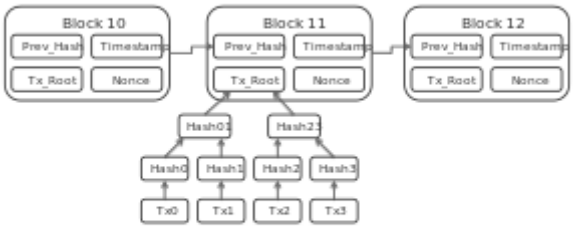
Blockchain

Een **blockchain** (blokketen) is een keten van data-elementen, blokken (*blocks*) genoemd, in volgorde van totstandkoming. Er is daarbij een eenvoudig te controleren systeem volgens welke opeenvolgende blokken aan elkaar gerelateerd behoren te zijn, zodanig dat naast verlengen alleen vertakken van de keten praktisch mogelijk is, niet het bij elkaar komen van twee takken. Binnen dit systeem zijn twee even lange ketens met hetzelfde laatste blok daardoor vrijwel zeker gelijk.



Schematisch overzicht van de blockchain van onder meer Bitcoin. Bovenaan staan drie *block headers*. Blok 11 wordt schematisch in zijn geheel getoond.

Een blockchain is een gedistribueerde database, dat wil zeggen dat meerdere partijen (nodes) een kopie hebben en werken aan het bijhouden van de keten, en elkaar controleren. Verder wordt bij een tijdelijke vertakking van de keten op basis van een vorm van consensus bepaald met welke tak wordt verder gegaan.

Een blockchain kan openbaar zijn, wat vaak samengaat met de mogelijkheid voor iedereen om als node op te treden. Dit vergt speciale voorzieningen om bescherming te bieden tegen manipulatie en vervalsing[1], zoals het veelgebruikte systeem *proof of work*.

Een blockchain kan ook besloten zijn, waarbij een autoriteit of vaste regels bepalen wie node is of kan worden.[2]

Verder zijn er per toepassing regels hoe data verwerkt worden in blokken.

Het komt voor dat met twee takken wordt verdergegaan (een *fork*), meestal met in één tak gewijzigde regels, en ook weleens bij onenigheid over het terugdraaien van dubieuze blokken.

Inhoud

Openbare blockchain met proof of work
- Werking
- Nadere uitleg
- Mining
- Toepassingen

Besloten blockchain

Blokfrequentie

IOTA

Billon

Nederland

België

Transacties buiten de blockchain

Zie ook

Openbare blockchain met proof of work

Vaak is er geen centrale autoriteit en zijn het ketensysteem, de regels voor het daarin verwerken van data, en de blockchain zelf openbaar, zodat iedereen kan controleren of de keten aan alle regels voldoet. Ook kan iedereen node worden. Hieronder wordt hiervan uitgegaan.

Werking

Een blok bestaat uit:

- de hash (hiermee wordt in dit verband altijd een cryptohash bedoeld) van het vorige blok (dit verbindt de blokken als schakels in de keten; als het vorige blok wordt gewijzigd is dit gemakkelijk te constateren doordat deze hash dan nie meer klopt)
- de eigenlijke data
- de nonce (zie hieronder)
- de datum en tijd waarop het blok is gevonden

Hetzelfde, maar met in plaats van de eigenlijke data de top van de hash-boom daarvan (*merkle root hash*, in de illustratie aangegeven met Tx_Root), wordt de *block header* genoemd.

Het vinden van een blok begint met het controleren dat binnengekomen transacties voldoen aan algemene regels, zoals dat iemand een ontvangen tegoed niet een tweede keer uitgeeft, en eventueel speciale regels, zoals bij het uitvoeren van een *smart contract*; ook kan uit het smart contract zelf een transactie voortvloeien, bijvoorbeeld bij een aflopende future.

Vervolgens wordt door wie dat wil (zogenaamde *miners*) een nonce gezocht waarbij de hash van het blok (anders gezegd, de hash van de block header) aan bepaalde speciale eisen voldoet. Dit is doelbewust ontworpen als veel werk (*proof of work*), met brute force, zodat het zeer moeilijk is een blok te wijzigen als er blokken na gekomen zijn, want die moeten dan ook gewijzigd worden, dat wil zeggen opnieuw gevonden. In onder meer de bitcoinsoftware is de grootte van de nonce bepaald op 32 bits.[3] Dit geeft 2^{32} (ruim vier miljard) mogelijkheden. Vaak voldoet geen enkele aan de eisen, zoals blijkt door ze allemaal te proberen. De miner maakt dan inhoudelijk niet relevante wijzigingen in het blok, zoals het wijzigen van de volgorde van de transacties, of het gebruiken van een *extranonce*, een extra serie bits die veranderd kan worden zonder inhoudelijke consequenties.[4] In zulke gevallen moet ook de top van de hash-boom opnieuw worden berekend.

Een gevonden blok bevat vaak automatisch een beloningstransactie, de uitgifte van een bedrag aan cryptogeld. Bij het vinden van een blok kan een deel van de transacties ook een beloning (*fee*) inhouden, namelijk als er een input van cryptogeld is die groter is dan de output ervan.

Vele miners concurreren om het eerst een blok te vinden. Het te vinden blok is om diverse redenen niet uniek. Zodra een blok gevonden is wordt dat blok bekendgemaakt. Als het correct blijkt heeft het voor de andere miners geen zin meer om te blijven zoeken naar een andere goede versie (ook omdat het feit dat men al veel werk heeft verricht aan het vinden van een blok de kans dat men dat vervolgens snel vindt nauwelijks vergroot). Ze gaan daarom vervolgens zoeken naar een blok dat voortbouwt op het nieuwe blok.

Nadere uitleg

Als aan een keten van blokken een nieuw blok wordt toegevoegd, dan is dit nieuwe blok gebaseerd op het vorige blok, op nieuwe data, en op een met veel rekenkracht gevonden bitreeks in het nieuwe blok (*cryptografische nonce*) waarbij de hash van het blok met een vereist aantal nulbits begint (cryptohashing). Het rekenwerk om de keten te verlengen kan dus pas beginnen als het vorige blok vaststaat.

Een blok wordt dus gekoppeld door middel van een verwijzing naar een vorig blok. Deze verwijzing is eigenlijk een cryptohash van de header van het vorige blok.[5] Bij een blockchain kan er worden gekozen om een extra moeilijkheid aan te brengen in het berekenen van deze verwijzing. Dit gebeurt door eisen te stellen aan de hash die wordt berekend. Er wordt gezocht naar een hash die begint met een aantal nullen. Hoe hoger het aantal geëiste nullen, hoe moeilijker het is om een hash te vinden. Deze methode is voor het eerst gebruikt om spam op e-mailadressen tegen te gaan.

Omdat een hash een zogenaamde "one-way function" is, kan van een hash niet worden afgeleid hoe de gegevens eruitzien. Ook is het de bedoeling dat een hash uniek is. Als er een bit of teken verandert in een stuk code of document, zal de hash in zijn geheel veranderen. Elke wijziging is dus waarneembaar

Blokken zijn dus met elkaar verbonden via een hash. Deze hash wordt opgeslagen in de header, en deze zal gebruikt worden voor het maken van de hash van dat blok. Dit betekent dat bij een wijziging in een blok, alle blokken die daarna komen ook gewijzigd moeten worden.

Stel dat er een blok 1 is. Na blok 1 komt er een blok 2, 3 en 4. Als blok 1 wordt aangepast, klopt de verwijzing in (de header van) blok 2 niet meer (omdat de hash erin opnieuw berekend moet worden). Blok 2 moet hierdoor ook aangepast worden. De verwijzing in blok 3 klopt niet meer, dus blok 3 moet worden aangepast, etc.

Omdat er meerdere nodes zijn, kan dit soort problemen worden gedetecteerd en opgelost (door de aanpassingen stop te zetten of de node die deze gegevens verzendt te negeren). Dit systeem zorgt voor de integriteit die blockchains biedt.

Mining

Bij een blockchain waar iedereen aan mee kan werken is er een systeem van concurrentie waarbij veel rekenkracht nodig is om een nieuw blok te vinden: het blok is pas af als met hashberekeningen (meestal zeer veel, maar dit aantal is van het toeval afhankelijk) een blok gevonden wordt dat aan de eisen voldoet. De eerste die dat lukt wordt beloond. Het is een vorm van *proof-of-work*-systeem. De deelnemers worden *miners* genoemd, het werk *minen*.

Miners controleren transacties en verrichten digitale handelingen voorgeschreven door de eventuele smart contracts, en verwerken een en ander in een blok. Verschillende miners kunnen transacties verschillend selecteren (wel krijgen die met een grote *fee* vaak voorrang) waardoor ze hashes zoeken voor verschillende potentieel correcte blokken. Als een blok is gevonden gaan de miners dat eerst controleren en vervolgens daarop voortbouwen, met inachtneming van wat in het winnende blok al gedaan is.

De miners hebben belang bij correct werken, want een gevonden blok wordt door andere miners gecontroleerd, en in het geval van een fout verworpen. Miners gaan dan verder werken met een vertakking van de blokchain waarin dit verkeerde blok is vervangen door een goed blok. De geaccepteerde blokchain bevat dan niet het verkeerde blok. Bij een systeem waarbij de beloning een bedrag in cryptogeld is dat in het blok geregistreerd staat wordt deze zo vanzelf onbruikbaar

Miners ontvangen naast de beloning voor veel transacties ook een transactievergoeding (fee), vaak een vrijwillige bijdrage van de betaler om de verwerking te bespoedigen.

Bij het bezitten van een hoeveelheid rekenkracht die groter is dan 50% van de totale rekenkracht binnen het miningnetwerk, is het mogelijk om gegevens in een blockchain aan te passen. Het gaat daarbij om de rekenkracht met betrekking tot het betreffende hashingalgoritme. Een miner van bitcoin met 10% van de totale rekenkracht van het minen van bitcoin kan bijvoorbeeld, omschakelend naar een blockchain met hetzelfde hashingalgoritme, 51% van de totale rekenkracht van het minen daarvan hebben. In die zin zou een blockchain met hetzelfde hashingalgoritme als bitcoin, maar met een veel kleinere benodigde rekenkracht per seconde, relatief kwetsbaar kunnen zijn.[6]

Een en ander is ook de reden dat sommige bedrijven kiezen voor een blockchainnetwerk zonder miners.[7]

Toepassingen

Blockchaintechnologie ligt aan de basis van cryptovaluta als bitcoin, maar er zijn ook andere toepassingen in gebruik of in onderzoek, zoals bij het R3 consortium (tussen banken).[8]

Zoals een blockchain de overdracht van bedragen in een cryptovaluta als transacties vastlegt (met daaruit steeds af te leiden het bij een cryptogeldadres behorende bezit), zou één blokchain ook transacties in allerlei verschillende valuta, effecten en goederen kunnen vastleggen. Het object van een transactie hoeft namelijk niet in een getal uit te drukken te zijn (zoals aantal bitcoins waarbij bijv. het ene bedrag van 3 bitcoin gelijkwaardig is aan het andere van 3 bitcoin), maar kan ook bestaan uit een hoeveelheid en een soort, of

zelfs iets unieks zoals een bepaald huis, of een bepaalde zitplaats voor een bepaalde voorstelling. Men spreekt in dit verband wel van *colored coins*. In één transactie zouden ook de overdracht van het goed en de omgekeerde overdracht van de koopsom kunnen worden vastgelegd.[9][10][11] EPOBC is een van de manieren om colored coin transacties te coderen in de bitcoin-blockchain.[12]

Soms wordt een blockchain mede gebruikt voor een ander doel dan waarvoor deze gemaakt is, zoals het permanent vastleggen van een tekst op de plaats van de hash van de publieke sleutel van de begunstigde van een kleine cryptogeldtransactie.[13]

Besloten blockchain

Een blockchain kan in een of meer van de volgende opzichten besloten zijn (naast *besloten blockchain* worden ook de uitdrukkingen *gesloten blockchain* en *permissioned blockchain* gebruikt):[14][15][16]

- niet-openbare inhoud van de blockchain
- niet iedereen kan meedoen met het uitvoeren van transacties (wat bijvoorbeeld wel kan bij cryptovaluta, hoewel mer natuurlijk pas een bedrag kan uitgeven als men het eerst ontvangen heeft)
- niet iedereen kan een nieuw blok aan de keten toevoegen

Bij een vergunning om de blockchain in te zien hoeft het niet alles of niets te zijn, een deelnemer kan ook vergunning hebben om kennis te nemen van een deel van de inhoud, dat per deelnemer kan verschillen. Evenzo kan een deelnemer beperkt vergunning hebben tot het uitvoeren van transacties.

Als alleen bepaalde deelnemers een blok aan de keten mogen toevoegen kan het zijn dat *proof of work* niet nodig is. Absoluut vertrouwen in elk van deze deelnemers is niet nodig, want ook bij een besloten blockchain is er consensus nodig onder een groep deelnemers.

In zo'n geval wordt een blok niet *gevonden*, maar gewoon *gemaakt*, en is de nonce niet van toepassing, en bestaat het blok uit:

- de hash van het vorige blok (dit verbindt de blokken als schakels in de keten; als het vorige blok wordt gewijzigd is dit gemakkelijk te constateren doordat deze hash dan niet meer klopt)
- de eigenlijke data
- de datum en tijd waarop het blok is gemaakt

Anders dan bij een systeem dat in geen van de genoemde opzichten besloten is, en waarbij dus alle details over de werking van het systeem openbaar moeten zijn, is er over besloten blockchains soms minder bekend. Het is soms bij een geclaimde toepassing van blockchaintechnologie zelfs niet duidelijk wat daarbij nu eigenlijk de significantie van het blockchainconcept is.

Enkele Europese banken proberen bijvoorbeeld het gebruik van een blockchain uit voor handel in olie en landbouwproducten, op het platform *Easy Trade Connect*, ook *Easy Trading Connect* genoemd. Er wordt vooral gewezen op de voordelen van digitalisering en standaardisering. Het lijkt te gaan om een blockchain die besloten is in de zin van niet-openbare data, en in de zin van een besloten groep nodes, zoals de koper, de verkoper, de vervoerder en de bank, met van die rol afhangende bevoegdheden tot het toevoegen van data. Het lijkt te gaan om een blockchain zonder *proof of work*.[17][18][19] Het is niet duidelijk of er iedere keer bij nieuwe data (zoals contracten, certificaten en kredietbrieven) een blok aan de keten wordt toegevoegd, of dat meerdere toevoegingen van data samen in één blok worden geplaatst (en trouwens ook niet of dit hierbij een relevant verschil zou zijn).

Blokfrequentie

Eens in de 10 minuten wordt een bitcoinblok gevonden, en eens in de 12 tot 15 seconden een ethereumblok.[20][21]

IOTA

De cryptovaluta IOTA gebruikt in plaats van een blockchain een acyclische gerichte graaf (*directed acyclic graph*, DAG). met als knooppunten afzonderlijke transacties (er zijn geen blokken). Een transactie doorgeven gaat gepaard met het controleren van twee willekeurig gegenereerde andere transacties. Er is geen fee verschuldigd. Er is een vast aantal eenheden van de cryptovaluta, en er is geen mining.

Billon

Het Poolse bedrijf Billon gebruikt een blockchain voor fiatgeld, zonder mining, dat veel meer transacties per seconde aankan dan Bitcoin.[22]

Nederland

Om de kansen voor de Nederlandse overheid van de nieuwe technologie vast te stellen, worden sinds 2016 diverse pilots georganiseerd met o.a. hetkadaster, de belastingdienst en de Kamer van Koophandel[23]

Juridische aspecten van een blockchain kunnen onder meer aan de orde zijn als er persoonsgegevens in staan. Gezien de Algemene verordening gegevensbescherming is een open blockchain dan wellicht niet mogelijk.[24]

België

In België werd in juli 2017 een pilootproject opgezet in de Antwerpse haven, voor de verwerking van containers.[25] Ook de Vlaamse overheid werkt aan de introductie van de blockchain-technologie.[26]

Transacties buiten de blockchain

Soms heeft het voordelen bepaalde transacties niet afzonderlijk in de blockchain te registreren, maar slechts het saldo van meerdere van deze transacties (niet noodzakelijk tussen dezelfde twee partijen). Dit is het principe van het in ontwikkeling zijnde *Lightning Network*, en kan ook toegepast worden door een handelsplatform waarbij klanten een rekeningcourant van cryptovaluta en fiatgeld aanhouden.

Zie ook

- Joseph Lubin, Canadese entrepreneur en blockchain-ontwikkelaar
- Satoshi Nakamoto, pseudoniem van de ontwerper van bitcoin
- Vitalik Buterin, computerprogrammeur en mede-oprichter van Ethereum

Bronnen

- Dit artikel is gebaseerd op de Engelse wikipedia.

Noten

1. Forbes: Beyond bitcoin: how the blockchain could disrupt our financial system (http://www.forbes.com/sites/sap/2015/08/11/beyond-bitcoin-how-the-blockchain-could-disrupt-our-financial-system)
2. https://www.ibm.com/blogs/blockchain/2017/05/the-dif ference-between-public-and-private-blockchain
3. https://en.bitcoin.it/wiki/Nonce
4. bitcointalk.org/index.php?topic=1040859.0
5. Bitcoin wiki: Blockheader/hashing algorithm (https://en.bitcoin.it/wiki/Block_hashing_algorithm)
6. http://docplayer .net/57444877-Gulden-improving-the-blockchain.html
7. Bitcoin Developer Documentation, z.d. (https://bitcoin.org/en/developer-documentation/)
8. https://techcrunch.com/2017/05/23/blockchain-consortium-r3-raises-107-million/
9. https://www.bestebank.org/colored-coins
10. https://en.bitcoin.it/wiki/Colored_Coins
11. Zie https://web.archive.org/web/20170923071105/https://tokenmarket.net/blockchain/ voor een overzicht van blockchains met de transacties van diverse bezittingen per blockchain.
12. https://github.com/chromaway/ngcccbase/wiki/EPOBC_simple
13. Zoals https://CryptoGraf fiti.info detecteert en vergemakkelijkt op de blockchain van Bitcoin Cash.
14. https://www.coindesk.com/information/what-is-the-dif ference-between-open-and-permissioned-blockchains
15. https://www.ibm.com/blogs/blockchain/2017/05/the-dif ference-between-public-and-private-blockchain

16. https://monax.io/explainers/permissioned_blockchains
17. https://www.txfnews.com/News/Article/6200/Blockchain-or-blocked-chain
18. http://www.quotenet.nl/Nieuws/ABN-Amro-en-ING-verhandelen-als-eerste-voedsel- via-blockchain-infographic-209759
19. https://www.ing.com/Newsroom/All-news/Easy-T rading-Connect-on-the-verge-of-digitalising-an-age-old-sector.htm
20. https://www.coindesk.com/information/ethereum-mining-works
21. https://www.etherchain.org
22. https://www.realwire.com/releases/Billon-sets-industry-standard-benchmark-for-Blo ckchain-scalability
23. BLOCKCHAIN PILOTS (https://www.blockchainpilots.nl/)
24. Whitepaper Juridische aspecten van Blockchain (https://platformoutsourcing.nl/f/files/download/overig/whitepaper_blockchain.pdf)
25. Blockchain pilot solution to release Antwerp containers (https://www.enterprisetimes.co.uk/2017/07/03/blockchain-pilot-solution-release-antwerp-containers/) (3 juli 2017). Geraadpleegd op 7 december 2017
26. Infosessie blockchain - VOLZET (https://overheid.vlaanderen.be/infosessie-blockchain-volzet) . Vlaamse overheid (november 2017). Geraadpleegd op 7 december 2017