BLOCKCHAIN
EEN INTRODUCTIE
11 JANUARI 2021

Karl Moens

Blockchain
Introductie

- Wat is een “blockchain”?
- Welk probleem trachten we op te lossen?
- Hoe werkt het?
- Wat kunnen we er mee doen?
- Blockchain en Verzekeringen.
- Conclusie

Blockchain
Introductie

Ik ben opgeleid als jurist.

Ik was advocaat gedurende 15 jaar.

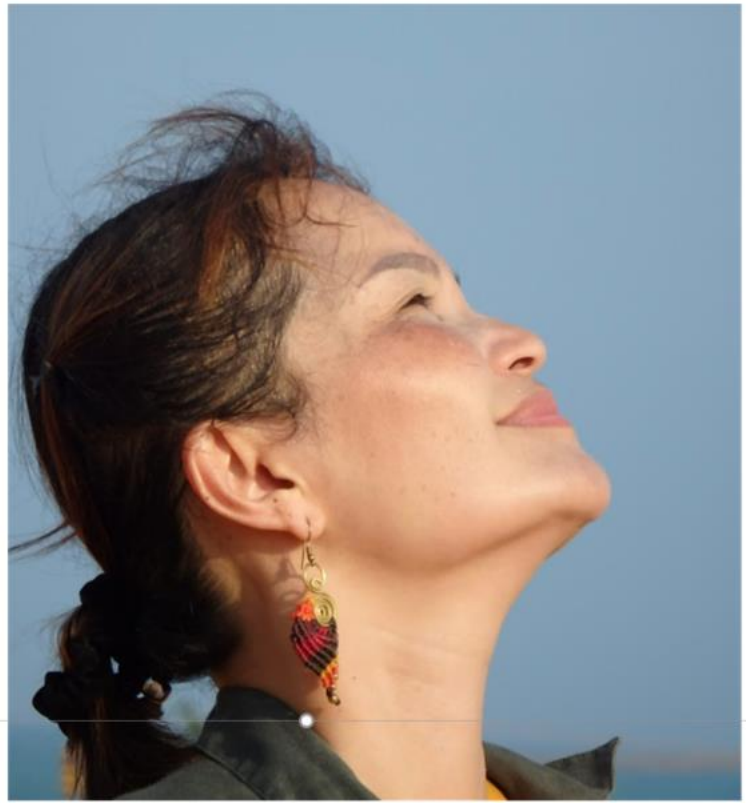
En ik werk sinds 1998 als een verzekeringsmakelaar.

Ik ben geen programmeur, noch een IT specialist.

Dus mijn leven is héééééél saai …

Ware het niet voor de volgende twee zaken:

1. Mijn Thaise vriendin



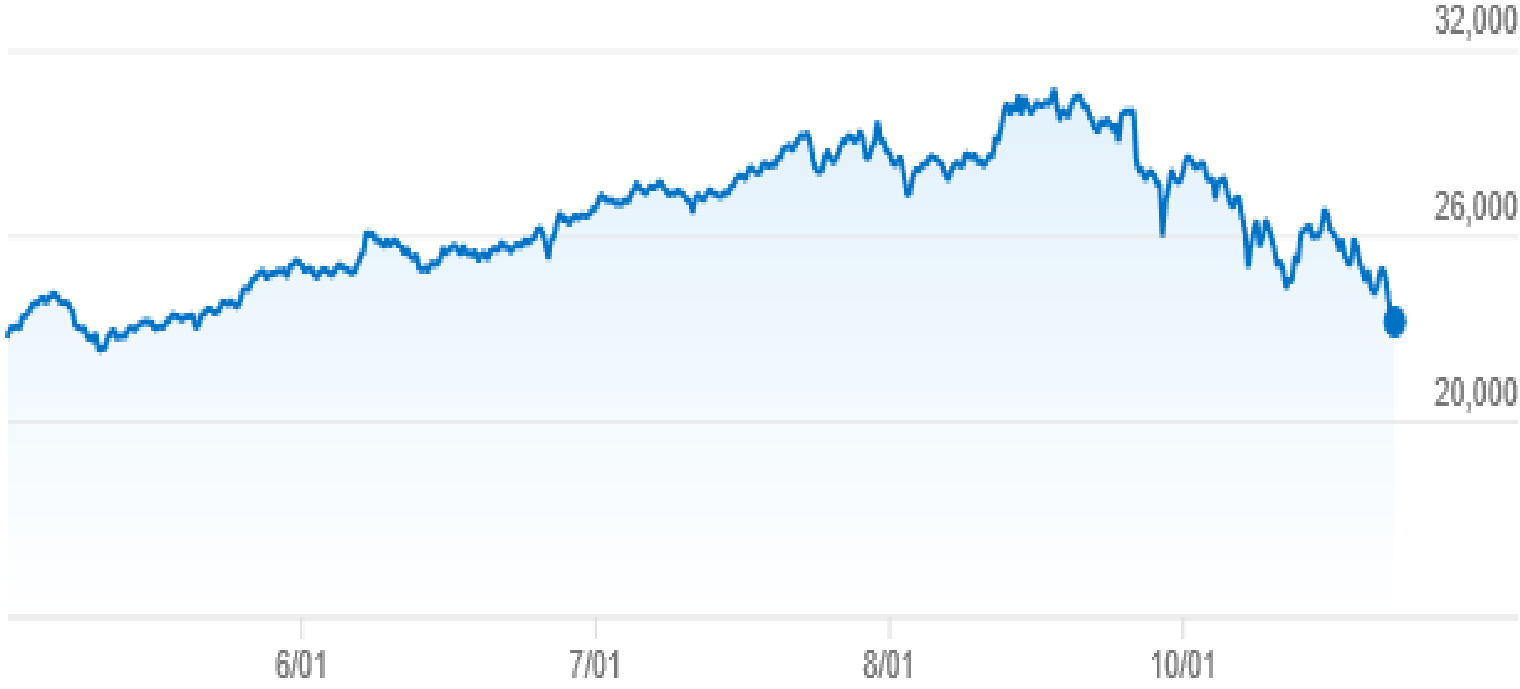
Blockchain
Introductie

2. De computerclub die ik zoveel jaren geleden mee heb opgericht:

Blockchain
Introductie

We gaan het niet over Bitcoin hebben!

Maar omdat jullie allemaal nieuwsgierig zijn over de prijs van een bitcoin:



De totale waarde van alle bitcoins is nu ongeveer 550 miljard USD. Men schat dat 20% daarvan “verloren” is omdat de houders hun paswoord zijn vergeten.

Blockchain
Blockchain in twee minuten

https://www.iftf.org/future-now/article-detail/understand-the-blockchain-in-two-minutes/

Blockchain
Blockchain in twee minuten

Interessant, maar niet erg informatief.

Niettemin, we leerden dat “blockchain”:

- Software is
- Die “records” in een chronologische keten van blokken beheert
- Gecontroleerd door een netwerk zonder centrale autoriteit
- En waar niemand kan valsspelen omdat iedereen toekijkt.

Voor een meer technische uitleg van Blockchain:

https://youtu.be/bBC-nXj3Ng4

De originele bitcoin-blockchain paper (31-10-2008) van Satoshi Nakamoto:

https://bitcoin.org/bitcoin.pdf

Het idee van een blockchain gaat terug tot 2004.

Blockchain
Definitie

Misschien dat de officiële definitie van “blockchain” ons verder helpt:

Een blockchain is een groeiende lijst van vermeldingen (records), “blokken” genoemd, die d.m.v. cryptografie met elkaar zijn verbonden. Ieder blok bevat een cryptografische “hash” van (tenminste), het vorige blok, een datum-tijd-stempel, en de eigen transactionele gegevens.

Het wordt geïmplementeerd als een open, verdeeld grootboek van transacties, simultaan bijgehouden op meerdere computers. Dit verdeelde grootboek kan transacties tussen partijen opnemen op een efficiënte, controleerbare, vertrouwde en duurzame wijze.

Informatief, maar niet erg interessant.

Blockchain
Definitie

Nu weten we dat:

Een blockchain

- Transacties registreert
- In steeds aangroeiende keten van blokken;
- En elk blok omvat het vorige blok;
- Alles wordt bijgehouden in een verdeeld open grootboek;
- Het genereert vertrouwen (door verificatie en duurzaamheid van de transacties) tussen partijen die elkaar niet noodzakelijk moeten vertrouwen;
- Op een efficiënte wijze.

Blockchain
Wat probleem trachten we op te lossen?

Het probleem is “Vertrouwen”.

- Wie kunnen we vertrouwen?
- Wie garandeert ons vertrouwen?
- Wie dwingt ons vertrouwen af?
- Wat kunnen we vertrouwen?
- Hoe weten we wanneer we worden bedrogen?
- …

Hoe kan een blockchain deze problemen oplossen?

Blockchain
Er was eens, lang, lang geleden … (vóór computers en blockchain)

Een huis waar 4 vrienden (An, Bert, Cindy en Dirk) samen woonden. Ze besloten elk bij te dragen in de kosten, maar niet elke transactie onmiddellijk te vereffenen.

Kosten en betalingen worden opgenomen in een grootboek, bijgehouden door An.

- An betaalt de huur van het huis: 100
- Bert koopt etenswaren: 40
- Cindy betaalt haar deel van de huur reeds aan An: 25
- Dirk leent An 50

Op het einde van de week, sluit An de rekeningen en berekent ze dat:

- An aan Dirk 25 betaalt; Dirk 10 moet aan Bert; Cindy Bert 10 geeft en Bert 15 betaalt aan An; of (meer efficient)
- An 15 betaalt aan Dirk; Bert en Cindy elk 5 betalen aan An

Blockchain
Er was eens, lang, lang geleden … (voor computers en blockchain)

In theorie werkt dit perfect, maar er zijn wat practische problemen:

1. Wat indien diegene die schulden hebben niet betalen?
2. An doet al het werk (gratis).
3. Iedereen vertrouwt An, maar wat als ze een fout maakt of bedrog pleegt?
4. Alleen An kent alle transacties.

Oplossingen:

1. Iedereen betaalt een voorschot en An weigert transacties die een individueel voorschot overschrijden (niemand gaat “in het rood”)
2. An wordt betaald voor haar werk.
3. Iemand controleert het werk van An. (Maar wie controleert de controleur?)
4. Voer een open boekhouding.

Blockchain
Er was eens, lang, lang geleden … (voor computers en blockchain)

Een open boekhouding lost alleen probleem 4 op.

Maar als iedereen zelf een grootboek bijhoudt, worden problemen 2 en 3 ook opgelost.

- Iedereen doet hetzelfde werk, dus niemand moet worden betaald.
- Indien iemand een fout maakt of bedrog pleegt, is zijn grootboek afwijkend.
  - Welk grootboek vertrouwen we?
    - De meerderheid wint!
  - Garandeert dit absolute zekerheid en juistheid?
    - Neen, maar er is een meerderheid nodig om een minderheid te bedriegen.
    - Hoe meer deelnemers, hoe moeilijker om bedrog te plegen.

Een open, verdeeld grootboek is eenvoudiger te vertrouwen zelfs als er geen vertrouwen is tussen de deelnemers.

Blockchain
Van open, verdeeld grootboek naar blockchain

(Al deze stappen worden uiteraard in software uitgevoerd)

- Alle deelnemers “luisteren” naar berichten die door andere deelnemers worden uitgezonden. De berichten worden voorzien van een digitale handtekening die de identiteit van de verzender en de integriteit van de inhoud garandeert.
- Alle berichten bevatten een datum-tijd-stempel en zijn uniek. Duplicaat berichten worden genegeerd!
- Elke deelnemer die een bericht ontvangt, checkt:
  - De digitale handtekening.
  - Duplicaat bericht?
  - Geldigheid overeenkomstig de afspraken over de transacties.

  Enkel een geldig bericht wordt opgenomen in het grootboek v/d ontvanger.

Deze procedure garandeert dat alle grootboeken correct en “in sync” zijn.

Maar enkel indien iedereen alle berichten altijd correct heeft ontvangen!

Blockchain
Van open, verdeeld grootboek naar blockchain

Waarom is het een probleem indien iemand een bericht heeft gemist?

- Zijn grootboek is niet meer gesynchroniseerd en is dus fout.
- Hij moet alle deelnemers naar hun versie van het grootboek vragen en een “meerderheidsversie” vinden die hij dan kan overnemen.

Maar misschien weet hij zelfs niet dat hij een bericht gemist heeft.

- Dus iedereen moet voortdurend aan iedereen vragen wat hun versie van het grootboek bevat en iedereen moet voortdurend de meerderheidsversie vaststellen. Ondertussen komen er nieuwe berichten bij, zodat misschien nooit een meerderheidsversie kan worden gevonden.
- Blockchain technologie lost dit probleem op.

Blockchain
Van open, verdeeld grootboek naar blockchain

- Deelnemers luisteren naar transacties en verzamelen die in een blok

Header
Transactie 1 (digitaal ondertekend, uniek, geldig)
Transactie 2 (digitaal ondertekend, uniek, geldig)
Transactie 3 (digitaal ondertekend, uniek, geldig)

- De deelnemer berekent de cryptografische hash van het blok en voegt die toe aan het einde van het blok.

Header
Transactie 1 (digitaal ondertekend, uniek, geldig)
Transactie 2 (digitaal ondertekend, uniek, geldig)
Transactie 3 (digitaal ondertekend, uniek, geldig)
01110101110000010101010111001110100 01

Blockchain
Cryptografische Hash

Een cryptografische hash functie is een hash functie die gebruikt kan worden bij cryptografie. Het is een wiskundig algoritme dat data van arbitraire lengte (het “bericht”) omzet in een sequentie van bits met een vaste lengte (“hash” of “message digest”). Het is een één-richtings functie, m.a.w. het is praktisch onmogelijk om de functie te inverteren.

“Lang bericht …” -> “1101001”

“Een ander bericht …” -> “0111001”

- Dezelfde berichten genereren eenzelfde hash. (Het is geen UUID!)
- Het hash-algoritme werkt heel snel.
- Het is praktisch onmogelijk om een bericht te genereren dat bij een bepaalde hash hoort (enkel d.m.v. “brute kracht” kan dit):

  “1101100” is de hash van “??????????”
- Elke wijziging in het bericht veroorzaakt onvoorspelbare wijzigingen in de hash

Blockchain
Cryptografische Hash

De cryptografische hash functie “SHA-256” (“Secure Hashing Algorithm”) genereert een hash van 256 bits lang.

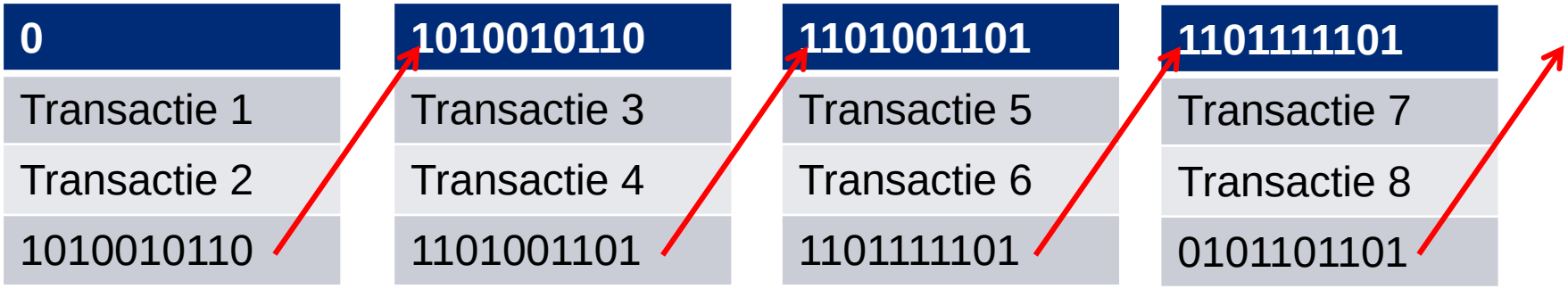
Probeer het op: https://passwordsgenerator.net/sha256-hash-generator/

Wat is de kans dat twee verschillende berichten eenzelfde hash genereren?

- Een bit sequentie van 256 bits is a getal dat ongeveer 1000 keer groter is dan het aantal atomen in het waarneembare universum.
- De kans dat twee verschillende berichten eenzelfde SHA-256 hash hebben is extreem klein. Het is echter zeker dat er oneindig veel berichten zijn die eenzelfde SHA-256 hash hebben.
- Het is praktisch onmogelijk om een bericht te maken dat eenzelfde SHA-256 hash heeft dan een welbepaald ander bericht. Er is nog geen betere methode gevonden dan “trial & error”.

Blockchain
Van open, verdeeld grootboek naar blockchain

- Elk blok gebruikt als hoofding, de hash van het vorige blok



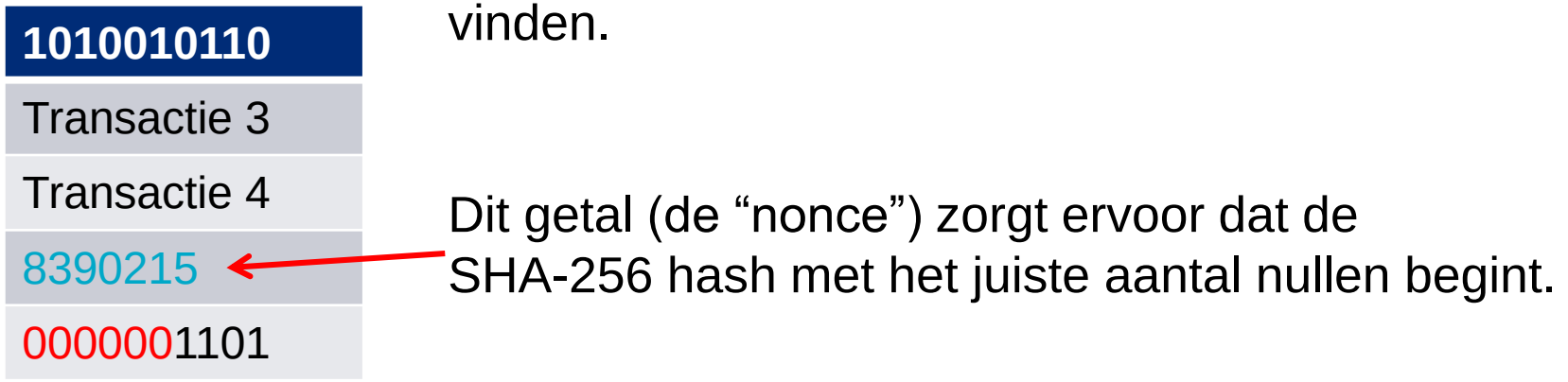
- Op deze manier wordt een keten (“chain”) van blokken gemaakt.
- De eerste deelnemer die de hash van de keten heeft gemaakt “wint” en zijn keten wordt door iedereen overgenomen. Indien er concurrerende ketens zijn, wint de langste keten.
- Elke verandering in een blok wijzigt de hash van dit blok en van alle volgende blokken. Vermits het berekenen van een hash heel snel gaat, is het dus heel eenvoudig om bedrog te plegen en transacties achteraf “aan te passen”. Moderne hardware kan 1 biljoen (10^{12}) SHA-256 hashes per seconde berekenen.

Blockchain
Van open, verdeeld grootboek naar blockchain

Om het rekenkundig “duur” te maken om bedrog te plegen wordt een bijkomende regel ingevoerd:

De SHA-256 van een blok moet beginnen met ***x nullen***.

“*x*” wordt zo gekozen dat het ongeveer 10 minuten duurt om een oplossing te vinden.



De “nonce” kan niet worden berekend, enkel d.m.v. “trial & error” worden geraden. Bij bitcoin zijn er nu gemiddeld meer dan 500 biljoen pogingen nodig om de juiste “nonce” te vinden. Dat duurt ongeveer 10 minuten. Het is eigenlijk een soort van loterij. Over hoe meer rekenkracht men beschikt, hoe groter de kans dat men wint.

Blockchain
Mining farm

Blockchain
Van open, verdeeld grootboek naar blockchain

De deelnemers die deze hashes “berekenen” noemt men “mijnwerkers”.

De eerste die een oplossing publiceert “wint” en krijgt een belonging (bij bitcoin nu: 6.25 bitcoins. Elke 210 000 “transacties” wordt deze belonging gehalveerd. Dus ongeveer eens per 4 jaar).

Als er twee concurrerende ketens zijn (met verschillende transacties), dan zal de langste keten winnen. Dit is het equivalent van de “meerderheids-beslissing). Hierdoor wordt bedrog uitgesloten.

Hoe werkt dit?

- A zendt een bericht naar B, maar niet naar het netwerk.
- A berekent de SHA-256 hash en – sinds niemand anders op de hoogte is van dit bericht – “wint” uiteraard. A zendt dit blok naar B, maar niet naar het netwerk. B denkt nu dat er een geldige transactie met A is.
- Vanaf nu moet A elke SHA-256 competitie winnen om B als eerste de bedriegelijke keten toe te zenden. Indien iemand anders sneller de juiste keten publiceert zal B merken dat de transactie van A ontbreekt.

Van open, verdeeld grootboek naar blockchain

- De andere mijnwerkers berekenen de SHA-256 hash van een keten die de valse transactie van A niet bevat.
- A moet B dus telkens een langere blockchain bezorgen dan de ketens die worden gepubliceerd door de andere mijnwerkers. Indien een andere mijnwerker een langere keten publiceert zal B automatisch de keten van A verwerpen.
- De hoeveelheid rekenkracht bepaalt de kans om een juiste oplossing te vinden. Om redelijk zeker te zijn dat men sneller is dan alle anderen, moet men over meer dan 50% van alle rekenkracht op het netwerk beschikken. Indien men over minder dan 50% van de totale rekenkracht beschikt, zal men na enige tijd de race verliezen en komt het bedrog uit.

  Dit wil zeggen dat men “nieuwe” blokken in de keten niet onmidddellijk mag vertrouwen. Pas wanneer een blok door meerdere nieuwe blokken wordt gevolgd, kan met vertrouwen de transactie aanvaarden.

Blockchain
Van open, verdeeld grootboek naar blockchain

Blockchain is dus een antwoord op volgende vragen:

- Hoe vertrouwen wekken tussen partijen die elkaar niet vertrouwen;
- Hoe een open, verdeeld grootboek te beheren dat:
  - Permanent,
  - Correct, en
  - Bestand (robuus)t is tegen manipulatie en verlies van connectiviteit.

Blockchain is echter geen antwoord voor:

- Krediet-risico (tenzij alle deelnemers een voorschot hebben gestort);
- De deelnemers aan het netwerk (“mijnwerkers”) aan te sporen om het netwerk te laten draaien.

  Bij bitcoin krijgen de mijnwerkers naast nieuwe bitcoins ook een kleine transactie-fee van de deelnemer. Transacties met hogere fees worden bij voorkeur in het mijnwerk opgenomen.

Blockchain
Wat kan je doen met een blockchain?

De inhoud van het transactie bericht kan eender wat zijn!

- Bitcoin (en een duizendtal gelijkaardige systemen) gebruiken het om betalingen buiten het klassieke bancaire systeem uit te voeren.
- Ethereum voerde “smart contracts” in. Bepaalde gebeurtenissen – terug te vinden in een transactie in een blok – lokken automatisch andere gebeurtenissen uit (bijv. overdracht van eigendomstitels). Er kan nooit een betwisting ontstaan: de software is “judge, jury and executioner”. Maar wat bij een “software” bug?
- Een verzekeringspolis kan in een blockchain worden gevat. Het bestaan, inhoud, aanpassingen, premies en schades kan in een blockchain worden gedocumenteerd. Eenmaal “blockchained” is er zekerheid dat de data niet meer kunnen worden gewijzigd.

  Marsh Digital ontwierp al in 2019 een blockchain applicatie voor “Proof of Insurance”.

Blockchain
Blokchain en verzekering

Blockchain kan het beheer van verzekeringen automatiseren, heeft geen behoefte aan tussenpersonen en een lage administratieve kost:

- Toekomstige verzekerden openen een nieuwe blockchain met hun vraag om verzekering en risico-informatie (in een afgesproken format) en plaatsen dit op het netwerk.
- Verzekeraars bieden (standaard) dekking aan voor het risico tegen een bepaalde premie en voegen dit aan de blockchain toe.
- Na een zekere tijd evalueert het netwerk de biedingen en sluit het automatisch een polis af met de “beste” verzekeraar. Dit wordt ook in de blockchain opgenomen.
- De blockchain bevat nu alle informatie nodig om een rechtsgeldige verzekeringspolis te documenteren. Premies, hernieuwingen, schades, aanpassingen, … kunnen ook in de blockchain worden opgenomen.

Een goed systeem voor standard-type verzekeringen waarbij geen gesofisticeerde risico-analyse nodig is.

Blockchain
Blokchain en verzekering

“Crowd-funded” verzekeringen via blockchain.

- De financiële zekerheid van de verzekeraars wordt gegarandeerd door de regels van het netwerk.
- Indien er statistisch robuste risico-modellen beschikbaar zijn, dan kan de financiële zekerheid continu worden geëvalueerd en aangepast bij het afsluiten van iedere nieuwe polis, het toetreden van nieuwe verzekeraars, het optreden van nieuwe schades, … Het verzekeringsbedrijf kan volledig worden geautomatiseerd. Er moet zelfs geen verzekeringsmaatschappij meer zijn! Het netwerk (= de deelnemers) zijn tegelijk verzekeraars en verzekerden.

Met een Internet of Things (“IoT”) blockchain kunnen “Things” zichzelf verzekeren en de polis aanpassen waar en wanneer nodig:

- Je auto meldt zelf wanneer je gaat rijden zodat je enkel premie betaalt wanneer je op de weg bent en niet wanneer je stil staat in de garage.
- De premie wordt aangepast aan je rijgedrag; of het gebied waar je rijdt.

Blockchain
Blokchain en verzekering

De basis van iedere verzekering is “vertrouwen”.

- De verzekeraar vertrouwt erop dat de verzekerde alle informatie over het risico bekend maakt.
- De verzekerde vertrouwt erop dat de verzekeraar kan en zal vergoeden als het risico zich voordoet.

De verzekeringswetgeving dwingt deze vertrouwensrelatie af.

Een centrale Autoriteit zorgt ervoor dat de verzekeraars dit vertrouwen waard zijn en blijven.

Dit systeem “werkt”, maar tegen een aanzienlijke kost.

Kan blockchain dit verbeteren?

Blockchain
Blokchain en verzekering

Een blockchain netwerk van gelijke deelnemers creëert vertrouwen tussen partijen die elkaar niet noodzakelijk vertrouwen.

- Hebben verzekeringen een vertrouwensprobleem?
- Wie zal deel uitmaken van het netwerk?
  - Het netwerk moet voldoende groot zijn om te vermijden dat 1 partij een meerderheid van de netwerk-schakels kan controleren.
  - Hoe spoor je de deelnemers aan om het netwerk draaiende te houden? De energiekost om hashes te berekenen is niet gering.
- Al wat een blockchain kan doen, kan ook worden gedaan door een vertrouwde centrale autoriteit en een klassieke database. Die centrale autoriteit kan een combinatie zijn van de verzekeraar, de makelaar(s) en de overhead.

Blockchain
Besluit

- Blockchain is een opwindende nieuwe technologie.
- Het belooft nieuwigheden en vervanging van bestaande systemen.
- Maar buiten “bitcoin”-systemen is er nog niet veel verwezenlijkt.
- Er zijn nog geen standaarden, geen algemeen aanvaarde werkmethodes, geen interactie tussen verschillende systemen, maar honderden elkaar uitsluitende systemen, patenten en applicaties.
- Is het een “oplossing op zoek naar een probleem”?
- Mijn voorspellingen:
  - Eerst zullen we toepassingen zien in welbepaalde niches met een beperkte scope (bijv. simpele verzekeringen), in parallel met bestaande systemen.
  - Standaarden zullen ontstaan binnen 2 tot 5 jaar. Hierdoor zullen er meer en bredere applicaties mogelijk worden.
  - Over 10 jaar zullen we ons afvragen hoe we ooit zonder blockchain hebben kunnen werken of het is totaal vergeten.

Met dank aan

Making our clients more successful