee kunnen kijken in het internetnetwerk van een huishouden. Doordat dit in de toekomst een mogelijke standaard wordt voor producten in een huis, neemt de veiligheid en discretie dus af en zijn er dus weer meer manieren voor cybercriminelen om ergens binnen te komen zelfs via de raarste omwegen. Deze technische ontwikkelingen zijn dus niet alleen bruikbaar voor een betere levensstandaard voor de eigenaar, maar ook een nieuwe toegang voor internetcriminelen.

De gevolgen van cybercrimes kunnen erg verschillen per deelgebied en tevens in grootte. Op het gebied van internetbankieren en phishing zijn er voor het slachtoffer voornamelijk negatieve economische gevolgen volgen, zoals geldafschrijvingen. Door recentelijke Europese regelgeving moeten bedrijven gegevens van klanten nu goed beveiligen, dit behoort tot de privacy van de klanten. Als een kwaadwillende deze gegevens weet te achterhalen door middel van hacken of een andere cybercrime zullen er voor het bedrijf grote negatieve gevolgen zijn. De klanten zullen als dit gebeurt niet tevreden zijn over het getroffen bedrijf en dit zal zorgen voor een daling in opbrengsten voor het bedrijf, ook op marketinggebied zal het bedrijf een slecht figuur slaan.

Om te voorkomen dat dit gebeurt zijn er dus veiligheidssystemen en andere soorten van cybersecurity. Om te zorgen voor steeds nieuwere en betere systemen, word er gebruik gemaakt van voornamelijk hackers. Doordat hackers (in dienst van een bedrijf/instantie) of ethische hackers, de beveiliging doorzoeken op zwakke punten . Door het adresseren van deze zwakke punten kan de cybersecurity worden verbeterd en zo kan het gegevens van klanten en vertrouwelijk informatie beschermen tegen de nieuwste cybercrime methodes.

Om terug te komen op de deelvraag die aan het begin van het hoofdstuk werd geïntroduceerd, Of je 100% zeker kunt zijn dat jouw online gegevens en transacties veilig zijn en niet door andere kunnen worden onderschept of herleid. Het antwoord op deze vraag is nee. In grote mate zal alles online goed worden beveiligd en zeker in de economische sectoren neemt deze beveiliging een steeds beter niveau aan. Zoals je terug kon zien in Figuur 2 wordt er verwacht dat er nog meer geld gaat naar de beveiliging in de toekomst. Er wordt dus zeker nagedacht over hoe alles te kunnen beveiligen. Toch zal je op cybersecurity gebied nooit met 100% zekerheid kunnen zeggen dat alleen jij en het bedrijf/instantie waar je een transactie naar maakt of gegevens hebt naar verstuurd de enige twee deelnemers zijn die de transactie of informatie hebben “gezien of genoteerd”. Zo is er ook de discussie of autoriteiten zoals de AIVD en FBI toegangen mogen krijgen tot bankgegevens van een verdachte.

Toch laat de praktijk zien dat er veel voorbeelden zijn van fouten in de onlinebeveiliging van gegevens. Zo zijn er de dataleaks bij grote bedrijven de afgelopen jaren, werd de onhackbare cryptowallet Bifti binnen een week gehackt en worden geheime rapporten buit gemaakt bij cyberaanvallen. Cybercriminelen zullen dus blijven zorgen voor die paar percentage onzekerheid die een kritische houding tegenover de digitalisering en de veiligheid daarvan zullen versterken.

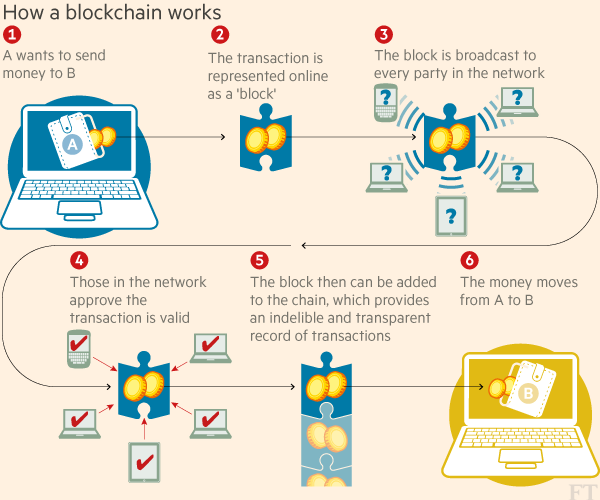
# **Hoofdstuk 2: De strijd der valuta’s**

**Deelvraag:** Zijn de nieuwe valuta van de afgelopen jaren goed te beveiligen en zou dit ervoor kunnen zorgen dat de fysieke valuta in de toekomst niet meer bestaat?

Bitcoin, Ethereum en Ripple zomaar een paar van de grootste cryptovaluta’s van deze tijd. De afgelopen jaren hebben deze digitale valuta’s zich laten gelden als een alternatief voor de reguliere betalingsmiddelen in de wereld. In totaal zijn er nu ongeveer 1300 verschillende cryptovaluta’s, de bekendste: Bitcoin. Bitcoin heeft zich de afgelopen jaren sterk ontwikkeld, maar nu lijkt de zogenaamde “bubble” te zijn gebarsten. Officiële autoriteiten en overheden zien cryptovaluta’s nog niet als gelijke aan de eigen traditionele valuta door onzekerheden over “het nieuwe geld”. Zo zou het nog te gevoelig zijn voor hackers, zijn de risico’s van investeringen erin nog te groot en is er te weinig stabiliteit in de koers. Gaan we in de toekomst afscheid nemen van de klassieke tastbare valuta en stappen we over naar de cryptovaluta op het internet om ons geld daar te bewaren en mee te handelen?

## **Veiligheid cryptovaluta’s**

Een vaak voorkomend argument tegen de cryptovaluta’s is de onzekerheid op het gebied van de beveiliging. Er wordt door vele financiële instanties gewaarschuwd voor de gevaren van het investeren in cryptovaluta’s. Er is namelijk geen 3de partij die de gegevens en de veiligheid checkt van een transactie zoals een bank doet bij een normale valuta. Hierdoor is er dus minder bescherming bij het handelen. Ook zijn er bij cryptovaluta’s risico’s om gehackt te worden. Om te voorkomen dat een hacker jouw cryptogeld van je computer haalt zijn er speciale wallets ontwikkeld. Dit zijn een soort kluisjes met cryptogeld erin die op je computer staan. Ze maken geen gebruik van een netwerk waardoor ze moeilijk te hacken zijn.

Om de echte cryptovaluta te beveiligen word er gebruik gemaakt van de blokchain techniek. Dit is een systeem van algoritmes en datastructuren dat ervoor zorgt dat er beveiligde transacties gemaakt kunnen worden. Hieronder is in figuur 5 de basis van deze technologie uitgelegd.

Figuur 5

**Bron:WEForum.org**

**Toelichting figuur 5**

* Onder “every party” bij puntje 3 verstaan we de verzender, de ontvanger en mining computers voor bevestiging.
* “Those” bij puntje 5 zijn hetzelfde als bij puntje 3 genoemd.

### **Cryptovaluta bemachtigen**

Hoe kom je aan cryptovaluta? Je kan cryptovaluta kopen op daarvoor opgezette websites. Er wordt geadviseerd goed te kijken naar de betrouwbaarheid van de sites. Veel sites beweren de hoogst mogelijke uitbetaling in de cryptovaluta, maar het zijn soms geraffineerde oplichtsites. Het is dus van belang je goed te oriënteren voordat je cryptogeld gaat aanschaffen. Je kan voor een bepaalde hoeveelheid aan cryptogeld kopen in ruil voor een x aantal euro’s, afhankelijk van de koers van de cryptovaluta.

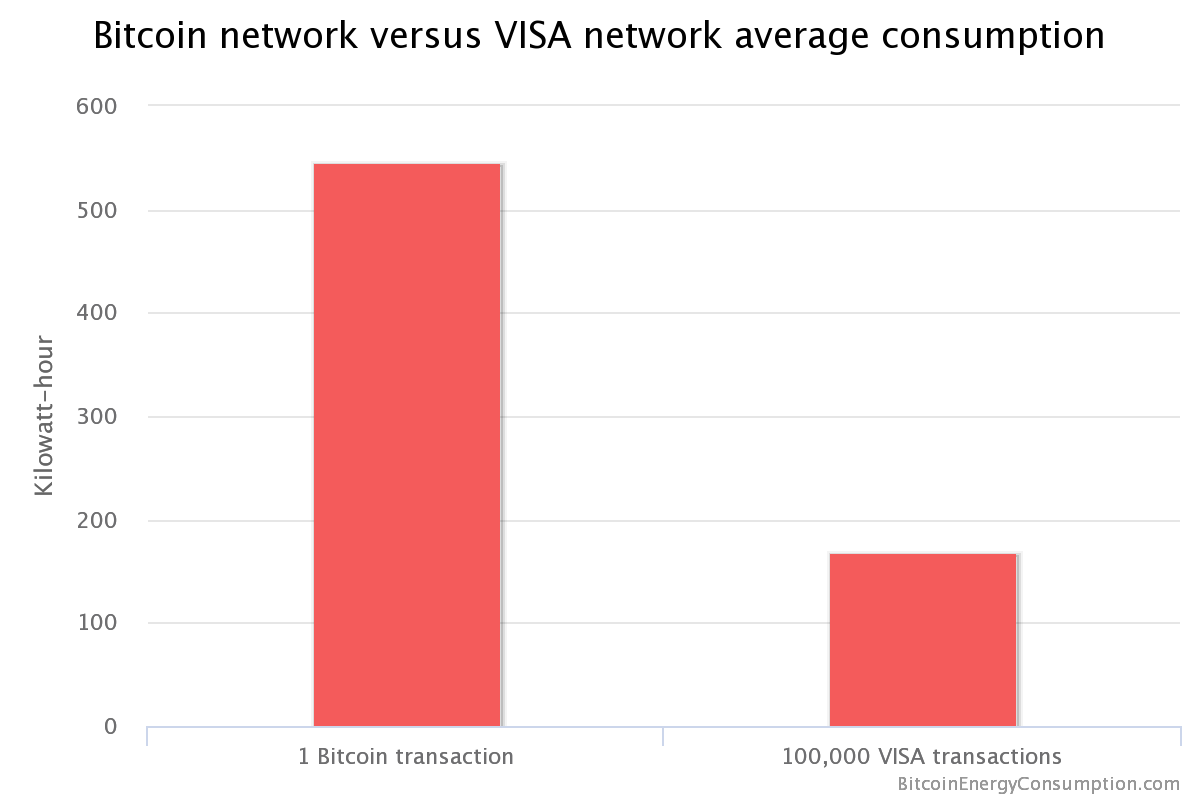
### **Cryptovalutamining**

Wat is *crypto mining*?

Cryptovaluta transacties moeten worden bevestigd in het systeem (de blockchain). Dit gebeurt door de zogenaamde miners. Zij hebben speciale computer apparatuur om zo snel mogelijk de berekeningen die nodig zijn te verrichten. Zij zullen echter niet voor niks hun apparatuur en stroom ter beschikking stellen. Als dank voor het onderhouden en controleren van de transacties. Krijgen ze “uitbetaald” in de cryptovaluta waardoor er een stimulans blijft voor mining.

Iedereen zou met de juiste apparatuur cryptovaluta kunnen minen, maar verreweg het grootste deel wordt gemined door Chinese bedrijven met megacomputers die enkel bezig zijn met mining. Door de opbrengsten van mining is dit een rendabele business geworden. Zelf kan je door verschillende mining-pools je computerrekenkracht bundelen met andere om zo de benodigde power voor de rekensommen te vergaren voor het mining-proces. De opbrengsten worden later eerlijk verdeeld. Door mining is er dus meer veiligheid in de cryptovaluta’s, want die worden hierdoor gecontroleerd op fouten en verbeteren deze.

Erg duurzaam is het cryptovaluta mining niet. Alleen al het energieverbruik van Bitcoin zou volstaan voor een 48ste plek op de lijst met landen en hun energieverbruik per jaar. Dit is gebaseerd op een rapport van de International Energy Agency (IEA). Alle cryptovaluta bij elkaar gebruiken dus een immens grote hoeveelheid energie. Om een perspectief te bieden ziet u hieronder een tabel met het energieverbruik van 100,000 VISA transacties en 1 Bitcoin transactie.



Over het algemeen kunnen de cryptovaluta worden gezien als veilig, op het gebied van beveiliging zijn er al goede methodes om te zorgen dat de valuta goed wordt beschermt. De manieren waarop je geld in de echte wereld kan verliezen zoals een overval of afpersing zijn vergelijkbaar met die bij cryptovaluta’s. Alleen in plaats van een fysieke overval wordt er geprobeerd bij het geld te komen via phising en andere cybercrime methoden. Een groter risico bij cryptovaluta in vergelijking met andere fysieke valuta is dat de opslag op 1 plek is namelijk de wallet, als die in de verkeerde handen zou komen ben je je gehele inhoud kwijt en kun je er niks tegen doen. Want je kan niet zoals met normale valuta melding maken bij de bank dat je pas is gestolen.

## **Cryptovaluta vervanger huidige valuta’s?**

De stormachtige opkomst van de cryptovaluta doet aan veel kanten vragen oprijzen. Is het ook een lange termijn alternatief voor de huidige valuta’s? Wat zijn de voordelen en nadelen ten opzichte van de huidige valuta’s. Wat is de visie van overheden en instanties over cryptovaluta? Kortom kunnen we een grote toekomst verwachten voor de cryptovaluta’s en misschien zelfs eventueel een afschaffing van de klassieke valuta’s?

### **Voordelen van cryptovaluta ten opzichte van normale valuta**

* Doordat elke cryptovaluta een unieke code heeft zal er minder fraude zijn met dupliceren. Het is onmogelijk om een duplicatie te maken er zal dus geen sprake zijn van nep biljetten zoals bij het huidige chartale geld. Ook zal het dus onmogelijk zijn om fraude te plegen door nagemaakte transacties.
* Decentralisatie van het geld. Dit betekent dat de macht van het geld niet meer bij een centrale organisatie ligt maar bij de gebruikers van de valuta. Door het afnemende vertrouwen in de centrale bestuur van het geld door onder andere de economische crisis.
* Cryptovaluta hebben over het algemeen lage transactiekosten, terwijl dit bij elektronische betalingssystemen zoals PayPal vele malen hoger ligt.
* Cryptovaluta is in zijn geheel privé. Er is geen registratie nodig bij een bank zoals wel het geval is met normale valuta.

### **Nadelen van cryptovaluta ten opzichte van normale valuta**

* Doordat cryptovaluta gebaseerd is op het gebruik van internet is het gevoelig voor storingen en het uitvallen van het internet. Dit betekent dus in geval van noodsituaties waarbij het internet het niet doet er in zijn geheel geen gebruik kan worden gemaakt van deze valuta. Normale valuta’s kunnen altijd worden gebruikt.
* Een gevolg dat kan worden genoemd bij voordelen en nadelen is de privacy die cryptovaluta met zich meebrengt. Het kan als nadeel worden beschouwd omdat door de anonimiteit het goed kan worden gebruikt bij criminele activiteiten en de financiering hiervan. Zo kan een persoon in Europa anoniem cryptovaluta sturen naar terroristische organisaties. Ook zouden geld witwassers en de handelaren in illegale goederen goed gebruik kunnen maken van de cryptovaluta.
* Cryptovaluta hebben het kenmerk een hoge volatiliteit te hebben. Als voorbeeld de Bitcoin die binnen een jaar van een waarde van $30 naar de $1000 schoot. Dit kan ook andersom zijn wat laat zien dat cryptovaluta niet een stabiele waarde kunnen aanhouden, en hier kan door decentralisatie ook niet worden ingegrepen door financiële instanties.

Deze voor en nadelen laten zien wat de gevolgen zouden zijn als we de cryptovaluta gaan zien als een legitieme valuta. Een belangrijke gedachte hierover is hoe we ons geld willen gaan gebruiken, nemen we de nadelen zoals het paradijs dat ontstaat voor criminelen door cryptovaluta voor lief in ruil voor meer vrijheid van ons geld? Verder zou een omschakeling in de toekomst naar alleen cryptovaluta een grote groep werkelozen met zich meebrengen, doordat er een noodgedwongen afscheid van de financiële instanties als gevolg is. Een logischere tussenweg is dat overheden cryptovaluta gaan accepteren en dat dit gebeurt met behoud van de huidige valuta’s. Maar wat is de kijk van overheden op cryptovaluta?

### **Overheden en hun blik op cryptovaluta**

Uit een brief[[7]](#footnote-7)van de Minister van Financiën Hoekstra 8 Maart 2018 aan de Staten Generaal is gebleken dat hij wilt dat Nederland een voortrekkersrol gaat spelen in het maken van regelgeving voor cryptovaluta. Uit de brief blijkt dat Hoekstra bijvoorbeeld reclame voor cryptovaluta’s zou willen verbieden en zou er sprake zijn van een toekomstige belasting over cryptovaluta. Voor de uitvoering van deze regels gaat Hoekstra in overleg met verschillende landen. De minister is nog zeer terughoudend over cryptovaluta’s en adresseert de grote risico’s en de verbanden met terrorisme van cryptovaluta in zijn brief.

De Europese Unie heeft zich recentelijk in een rapport[[8]](#footnote-8) uitgesproken over de toekomst van cryptovaluta in de Europese Unie. Uit het onderzoek (Janikowski & Dabrowski 2018) is voortgekomen dat de Europese officials de cryptovaluta serieus moeten nemen. De grotere cryptovaluta worden in het rapport onder de loep genomen en de kansen en bedreigingen ervan worden beschreven. Als casus voor een positieve werking van cryptovaluta als algemeen geaccepteerd ruilmiddel wordt Venezuela benoemd. Door hyperinflatie in dat land heeft President Maduro dit jaar de cryptovaluta Petro ingevoerd om zo de inflatie te stoppen. Naar eigen zeggen van Maduro zou het een succes zijn, maar dit moet nog blijken de komende tijd. Als conclusie van het rapport zagen de onderzoekers een toekomst in de cryptovaluta, maar zouden er nog wel negatieve aspecten zoals witwassen moeten worden verwijderd wil het een concurrent worden van de door overheid uitgebrachte valuta.

Een belangrijk punt is dat het huidige uitgaven van valuta via de overheid worden gedaan en dus ook gecontroleerd kan worden door overheden. Bij cryptovaluta is dit niet het geval en heeft de overheid dus minder controle en macht. Mede hierdoor zullen de meeste overheden kritisch zijn over de cryptovaluta in het begin, er wordt dus vooral gesproken over de regelgeving ervan. Deze regelgeving leidt tot het wegvallen van sommige voordelen van de cryptovaluta.

Als we terugkijken naar de deelvraag van dit hoofdstuk: Zijn de nieuwe valuta van de afgelopen jaren goed te beveiligen en zou dit ervoor kunnen zorgen dat de huidige fysieke valuta in de toekomst niet meer bestaat? Kunnen we over het eerste gedeelte een ja antwoorden. De beveiliging van het cryptogeld is over het algemeen zeer goed, wel moet je zelf investeren in een goede wallet wil je een veilige opslagplaats. Ook de bijdrage van mining versterkt de veiligheid van cryptovaluta’s. Maar dat mining zorgt aan de andere kant voor een zeer milieuonvriendelijk beeld bij cryptovaluta’s. Over het tweede gedeelte van de vraag is toch een ander antwoord te geven, een waarschijnlijke nee namelijk. In het rapport van de EU kun je lezen dat een totale overname van de huidige valuta in rijke landen zeer onwaarschijnlijk zal zijn. De cryptovaluta zal zoals al eerder genoemd altijd afhankelijk zijn van internet en dus gevoelig voor storingen, wat dus als gevolg heeft dat het niet altijd kan worden gebruikt, wat wel een van de grootste vereisten is van een valuta. Een andere reden waarom het niet de huidige valuta gaat vervangen is dat het simpelweg nooit zo ver zal komen door tussenkomst van overheden die zo proberen grip te houden op de gehele economie. Wel voorzien onderzoekers in de toekomst, als verschillende problemen van de cryptovaluta worden verholpen of verbeterd een grotere rol in de wereldeconomie.

# **Hoofdstuk** **3: Cryptovaluta instituut en verantwoordelijkheid betalingsmogelijkheden**

**Deelvraag:** Zou er een instituut moeten komen dat zorgt voor de cryptovaluta en transacties controleert of beveiligt en bij wie ligt de verantwoordelijkheid als er iets misgaat met het nieuwe geld en de betalingsmogelijkheden hiervan?

Over het eerste gedeelte van deze vraag zijn er verschillende meningen, want dit zou namelijk in strijd zijn met een van de fundamenten van cryptovaluta. Als een van de grondbeginsels bij cryptovaluta wordt namelijk de onafhankelijkheid ervan geprezen. Er zou geen derde partij bij transacties nodig zijn wat zorgt voor lage kosten en geen partij in de wereld zou inspraak hebben over de koers van de valuta. Voor mensen die de banken na de economische crisis wantrouwen is dit dus een mooi alternatief. Veel aanhangers van de cryptovaluta voorzien dan ook een ondergang als officiële organisaties zich gaan bemoeien met de valuta.

## **Officiële verbindingen aan cryptovaluta**

Er is steeds meer interesse is er van bedrijven en overheden over de hele wereld om zich te verbinden met de cryptovaluta. Door steun van deze bedrijven zal de markt zich verstevigen en meer zekerheid krijgen, wat dan wel weer zorgt voor een mindere fluctuatie van de koers en er dus minder winst zal zijn bij beleggingen. Maar als pluspunt ook mindere verliezen. Niet iedereen is hier voorstander van door al eerder uitgelegde redenen zoals decentralisatie.

### **Interesse in cryptovaluta van banken**

Meerdere banken in de wereld zijn zich aan het interesseren in de cryptovaluta wereld. Zo zouden Zwitserse banken cryptovaluta gaan accepteren. De Britse bank Barclays zou ook gaan werken met cryptovaluta en hier vooral mensen in willen helpen hoe te investeren erin. Maar eind 2018 werd dit plan stopgezet.

### **Landen over cryptovaluta**

In Rusland zou er sprake zijn van een eigen CryptoRuble als nationale cryptovaluta. Putin leek een paar jaar geleden niet erg te spreken over cryptovaluta. Zo zou hij gezegd hebben dat “cryptovaluta serieuze risico’s veroorzaken en worden gebruikt bij misdaden.” Toch lijkt in begin 2018 door uitspraken van Russische autoriteiten dat er wel degelijk een CryptoRuble komt, deze zou dan alleen te gebruiken zijn in Rusland. Volgens de financiële adviseur van Putin Sergei Glazyev zou het ontstaan van de CryptoRuble zorgen voor een verlichting van de westerse sancties gericht tegen Rusland. Deze ideeën worden overgenomen in Iran en Venezuela waar er ook interesse is in een eigen cryptovaluta.

## **Verantwoordelijkheden cryptovaluta**

Als er iets fout gaat bij cryptovaluta, wie is er dan aansprakelijk? Op deze vraag kan je nog niet echt goed antwoorden, simpelweg doordat er nog discussie is over de regelgeving over cryptovaluta. Bij een grote hack van een uitgever van een cryptovaluta, zoals er gebeurt is bij het bedrijf Mt. Gox in 2014. Mensen die via dit bedrijf handelden in Bitcoins hadden door een hack al hun totale 850.000 Bitcoins verloren. De totale waarde zou in de hoogtijdagen van Bitcoin miljarden waard zijn geweest. Het bedrijf vroeg zijn faillissement aan en klanten konden fluiten naar hun geld. Er is dus vooral een eigen verantwoording in de cryptogeld wereld. Er is geen centrale unie die belangen van gebruikers beschermt. Bij fraude is er ook geen mogelijkheid om geld terug te krijgen.

## **Digitalisering van betalingsmogelijkheden**

Tegenwoordig kun je overal ter wereld je betalingen doen en je rekeningen checken via mobiele apps. Ook zijn er nu mogelijkheden om contactloos te betalen in winkels, in Nederland tot een maximaal bedrag van 25 euro. Boven de 25 euro moet je de pincode alsnog invoeren, wat het voordeel van het niet te hoeven intypen van de pincode wegneemt en ook dat van pincode afkijkers. Andere voordelen van deze ontwikkelingen zijn dat we minder tijd kwijt zijn met betalingen en een beter overzicht krijgen over ons financiële leven. Maar er kleven ook zeker nadelen aan.

Zo zouden door de contactloze bankpassen criminelen door middel van gebruik van een contactloze pinautomaat mensen ongewenst betalingen laten doen. Maar deze risico’s worden weerlegt in een reactie van de Minister van Financiën (2016) en de Betaalvereniging Nederland na Kamervragen over de veiligheid van contactloos pinnen[[9]](#footnote-9). Hierin beschrijft de heer Dijsselbloem dat het alleen mogelijk is om aan een contactloos pinapparaat te komen als je ingeschreven staat in de Kamer van Koophandel. Dit verlaagt volgens Dijsselbloem de kans op deze fraude. Er is volgens de Betaal Vereniging Nederland (BVN) nog geen melding gedaan door deze manier van fraude. Bovendien moet de afstand volgens BVN kleiner dan 5 centimeter zijn om de betaling te voltooien. Critici zeggen wel dat via omwegen deze apparaten kunnen worden aangeschaft en het geld via het buitenland in theorie zou kunnen verdwijnen.

### **Mobiel bankieren apps**

De afgelopen jaren hebben veel banken een eigen app gemaakt waarop klanten hun saldo kunnen checken en betalingen vanuit kunnen voltooien. Deze vorm van bankieren valt onder het internetbankieren, de mogelijkheden als je internetbankiert vanaf een PC zijn groter, maar via de app is veel toegankelijker. De beveiliging van internetbankieren is altijd in 2 stappen, terwijl dat bij mobiel bankieren maar 1 stap is. Doordat smartphones vaak geen virusscanners hebben kun je je afvragen of het dus wel veilig is. De Fraudehelpdesk krijgt weinig meldingen over deze apps. Wel wordt ook hier gewaarschuwd voor phising door middel van nepmailtjes. Bij installatie van malicieuze fake-bankapps loop je wel kans om zo slachtoffer te worden van fraude.

Nog nieuwer is het betalen via de mobiele telefoon, zonder gebruik te maken van een pas dus. Dit is bij veel banken al mogelijk, wel kost deze wallet geld om te gebruiken. De meeste banken hanteren een tarief van €0,50 per maand. Deze wallet is dus een betaalde app voor op de mobiel.

### **Aansprakelijkheid internetbankieren**

Bij fraude met betaalmiddelen is het de bank die aansprakelijk kan worden gehouden, zij hebben tenslotte het beste overzicht in het geval van fraude en kunnen dit voorkomen. De banken in Nederland hebben samen met de consumentenbond een paar regels opgesteld om in aanmerking te komen voor vergoeding in gevallen van fraude met internetbankieren. Hieronder wordt verstaan we dat er geen illegale software geïnstalleerd mag zijn, de computer up-to-date moet zijn met de nieuwste systeemversie en de rekening regelmatig gecontroleerd is bij de individu. Bij overtreding van deze eisen door het individu mag de bank een eigen risico geven van 150 euro aan de individu. De individu moet dan dus tot 150 euro van de totale kosten betalen. Als kan worden aangetoond dat de individu nergens een fout heeft gemaakt of te laks is geweest, hoort de bank alle schade te vergoeden. Indien de bank kan aantonen dat de individu een fout heeft gemaakt of te laks is geweest kan het te betalen eigen risico stijgen. In het grootste aantal gevallen is het moeilijk dit te bepalen en wordt er dus een eigen risico betaalt van 150 euro door de individu.

Terugkomend op de deelvraag van dit hoofdstuk namelijk of er een instituut zou moeten komen voor cryptovaluta en wie aansprakelijkheid heeft bij het misgaan van transacties met nieuwe betalingsmogelijkheden. De kans dat er een instituut zal komen is zeer klein tot nihil, omdat dit de onafhankelijkheid van de cryptovaluta zal weghalen en de transactiekosten zou verhogen. Wel zou een instituut voor cryptovaluta zorgen voor meer zekerheid, wat de cryptovaluta dan weer dichterbij een officiële valuta maakt door de ogen van overheden en bedrijven. Bij cryptovaluta wordt de aansprakelijkheid verdeeld over de koper en verkoper zij lopen beide het risico om hun geld te verliezen. Bij valuta die via de banken worden beheert is er wel wetgeving over aansprakelijkheid. De bank wordt gezien als eindverantwoordelijke, maar zij mogen wel regels opstellen waaraan de klanten zich moeten houden. Als niet aan deze regels wordt voldaan hoeft de bank geen vergoeding te betalen aan de klant en zijn de kosten van de fout voor de klant. Behalve als er kan worden aangetoond dat de fout vanuit de bank zelf komt.

# **De conclusie**

Aan het begin van dit werkstuk heb ik een hoofdvraag opgesteld. Die luidde als volgt: Hoe ziet de toekomst van het geld eruit en wat heeft dit voor gevolgen voor consumenten, banken, overheden en hoe zit het met de veiligheid en privacy van het “nieuwe” geld. Door middel van de antwoorden op de deelvragen die gesteld worden in de hoofdstukken kan ik nu tot slot een conclusie vormen.

Terugkomend op dit werkstuk geef ik een korte weerspiegeling van de hoofdstukken. In het eerste hoofdstuk wordt er gesproken of er 100% garantie is op de veiligheid van online gegevens. Door gebruik te maken van cijfers uit onderzoeken kwam ik tot de conclusie dat je deze garantie niet kan geven. Zeker met een toenemende hoeveelheid online gegevens kan dit zeer moeilijk om zijn om overal 100% veiligheidsgarantie op te kunnen geven.

In het tweede hoofdstuk bespraken we de vraag: Zijn de nieuwe valuta van de afgelopen jaren goed te beveiligen en zou dit ervoor kunnen zorgen dat de huidige contante valuta in de toekomst niet meer bestaat? Over de veiligheid van het nieuwe geld kun je zeggen dat het ongeveer hetzelfde is als het nu is met normaal geld. Zo kan het per persoon verschillen hoe goed iemand het heeft beveiligd. Echte problemen met de veiligheid zijn er dus niet te noemen. Om erachter te komen of er een toekomst in zit voor cryptovaluta en dit de ondergang van het huidige geld zou betekenen hebben we een paar voor en nadelen tegen elkaar afgewogen. Hieruit konden we concluderen dat het een belangrijke factor is hoe we zelf ons geld willen zien. Moet dit zeer vrij zijn en anoniem, zoals met cryptovaluta. Of gecontroleerd en stabiel zoals met het huidige geld. Doordat het laatste zorgt voor meer macht voor overheden zullen zij dus vooral tegen cryptovaluta zijn. Ook grondbeginselen van een valide valuta zoals het ten alle tijden kunnen gebruiken ervan worden niet erkend bij cryptovaluta. Kortom de huidige valuta zal de komende tijd blijven bestaan, maar met een bijrol van cryptovaluta.

In het laatste hoofdstuk werd de vraag: Zou er een instituut moeten komen die zorgt voor de cryptovaluta en die transacties controleert of beveiligd en bij wie ligt de verantwoordelijkheid als er iets misgaat met het nieuwe geld en de betalingsmogelijkheden hiervan besproken. Als conclusie op deze vraag kwam ik op een zeer klein tot nihil kans voor een instituut, doordat die de voordelen van cryptovaluta zou ondermijnen. Verder ligt de verantwoordelijkheid bij cryptovaluta bij koper en verkoper, anders dan bij normale valuta waar de bank eindverantwoordelijke is. Soorten betalingsmogelijkheden nemen steeds meer toe in de toekomst en er wordt gestart met het invoeren van nationale cryptovaluta’s.

### **Wat zijn de gevolgen van het digitaliseren van het geld voor consumenten?**

Consumenten zullen in de toekomst veel meer te maken krijgen met het online beheren van hun geld in plaats van de fysieke loonstrookjes en facturen van vroeger. De keuze uit betalingsmogelijkheden neemt voor de consument in de toekomst ook toe. Door bankierapps zal er een beter overzicht zijn over de financiële situatie, wat positief zou kunnen uitwerken voor de consument. Anderzijds kunnen al die verschillende betaalmogelijkheden ervoor zorgen dat de drempel voor een aankoop laag is en de consument dus meer uitgaven gaat doen.

### **Wat zijn de gevolgen van het digitaliseren van het geld voor banken?**

Bij het opkomende nieuwe geld wordt er weinig gesproken over een plek voor de banken. Bij de cryptovaluta zijn er natuurlijk geen banken nodig, dit zou dus betekenen dat de belangrijkheid van de banken zal afnemen in de toekomst. De banken zorgen echter zelf ook voor de digitalisering van het geld door bankierapps en betalingsmogelijkheden te introduceren. Door cryptovaluta hebben de banken er nu wel een tegenstander erbij.

### **Wat zijn de gevolgen van het digitaliseren van het geld voor overheden?**

De banken staan onder toezicht van de overheden en overheden kunnen zo dus invloed uitoefenen op de economie. Met de komst van cryptovaluta wordt dus niet alleen de bank minder belangrijk maar heeft de overheid dus ook minder invloed. Door internetbankieren is de belastinginning voor de overheid wel een stuk makkelijker geworden. Bovendien kan er een hoop papierwerk worden bespaard.

### **Hoe zit het met de veiligheid en privacy van het nieuwe geld?**

Doordat al het nieuwe geld over het internet gaat wordt hier al met scepsis naar gekeken. Eigenlijk zou dit niet hoeven het overgrote deel is namelijk veilig en wordt goed beveiligd. Toch is er altijd de kans dat via eigen nalatigheid er een ander bij je geld kan komen. De veiligheid van het nieuwe geld hangt ook af van de soort nieuw geld zo is een Bitcoin betrouwbaarder dan een klein derderangs cryptovaluta dat via een malicieuze site wordt verhandeld. Over de privacy is er bij het nieuwe geld veel te zeggen, zo is dit vrijwel geheel anoniem en is er dus veel privacy. Aan de andere kant kan deze privacy dan weer worden misbruikt door criminelen of terroristen bij de financiering van hun daden. Het heeft dus zijn voor en nadelen.

### **Hoe ziet de toekomst van ons geld eruit?**

In de toekomst zal een groot deel van ons geld worden beheerd en uitgegeven door middel van het internet en zal de hoeveelheid chartaal geld flink zijn gedaald. Contactloos zal er worden afgerekend voor de boodschappen of andere aankopen. Verder zal de cryptovaluta op veel plekken worden geaccepteerd als officieel ruilmiddel. Banken zullen minder belangrijk zijn en de mensen kunnen hun geld opbergen in speciale wallets, als ze geen vertrouwen hebben in de banken. Overheden zullen zich meer gaan bemoeien met de cryptovaluta, omdat deze een gevaar kunnen vormen voor de normale valuta. Een andere mogelijkheid voor overheden is toegeven aan de cryptovaluta en beginnen met het testen van eigen beheerde cryptovaluta’s. In diverse landen staan deze testen al op de agenda.

Doordat alles meer digitaal wordt met betrekking tot geld zal de beveiliging en veiligheid hiervan ook mee moeten groeien. De systemen moeten immuun worden voor aanvallen om zo de vraag naar geld altijd te kunnen beantwoorden. Veel geld zal daarom worden geïnvesteerd in de digitale infrastructuur om die zo te verbeteren en hierdoor de wereld klaar te maken voor een nieuwe fase in het bestaan van geld.

# Literatuuropgave

**Hoofdstuk 1**

* CBS. (2018). *Cybersecuritymotor 2018*. Gedownload op <https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018>
* Dutchcowboys, & Slobbe, J. (2018, 6 maart). Veelvoorkomende vragen over cybersecurity beantwoord door experts. Geraadpleegd op 23 september 2018, van <https://www.dutchcowboys.nl/cybercrime/veelvoorkomende-vragen-over-cybersecurity-beantwoord-door-experts>
* Hijink, M. (2017, 1 november). NRC checkt: ‘Misdaad gaat omlaag, behalve cybercrime’. Geraadpleegd op 28 september 2018, van <https://www.nrc.nl/nieuws/2017/11/02/misdaad-gaat-omlaag-behalve-cybercrime-13791268-a1579594>
* Security.nl. (2018, 18 september). Kabinet investeert miljoenen extra in bestrijding cybercrime. Geraadpleegd op 7 oktober 2018, van <https://www.security.nl/posting/577545/Kabinet+investeert+miljoenen+extra+in+bestrijding+cybercrime>

**Hoofdstuk 2**

* Centraal Planbureau. (2018). *CPB Risicorapportage Financiele Markten 2018 Cryptovaluta*. Gedownload op <https://www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-29mei2018-Risicorapportage-financiele-markten-2018-2e-deel.pdf>
* Cryptocurrency facts. (z.d.). Cryptocurrency Pros and Cons. Geraadpleegd van <https://cryptocurrencyfacts.com/cryptocurrency-pros-and-cons/>
* Digiconomist. (z.d.). Bitcoin Energy Consumption Index - Digiconomist. Geraadpleegd op 17 januari 2019, van <https://digiconomist.net/bitcoin-energy-consumption>
* Guido (2018, 15 maart). Wat is mining? Geraadpleegd op 20 november 2018, van <https://cryptocoinkoers.nl/faq/wat-is-mining/>
* Hoekstra, W. B. (2018). Kamerbrief over de ontwikkelingen rondom cryptovaluta. Geraadpleegd van <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/03/08/kamerbrief-over-de-ontwikkelingen-rondom-cryptovaluta/kamerbrief-over-de-ontwikkelingen-rondom-cryptovaluta.pdf>
* Janikowski, L., & Dabrowski, M. (2018). *Virtual currencies and central banks monetary policy: challenges ahead* (PE 619.009). Geraadpleegd van <http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf>
* The Economist. (z.d.). Safe Cities 2017. Geraadpleegd op 2 december 2018, van <http://safecities.economist.com/qa-just-how-secure-are-cryptocurrencies>+

**Hoofdstuk 3**

* Dijsselbloem, J. (2016, 4 maart). De mogelijke veiligheidsrisico's van pinpassen waarmee contactloos betaald kan worden [Kamerstuk]. Gedownload op 27 november 2018, van kamerbrief-beantwoorden-vragen-over-veiligheidsrisico-s-pinpassen-bij-contactloos-betalen
* Engelfriet, A. (2013, 4 december). Juridische vraag: wie is aansprakelijk voor fraude met internetbankieren? Geraadpleegd op 17 januari 2019, van <https://www.security.nl/posting/371573/Juridische+vraag%3A+wie+is+aansprakelijk+voor+fraude+met+internetbankieren%3F>+

* O'Neal, S. (2018, 17 november). Latest Bitcoin, Blockchain and Ethereum news. Geraadpleegd op 17 januari 2019, van <https://cointelegraph.com/news/cryptoruble-how-stable-could-russian-national-stablecoin-be>
* Magas, J. (2018, 29 juni). Six Tools Used by Hackers to Steal Cryptocurrency: How to Protect Wallets. Geraadpleegd op 17 januari 2019, van <https://cointelegraph.com/news/six-tools-used-by-hackers-to-steal-cryptocurrency-how-to-protect-wallets>
* Zuurmond, I. (2018, 23 oktober). Mobiel bankieren. Geraadpleegd op 17 januari 2019, van <https://www.consumentenbond.nl/betaalrekening/mobiel-bankieren>
* Zuurmond, I. (2018b, 23 oktober). Mobiel en contactloos betalen. Geraadpleegd op 17 januari 2019, van <https://www.consumentenbond.nl/betaalrekening/mobiel-en-contactloos-betalen>

# Bijlagen

* **Cybersecuritymonitor 2018**



* **Risicorapportage Financiële markten 2018**



* **Kamerbrief Dijselbloem**

# Begrippenlijst

**Hoofdstuk 1**

Cybercrime: Een delict (strafbaar feit) dat wordt gepleegd met behulp van ICT.

Ransomware: Ransomware is een chantagemethode op internet door middel van malware. Deze malware blokkeert/gijzelt een computer (of bestanden) en vraagt geld voor teruggave.

Dataleaks/Data breach: Het opzettelijk of onopzettelijk vrijgeven van beveiligde informatie.

Cybersecurity: Het beveiligen van computers, netwerken en programma’s tegen vormen van cybercriminaliteit.

Internet of things: Het verbinden tussen apparaten onderling om gegevens te kunnen uitwisselen.

Phishing: Vorm van internetfraude waarbij het slachtoffer naar een valse webpagina wordt gelokt, gebeurt meestal via e-mails.

**Hoofdstuk 2**

Cryptomining: Een proces waar transacties voor cryptovaluta’s worden geverifieerd en toegevoegd aan het blockchain systeem.

Cryptovaluta wallets: Een software programma waar sleutels in worden opgeslagen. Hierdoor kun je cryptovaluta verzenden en ontvangen.

**Hoofdstuk 3**

CryptoRuble: De mogelijke toekomstige nationale cryptovaluta van Rusland.

# **Nawoord**

Na het schrijven van dit profielwerkstuk kan ik terugkijken op een leerzaam proces. Aan het begin zocht ik een voor mij interessant onderwerp en ik kan stellen dat de digitalisering van geld mij vanaf het begin tot het eind heeft geboeid. Ik hoop dat ik met mijn opgedane kennis door dit profielwerkstuk ook een bredere voorkennis heb voor een studie. Op dit moment ben ik aan het kijken naar de studie Security Studies aan de Universiteit Leiden. Het programma van de studie toont raakvlakken met mijn profielwerkstuk. Tot slot vond ik het dus leerzaam en interessant om te doen en vond ik het leuk om aan te werken.

1. Bron: Cybersecuritymonitor 2018, Hoofstuk 5. Cybercrime [↑](#footnote-ref-1)
2. Bron: Cybersecuritymonitor 2018, Hoofstuk 4. Cybersecurity, Incidenten [↑](#footnote-ref-2)
3. Bron: Gartner 2016-2018, Statista.com [↑](#footnote-ref-3)
4. Bron: Gartner, Statista.com [↑](#footnote-ref-4)
5. Bron: Begroting ministerie van Justitie en Veiligheid, periode 2018-2019 [↑](#footnote-ref-5)
6. Bron: Cybersecuritymonitor 2018, Hoofstuk 3. Cybersecurity, Maatregelen [↑](#footnote-ref-6)
7. Hoekstra, W. B. (2018). Kamerbrief over de ontwikkelingen rondom cryptovaluta. [↑](#footnote-ref-7)
8. Janikowski, L., & Dabrowski, M. (2018). Virtual currencies and central banks monetary policy: challenges ahead [↑](#footnote-ref-8)
9. Dijsselbloem, J. (2016, 4 maart). De mogelijke veiligheidsrisico's van pinpassen waarmee contactloos betaald kan worden [Kamerstuk]. [↑](#footnote-ref-9)