Cryptovaluta: revolutie of *fake news*?

24 januari 2018

Teunis Brosens
ING Economisch Bureau

Inhoudsopgave

Overleven in een “Mad Max”-wereld: transacties doen met onbekenden, zonder vertrouwde tussenpersoon, zonder autoriteiten. De innovatieve blockchain-oplossing

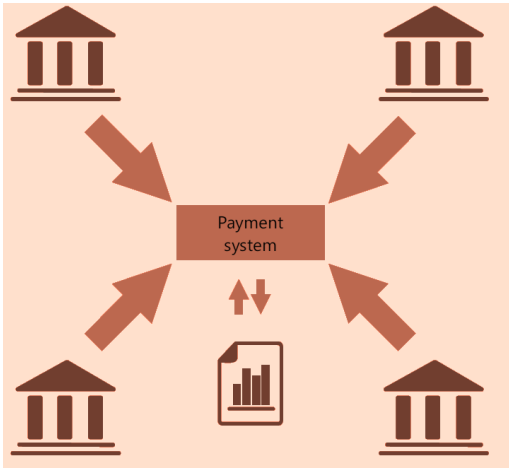
Drie stellingen rond cryptovaluta:

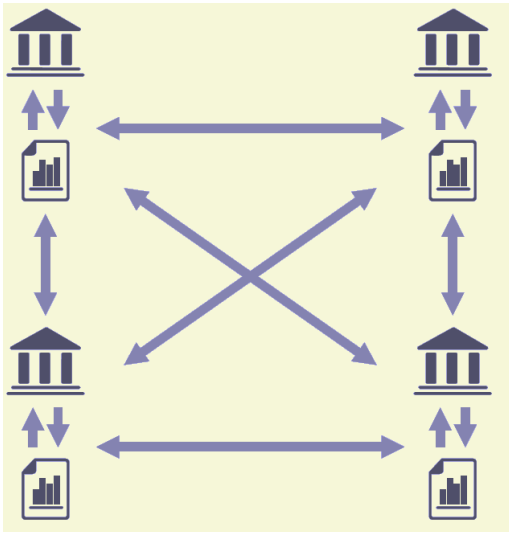
- Cryptogeld is veel minder decentraal dan vaak gedacht
- Ook in cryptogeld is een belangrijke rol voor tussenpersonen weggelegd
- Cryptogeld in huidige vorm is als betaalmiddel nog niet levensvatbaar

Conclusie: cryptogeld is nog onvolwassen, maar de ontwikkelingen gaan snel

Appendix: een introductie in crypto-terminologie

De belangrijkste belofte: weg met de tussenpersoon





Bij veel transacties wordt traditioneel gebruik gemaakt van een **centrale partij** die een database bijhoudt van transacties en tegoeden.
Voorbeelden:

- Banken houden tegoeden bij van hun rekeninghouders
- Centrale banken houden tegoeden bij van banken
- Het Kadaster houdt eigendom en transacties van huizen bij

Met blockchain-technologie kan deze centrale partij geschrapt worden. In plaats daarvan hebben **alle partijen een kopie van de database** in hun bezit. Het blockchain-protocol zorgt dat deze kopieën identiek blijven.
Ook moet in het netwerk **consensus** bereikt worden over welke mutaties geldig zijn, en welke niet.

In de context van cryptogeld-blockchains is meestal **onbekend wie de tegenpartij is**. In een gecentraliseerde setting vertrouwen we op de centrale partij om voor ons de transactie goed af te handelen.
In decentrale setting zijn we allemaal “**Mad Max**”, zonder overheid of politie om ons te beschermen.

Het “Mad Max-probleem” van blockchain: zonder centrale autoriteit valt geen enkele tegenpartij te vertrouwen…

- Is deze persoon wel wie hij zegt dat hij is?
- En is het geld dat hij me wil geven, wel echt?

De oplossing van Satoshi Nakamoto (Bitcoin)…

- Bewijs de authenticiteit van berichten en afzender met cryptografie
- Voorkom fraude met een openbare, door iedereen gemakkelijk raad te plegen historie van alle transacties

“Miners” voegen nieuwe transacties toe aan deze openbare historische database

- Genereren van nieuwe blokken kost moeite. Dat maakt fraude moeilijk

Waarom is minen aantrekkelijk, als dat zoveel moeite (elektriciteit) kost?

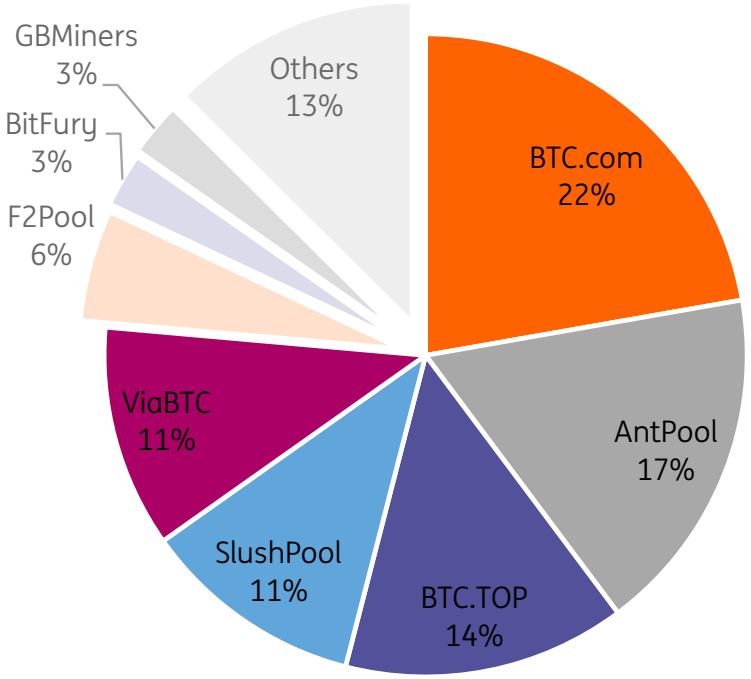
- Beloning met verse bitcoins (*block reward*) én de door gebruikers betaalde transactiekosten

Governance

De Bitcoin-programmacode voert de regels uit. Deze programmacode is openbaar, iedereen kan eraan bijdragen en de code controleren

Decentraal cryptogeld? Machtige miners

Verdeling computerkracht bitcoin-netwerk
Hash rate, laatste 4 dagen



5 coöperaties controleren >75% van netwerk.
3 coöperaties controleren >50%.
Bron: blockchain.info

Een belangrijke belofte van Bitcoin en ander cryptogeld is: "**weg met tussenpersonen en centrale partijen**".

En inderdaad draait de Bitcoin-blockchain al sinds 2009 zonder bedrijf of overheid erachter, zonder *downtime* en zonder gehackt te zijn. Dat is **zondermeer indrukwekkend**!

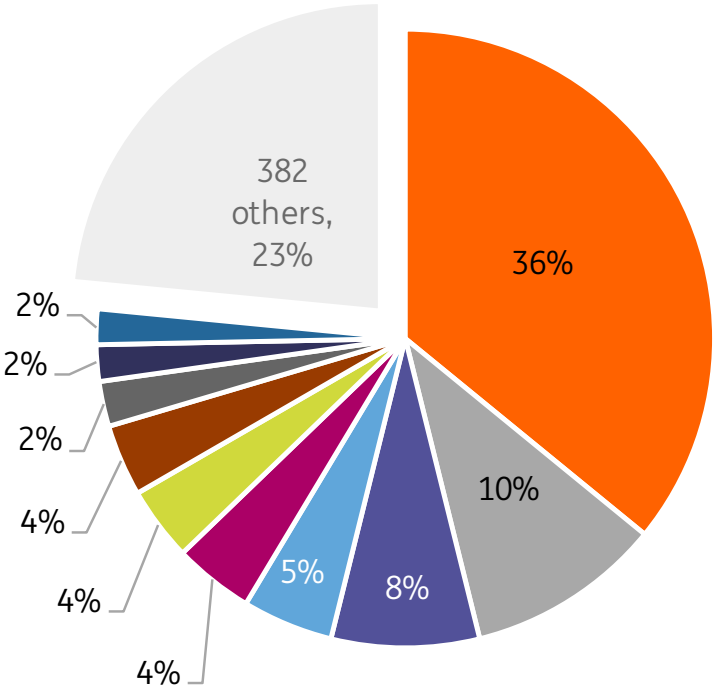
Toch zijn cryptogeld-blockchains vaak **veel meer gecentraliseerd dan gedacht**.

Ten eerste, de ***miners*** die blokken toevoegen aan de ketting. Zij kunnen zaken afdwingen of tegenhouden, door alleen blokken met bepaalde kenmerken te accepteren of andere te weigeren.

Bij Bitcoin (en de meeste cryptovaluta's) kan iedereen *minen*. We zien echter dat *miners* zich verenigen in *pools* (om meer kans te maken af en toe een blok te minen). In de praktijk hebben de **drie grootste *mining pools*** al geruime tijd **meer dan 50%** van (de computerkracht in) het Bitcoin-netwerk in handen. Dat geeft ze een **belangrijke machtsbasis**.

Decentraal cryptogeld? Prominente programmeurs

Programmeurs bitcoin broncode
% van alle updates



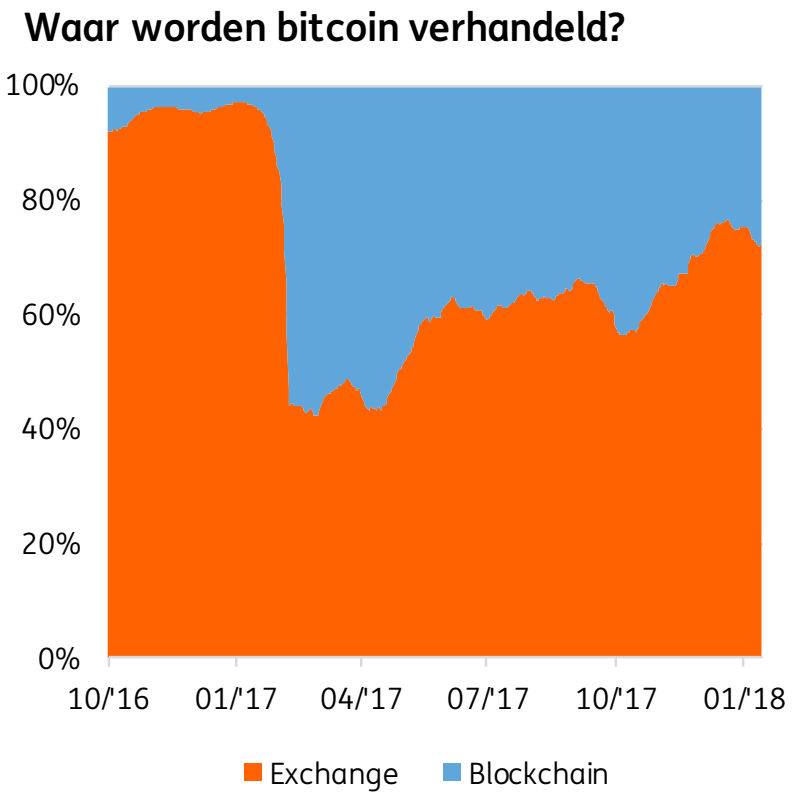
Iedereen kan updates voorstellen, maar alleen **drie beheerders** van "Bitcoin core" kunnen broncode wijzigen.
Bron: bitcoin.org, bitcoincore.org

Een andere **belangrijke machtsbasis** is de **ontwikkeling van de programmacode** (bijvoorbeeld van Bitcoin Core, de leidende Bitcoin client software). De meeste crypto-programmacode is openbaar, en iedereen kan eraan bijdragen. Zo bezien is de *governance* van cryptovaluta gedecentraliseerd.

Maar in de praktijk is de **kern van programmeurs veelal klein**. Bij Bitcoin zijn er 10 programmeurs die meer dan 75% van alle wijzigingen in de code voor hun rekening nemen (zie grafiek). Bovendien zijn er slechts drie beheerders die wijzigingen aan de broncode autoriseren.

De concentratie onder zowel miners als programmeurs speelt bij Bitcoin, maar ook bij andere munten. **Decentraal** betekent bij cryptovaluta dus vooral dat **minder zichtbaar is waar de feitelijke macht berust**. Dit is niet per se slecht, maar wel onderbelicht.

De tussenpersoon: terug van nooit weggeweest



30daags voortschrijdend gemiddelde. Bron: ING o.b.v. data.bitcoinity.org. Exclusief (o.a.) Koreaanse beurzen

Het oorspronkelijke doel van Bitcoin (en veel ander cryptogeld) is om te kunnen betalen zonder tussenpersonen. Satoshi Nakamoto's white paper:

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main

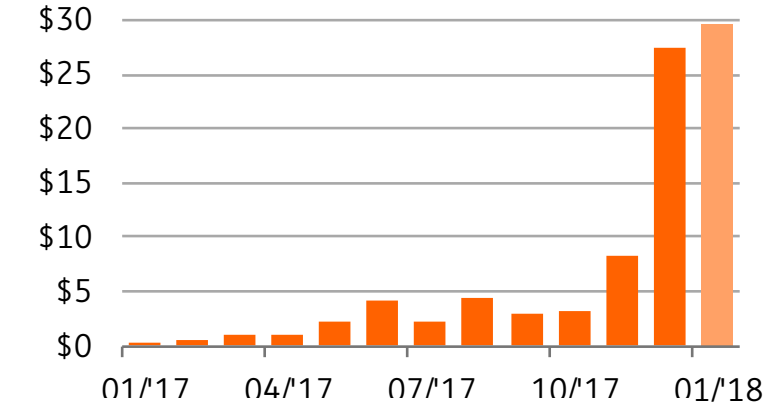
In de praktijk echter wordt in de cryptogeld-gemeenschap net zo goed als in het traditionele financiële verkeer, gebruik gemaakt van tussenpersonen, zoals aanbieders van **cryptogeld-portemonnees** en **beurzen**. Op dit moment vindt **70% van de Bitcoin-handel niet direct op de blockchain, maar via beurzen** plaats.

De grootste vier beurzen (Bitfinex, Coinbase, Bitflyer en Bitstamp) nemen gezamenlijk 75% van de beurstransacties voor hun rekening.

Kortom: hoewel decentraal in opzet, zijn er in cryptogeld in de praktijk **net zo goed "centrale" partijen actief** met een belangrijk marktaandeel. Dat maakt cryptovaluta in de praktijk een stuk traditioneler dan in theorie gedacht.

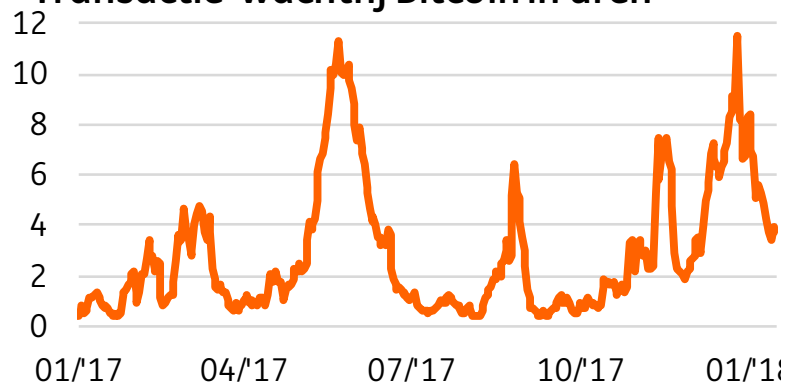
Cryptovaluta als betaal-middel: kinderziektes

Gemiddelde transactiekosten Bitcoin



Bron: charts.bitcoin.com

Transactie-wachtrij Bitcoin in uren



Dagelijks gemiddelde. Bron: ING o.b.v. blockchain.info

Het oorspronkelijke doel van Bitcoin was een **decentraal betalingssysteem** te creëren. Maar hier loopt Bitcoin op dit moment tegen **beperkingen** aan: door de **beperkte capaciteit** van het Bitcoin-netwerk ontstaan achterstanden. Het aantal transacties wachtend op bevestiging loopt de laatste maanden regelmatig op tot boven de 100.000, omgerekend een **wachttijd van meerdere uren**. Om een transactie snel bevestigd te krijgen moeten **hoge transactiekosten** betaald worden; in december (gemiddeld) $27.

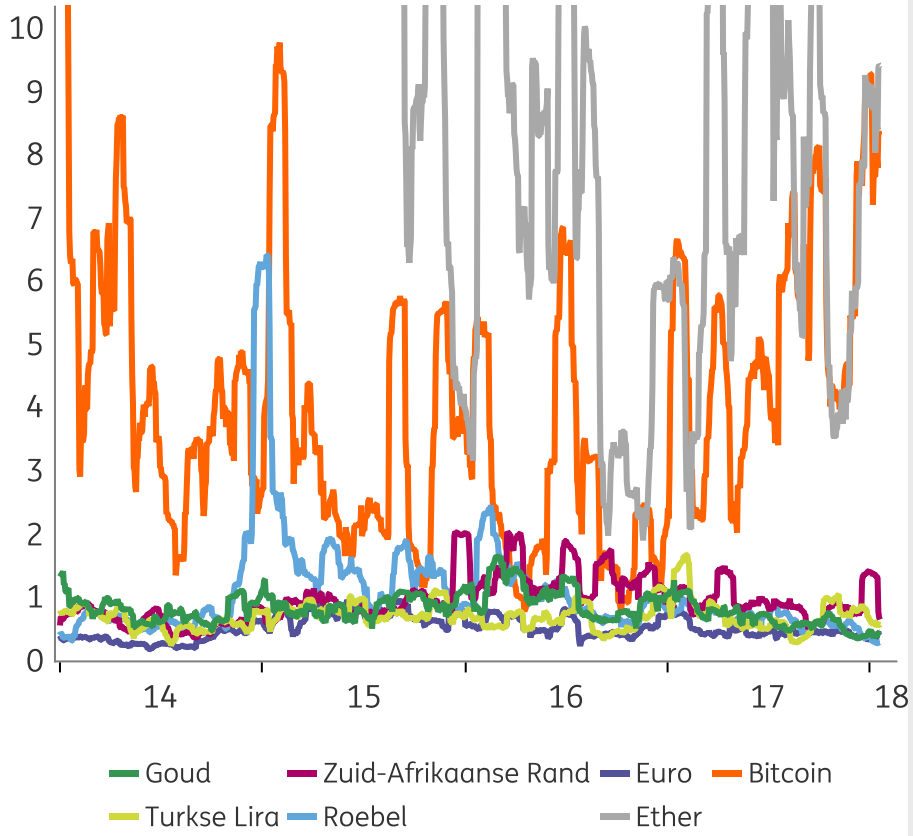
Ter relativering: transacties worden vaak op **interne beursplatformen** afgewikkeld (zie vorige pagina) en hoeven dan **geen last** te hebben van blockchain-congestie. Ook steekt een wachttijd van enkele uren nog gunstig af tegen traditionele internationale overboekingen.

De problemen zorgen in cryptoland voor een **richtingenstrijd**. Bij Bitcoin lijkt de betalingsdoelstelling overboord gezet ten gunste van een status als “**digitaal goud**”. Bitcoin Cash is in augustus 2017 afgesplitst van Bitcoin en beoogt wel (weer) een betalingsmunt te worden.

Cryptovaluta als geld: vooralsnog erg volatiel

Volatiliteit van valuta en goud tegenover dollar

Standaarddeviatie van dagelijkse %-veranderingen,voortschrijdend 1maands gemiddelde (alleen handelsdagen)



De meeste cryptovaluta's hebben te maken met een **hoge volatiliteit**.

De koers- (en daarmee prijs-) bewegingen van cryptovaluta zijn groter dan bijvoorbeeld die van de Russische Roebel en van goud.

Deze volatiliteit maakt cryptovaluta **als geld vooralsnog ongeschikt**. Het is ondoenlijk om de prijs van een cappuccino in cryptovaluta uit te drukken; de prijs zou iedere vijf minuten moeten worden aangepast.

Naarmate de acceptatie van cryptovaluta toeneemt, zou de volatiliteit wel moeten afnemen.

Maar het **inflexibele aanbod** blijft een **fundamenteel probleem**. Er is geen centrale bank die met monetair beleid kan sturen.

Een ander probleem voor cryptovaluta als betaalmiddel is het feit dat er **honderden varianten** zijn. Het ligt voor de hand dat de meeste hiervan op termijn zullen verdwijnen.

Conclusie:
Wat niet is, kan nog komen

De sceptische conclusies

- Huidige generatie cryptovaluta is onvolwassen (o.a. schaalbaarheid, energieverbruik, volatiliteit, *governance*).
- Tot nu toe zijn er twee bewezen *use cases*: i) criminaliteit en ii) speculatie.
- Er blijft behoefte aan tussenpersoon-dienstverlening.

De positieve conclusies

- De blockchain-belofte (in een decentrale context, zonder vertrouwen, op een veilige manier handelen) wordt waargemaakt.
- Cryptovaluta en blockchain doorlopen, wat betreft innovatie, *governance* en regulering, in 20 jaar waar traditionele financiële markten 200 jaar over gedaan hebben.
- *Initial Coin Offerings* kunnen nuttig aanvullend financieringsinstrument zijn.

- De **problemen** waar bitcoin en andere cryptovaluta tegenaan lopen zijn veelal **praktisch van aard**. Ze kunnen dus worden opgelost.

- De **ontwikkelingen** van blockchain en cryptovaluta **gaan erg snel**. Voor een aantal praktische beperkingen van bitcoin (bijvoorbeeld schaalbaarheid, energieverbruik) wordt druk geëxperimenteerd met oplossingen die toepasbaar zijn voor bitcoin of andere cryptovaluta's.

- Op het gebied van ***governance*** zijn er **veel smaken** cryptovaluta beschikbaar; van volledig decentraal tot door bedrijven geleid.

- De in cryptovaluta actieve **tussenpersonen** (beurzen, wallet providers) vormen een **divers gezelschap**. Tegenover bedrijven met een twijfelachtig imago (waartegen in toenemende mate wordt opgetreden) staan bedrijven die juist aan de *best practices* op het terrein van zorgplicht en klant-identificatie willen voldoen.

ING

Appendix:
Kan het minder cryptisch?

- Een **blockchain** is niet meer, niet minder dan **een soort database**. Het belangrijkste voordeel is dat **consensus** over de in de database vastgelegde feiten, **decentraal bereikt** kan worden. Dus zonder (centrale) bank of overheid, en zonder dat men elkaar kent of vertrouwt.
- De database bevat een **transactiehistorie** van “tokens”. Deze tokens kunnen in principe van alles representeren.
- Als de token “geld” representeert, hebben we het over een **cryptovaluta**.

- Er zijn honderden cryptovaluta’s, elk met eigen focus.
- Ook zijn er enkele cryptovaluta’s die niet op een blockchain werken, maar op basis van andere technologie (bijvoorbeeld “Iota”).
- En ten slotte wordt o.a. door banken druk **geëxperimenteerd met blockchain-technologie**, waarbij de tokens iets anders representeren dan cryptovaluta.

Terminologie

- **Bitcoin** = De bekendste cryptovaluta
- **Cryptovaluta** = (wannabe) geld, gebaseerd op blockchain-technologie
- **Token** = een eigendomsbewijs op een blockchain. Dit kan geld zijn, een aandeel, een ID of iets anders
- **Blockchain** = een type database
- **Distributed Ledger Technology** = een database “verdeeld” over verschillende servers. Voorbeeld: de bitcoin blockchain

- **Public blockchain** = Openbaar toegankelijk, iedereen kan meedoen
- **Permissioned blockchain** = Een blockchain waarbij een instantie (bedrijf, overheid) de toegang controleert. Banken experimenteren hoofdzakelijk met deze permissioned chains.

Disclaimer

Data from Macrobond, unless otherwise noted.

This publication has been prepared by ING (being the commercial banking business of ING Bank N.V. and certain subsidiary companies) solely for information purposes. It is not investment advice or an offer or solicitation to purchase or sell any financial instrument. Reasonable care has been taken to ensure that this publication is not untrue or misleading when published, but ING does not represent that it is accurate or complete. The information contained herein is subject to change without notice. ING does not accept any liability for any direct, indirect or consequential loss arising from any use of this publication. This publication is not intended as advice as to the appropriateness, or not, of taking any particular action. The distribution of this publication may be restricted by law or regulation in different jurisdictions and persons into whose possession this publication comes should inform themselves about, and observe, such restrictions. Copyright and database rights protection exists in this publication. All rights are reserved.

ING Bank N.V. is incorporated with limited liability in the Netherlands and is authorised by the Dutch Central Bank.

United States: Any person wishing to discuss this report or effect transactions in any security discussed herein should contact ING Financial Markets LLC, which is a member of the NYSE, FINRA and SIPC and part of ING, and which has accepted responsibility for the distribution of this report in the United States under applicable requirements.