

Hoofdstuk #9

Een introductie tot de technische kant van bitcoin

9.0 Inleiding

Activiteit: bekijk "Hoe bitcoin werkt onder de motorkap"

9.1 Public keys en private keys: beveiliging door cryptografie

9.1.1 Cryptografische public keys en private keys

9.1.2 Uitleg over hashing

Activiteit: genereer een SHA-256 hash

9.2 Het UTXO model

9.3 Bitcoinnodes en miners nader bekeken

9.3.1 Wat is een bitcoinnode en hoe zet ik er een op?

Activiteit: bekijk een video over bitcoinnodes

9.3.2 Wat is een bitcoinminer en hoe werkt mining?

9.4 Wat is de mempool?

Activiteit: mempool

9.5 Hoe bitcointransacties van begin tot eind werken

Activiteit: bitcointransacties in actie

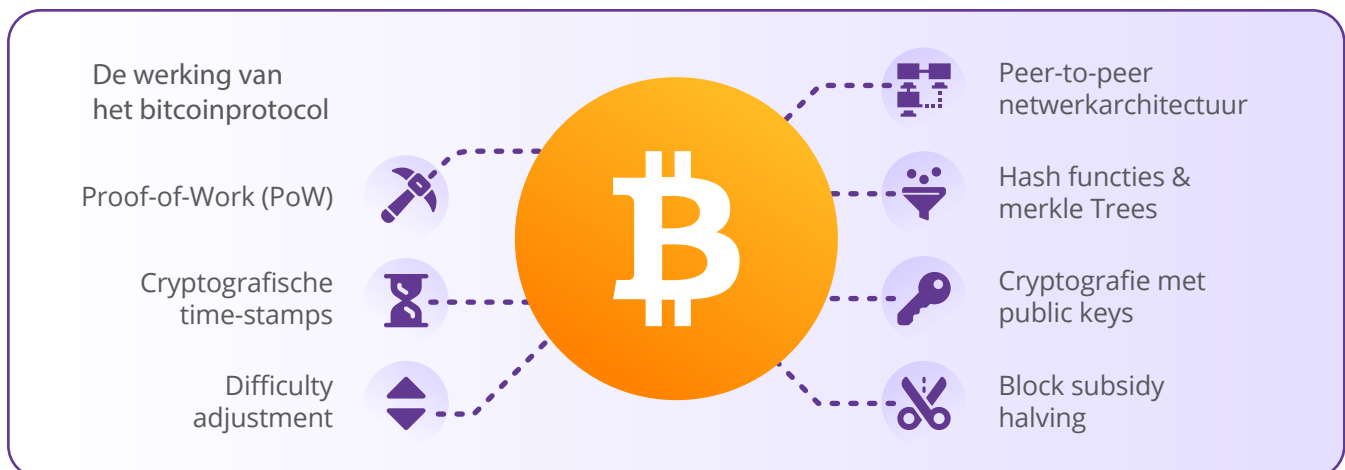
Een introductie tot de technische kant van bitcoin

9.0 Inleiding

Bitcoin is niet "ongereguleerd". Het wordt gereguleerd door een algoritme in plaats van dat het wordt gereguleerd door overheidsbureaucratieën, zonder corruptie.

Andreas M. Antonopoulos

In dit hoofdstuk gaan we dieper in op de technologie die ervoor zorgt dat het bitcoinnetwerk volledig gedecentraliseerd werkt. We leggen op een eenvoudige manier uit wat er gebeurt als je een bitcointransactie verstuurt, hoe deze transacties worden verwerkt en wat miners en nodes doen in het bitcoinnetwerk. We gaan in dit hoofdstuk een aantal uitdagende en technische concepten behandelen. Het is belangrijk om te onthouden dat veel mensen niet begrijpen hoe het internet werkt, maar dat ze het wel elke dag gebruiken om e-mails te versturen, contact te leggen met vrienden op sociale media en zelfs om hun rekeningen te betalen. Het leren van de technische kant van hoe bitcoin werkt is een lange reis die misschien niet iedereen wil maken, zelfs als ze besluiten om het als geld te gebruiken. We moedigen je aan om te blijven leren over de technische aspecten van bitcoin, al beperken we ons in dit hoofdstuk tot de belangrijkste basisbegrippen.



Als je een dieper technisch begrip wilt van hoe bitcoin werkt, hebben we achterin dit werkboek bronnen opgenomen. Je kunt je op onze website ook inschrijven voor Het Bitcoindiploma - Technische Editie om een bericht te krijgen als die meer technische cursus klaar is.

Laten we beginnen met het bekijken van een video die laat zien hoe het bitcoinnetwerk werkt.

Activiteit - bekijk
"Hoe bitcoin werkt
onder de motorkap".



Zoals je in de video hebt gezien, is het bitcoinnetwerk simpelweg een kasboek of registratie van transacties die is opgeslagen op meerdere computers die nodes worden genoemd. Het bitcoinkasboek is pseudoniem, wat betekent dat het geen persoonlijke gegevens bevat, alleen transactie- en adresinformatie. Het kasboek toont elke bitcoin en zijn bewegingen sinds de start van het netwerk op 3 januari 2009.

Nu gaan we dieper in op de technologie die dit systeem mogelijk maakt.

9.1 1 Public keys en private keys: beveiliging door cryptografie

Bitcoin geeft ons een harde belofte:
het programma zal precies zo worden uitgevoerd als gespecificeerd.

Andreas M. Antonopoulos

9.1.1 1 Cryptografische public keys en private keys

Cryptografie is een manier om informatie geheim te houden door het te verhullen in code.



- Encryptie is het proces waarbij informatie wordt omgezet in een speciale code, waardoor het onleesbaar wordt voor iedereen die niet over de juiste decryptiemethode beschikt. Dit is vergelijkbaar met het vergrendelen van een kluis, waarbij alleen de persoon met de juiste sleutel of combinatie deze kan openen.
- Decryptie daarentegen is het proces waarbij de versleutelde informatie weer leesbaar wordt gemaakt, alsof je de kluis ontgrendelt en de toegang krijgt tot de inhoud ervan.

Laten we bijvoorbeeld zeggen dat John een geheim bericht wil sturen naar Peter dat niet bedoeld is voor anderen om te lezen. Ze spreken af om de Pigpen-code te gebruiken om het bericht te verhullen voordat ze het versturen. Alleen degenen met de code kunnen het bericht ontcijferen, waardoor het onleesbaar wordt voor anderen. Hoewel deze methode tegenwoordig niet meer als veilig wordt beschouwd, illustreert het wel het principe van cryptografie met private keys om berichten te versturen.

Hoe werkt cryptografie in bitcointransacties?

In traditionele cryptografie met private keys moeten John en Peter eerst een geheime sleutel delen, zoals een wachtwoord of de Pigpen-code. John zal dan deze sleutel gebruiken om zijn bericht te versleutelen voordat hij het naar Peter stuurt. Peter, die ook de geheime sleutel kent, kan dan dezelfde sleutel gebruiken om het bericht te ontcijferen.

Als iemand anders echter in het bezit is van deze sleutel en het bericht onderschept, kan hij dit bericht ook ontcijferen en lezen.

De Pigpen-code ontcijferen

Bij het oplossen van de Pigpen-code krijgt de speler een versleuteld bericht en een cijfer. Om het bericht te ontcijferen, moet de speler het symbool van het versleutelde bericht op de code vinden om de ontcijferde letter te vinden.

Voorbeeld van een versleuteld bericht:



A	B	C	J	K	L	S	W
D	E	F	M	N	O	T	X
G	H	I	P	Q	R	U	Y
						V	Z

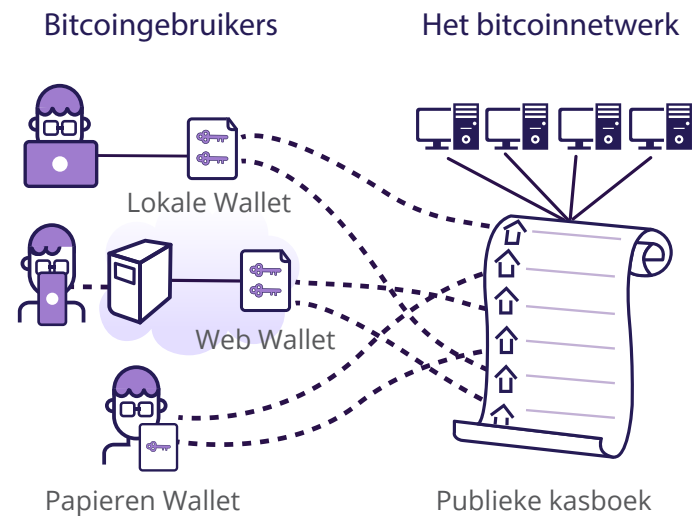
Een introductie tot de technische kant van bitcoin

Cryptografie met **public keys**, het type dat wordt gebruikt bij bitcointransacties, heeft dit probleem opgelost. Met cryptografie op basis van **public keys** hoeven John en Peter het wachtwoord of de versleutelmethode niet met elkaar te delen. In plaats daarvan hebben ze elk twee verschillende sleutels: een **public key** (die je veilig met iedereen kunt delen) en een **private key** (die je geheim moet houden).

In dit geval wil John een bericht naar Peter sturen. Hij gebruikt de **public key** van Peter om zijn eigen bericht te versleutelen voordat hij het naar Peter stuurt. Wanneer Peter het bericht ontvangt, kan alleen hij het ontsleutelen met zijn **private key**. Iemand anders kan het bericht niet lezen, zelfs niet als hij het onderschept. De kans is ook veel kleiner om de sleutel te stelen, omdat zelfs John en Peter de sleutel niet met elkaar hoeven te delen.

Het belangrijkste voordeel van cryptografie met **public keys** ten opzichte van cryptografie met een **private key** is dus dat het veilige communicatie mogelijk maakt zonder dat verzender en ontvanger eerst een geheime sleutel hoeven te delen (of een andere versleutelmethode zoals Pigpen-code), die door een derde partij onderschept zou kunnen worden.

Bij bitcoin wordt cryptografie met public keys niet gebruikt om versleutelde berichten te versturen. In plaats daarvan wordt het gebruikt om unieke **digitale handtekeningen** te maken die bitcointransacties onveranderbaar maken. Een **digitale handtekening** is een manier om de authenticiteit van een bitcointransactie aan te tonen, vergelijkbaar met een handtekening op een fysiek document.



Cryptografie met public keys (voor transacties tussen twee gebruikers):

Elke gebruiker heeft twee sleutels, een **private key** die geheim wordt gehouden en een **public key** die met anderen kan worden gedeeld.

De **private key** dient als een vorm van identificatie en bewijs van eigendom en bevestigt "dit adres is van mij en ik heb er controle over".

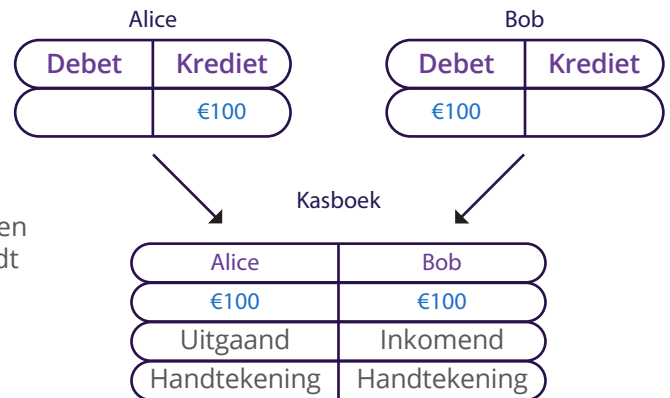
Digitale handtekeningen worden gemaakt om unieke transacties te identificeren.



Digitale handtekening



- ☀ Een bitcointransactie houdt in dat iemand een bepaalde hoeveelheid bitcoin rechtstreeks overmaakt aan een ander.
- ☀ Encryptie wordt gebruikt om ervoor te zorgen dat alleen de echte eigenaar van de bitcoin de controle heeft om zijn geld naar iemand anders te sturen. Het zorgt ervoor dat het eigendom wordt beschermd tegen kwaadwillende actoren.
- ☀ Als extra beschermingsmaatregel krijgt elke transactie die je in bitcoin verstuurt automatisch een **unieke** handtekening. Deze **unieke handtekening** wordt mogelijk gemaakt door manipulatiebestendige technologie die het netwerk helpt te verifiëren dat de echte eigenaar van de bitcoin de bitcoin heeft verzonden, en niet iemand anders.



Hoe dit werkt in een echte bitcointransactie?

- 1** Bitcointransactie creëren:
Een gebruiker initieert een bitcointransactie door bepaalde details op te geven zoals het adres van de ontvanger en de hoeveelheid bitcoin die verstuurd moet worden.
- 2** Digitale handtekening genereren:
De verzender genereert een unieke **digitale handtekening** met behulp van zijn private key. Deze handtekening is een unieke cryptografische code die de authenticiteit van de transactie bewijst.
- 3** Transactie "broadcasten":
De ondertekende transactie wordt als een broadcast verzonden naar het bitcoinnetwerk om aan te geven dat het eigendom van de bitcoin overgedragen moet worden aan de ontvanger.
- 4** Verificatie op het netwerk:
Nodes op het bitcoinnetwerk ontvangen de transactie en gebruiken de **public key** van de ontvanger om de transactie te ontsleutelen en de integriteit ervan te verifiëren. Tegelijkertijd gebruiken ze de **public key** van de verzender om de **digitale handtekening** te verifiëren.
- 5** Bevestiging op het bitcoinnetwerk:
Als de verificatie succesvol is, wordt de transactie toegevoegd aan het kasboek (ook wel ledger genoemd), dat dient als een veilige, transparante registratie van alle transacties. Na bevestiging is het eigendom van de bitcoin overgedragen van de verzender naar de ontvanger.



Samengevat: een **digitale handtekening** die je maakt met je **private key** dient als cryptografisch bewijs van authenticiteit en eigendom. Pas na ondertekening van een transactie met je **digitale handtekening** kan het bitcoinnetwerk de transactie verifiëren en vastleggen in het kasboek.

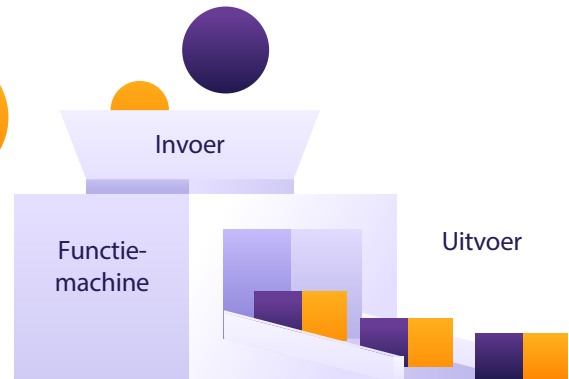
Een introductie tot de technische kant van bitcoin

9.1.2 Uitleg over hashing

Laat je alsjeblieft niet intimideren door de technische termen en wiskundige concepten die voor je liggen. We begrijpen dat niet iedereen gek is op wiskunde, maar misschien verras je jezelf en zie je dat zelfs de meest complexe ideeën met een beetje moeite te begrijpen zijn.

Wat is een functie?

Een functie is zoals een machine die bepaalde informatie verandert in iets nieuws. De informatie die je de functie geeft wordt de **invoer** genoemd. De nieuwe informatie die de functie maakt, wordt de **uitvoer** genoemd. Functies helpen computers om taken uit te voeren en problemen op te lossen.



Vergelijk het met een recept voor het maken van een salade. Het recept (of de functie) vertelt je welke ingrediënten je moet gebruiken en hoe je ze moet mengen om de salade te maken. Je kunt er andere ingrediënten in doen, maar het recept geeft je altijd een salade als resultaat. Functies kunnen worden gebruikt om dingen gemakkelijker en efficiënter te maken.

Dit recept is dus een functie die de ingrediënten als **invoer** neemt en de gemengde salade als **uitvoer** genereert.

In bitcoin worden functies gebruikt om transacties uit te voeren. We weten al dat transacties in bitcoin in wezen overdrachten van waarde (geld) van het ene adres naar het andere zijn. Om een transactie uit te voeren, worden een aantal cryptografische functies gebruikt om de transactie te valideren en het kasboek bij te werken.



De functies die gebruikt worden bij een bitcointransactie zijn onder andere het verifiëren van de authenticiteit van de transactie-invoer, controleren of de verzender voldoende geld heeft en het bijwerken van de tegoeden van de betrokken adressen. Zodra een transactie is geverifieerd en is toegevoegd aan een block in het kasboek, wordt deze onderdeel van de permanente registratie van alle transacties op het netwerk.

Wat is een eenrichtingsfunctie?

Een eenrichtingsfunctie gebruikt een reeks instructies om de informatie te verwerken en verandert het in iets nieuws, zoals een smoothierecept ingrediënten verandert in een nieuw drankje. Maar net zoals je een smoothie niet kunt 'un-blenden' om de oorspronkelijke ingrediënten terug te krijgen, kun je de eenrichtingsfunctie niet omkeren om de oorspronkelijke informatie terug te krijgen.



Cryptografie met **private keys** en **public keys**, berust op het gebruik van eenrichtingsfuncties, waardoor het moeilijk is om de **private key** uit de public key te bepalen. In theorie is het niet helemaal "onmogelijk" om de **private key** uit de public key te achterhalen, maar het is extreem moeilijk om dit te doen en het zou een buitensporige hoeveelheid tijd en rekenkracht kosten.

Het vinden van een **private key** uit een public key in bitcoin is als het proberen te vinden van een naald in een hooiberg zo groot als een voetbalveld. De naald staat voor de **private key** en de hooiberg voor alle mogelijke **private keys**.

Op dezelfde manier zijn eenrichtingsfuncties ontworpen om onomkeerbaar te zijn en niet ontcijferd te kunnen worden.



Wat is een hashfunctie?

Hashing is als een vingerafdruk voor digitale gegevens. Het is een proces waarbij een digitaal bericht wordt omgezet in een code met een vaste lengte, die dient als een unieke identificatiecode.



Net zoals een vingerafdruk een persoon kan identificeren, kan een hash een digitaal bericht identificeren. Hashes worden in veel toepassingen gebruikt, waaronder bitcointransacties.

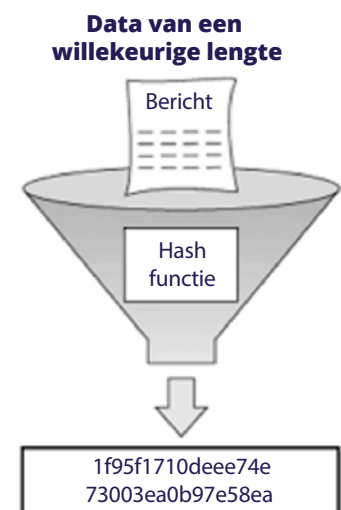
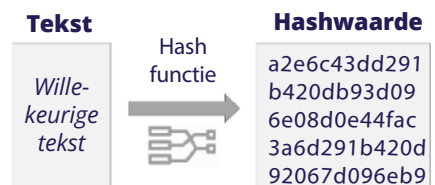
Hoe hashing wordt gebruikt in bitcointransacties

Elke bitcointransactie wordt gehasht voordat deze wordt toegevoegd aan het kasboek. De hash fungeert als handtekening voor de transactie en verifieert dat de transactie geldig is en dat er niet mee geknoeid is. Als iemand zelfs maar één letter in de transactie probeert te veranderen, zal de hash compleet anders zijn en zijn anderen gewaarschuwd.

De rol van hashing in beveiliging

Hashing is essentieel voor de veiligheid van het bitcoinnetwerk. Door hashes te gebruiken voor de identificatie van transacties, kan het netwerk elke poging tot verandering of manipulatie van een transactie detecteren. Dit helpt fraude te voorkomen en zorgt ervoor dat alle transacties nauwkeurig worden geregistreerd in het kasboek.

Een hashfunctie is een soort eenrichtingsfunctie die een **invoer** (aangeduid als het "bericht" of "gegevens") omzet in een uitvoer, in de vorm van een numerieke weergave die een "hash" wordt genoemd. Deze hash is uniek voor de specifieke invoergegevens die zijn gebruikt, dus zelfs een kleine verandering in de invoergegevens resulteert in een compleet andere hash.

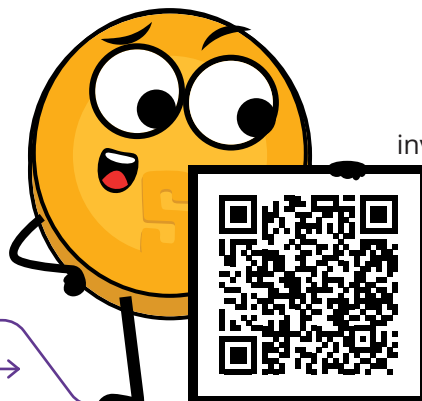


Een hash functie is als een machine die geheime code maakt. Het verandert een normaal **bericht** in een code.



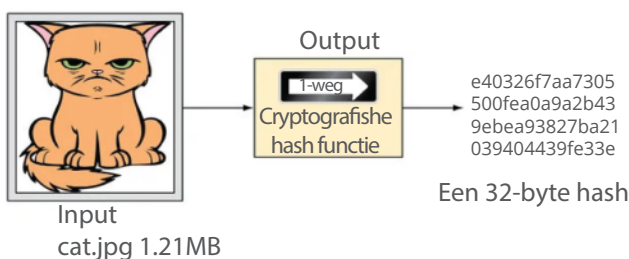
Een introductie tot de technische kant van bitcoin

De code ziet er altijd hetzelfde uit voor hetzelfde bericht. Als je het bericht ook maar een beetje verandert, ziet de code er compleet anders uit. Dit helpt computers dingen te onthouden en te controleren of er iets is veranderd.

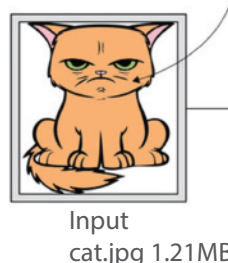


Direct een SHA-256 hash genereren van een willekeurige tekenreeks of invoerwaarde. Hash functies worden gebruikt als eenrichtingsmethoden.

Activiteit: genereer een SHA-256 Hash →



Er ontbreekt een snorhaar in dit plaatje



Een volledig andere hash dan het vorige plaatje

De **uitvoer** van een hash functie is altijd even lang, ongeacht de lengte van de oorspronkelijke invoer.

Bitcoin gebruikt specifieke hashfuncties: SHA-256 en RIPEMD160. Hieronder een paar voorbeelden:

☀ Merk op dat een "." in de tweede invoer de uitvoer volledig verandert ten opzichte van de eerste.

☀ De derde invoer is een enorm bestand, maar de uitvoer heeft nog steeds dezelfde vaste lengte als de andere twee.

De SHA-256 waarde van "hello world"

B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcded

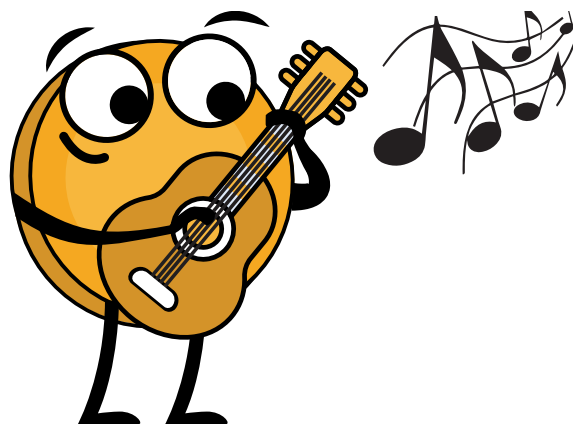
De SHA-256 waarde van "hello world."

7ddb22731 5f423250fc67f3be69c544628dffe41752af91 c50aeQa9c49faeb87

De SHA-256 waarde van een groot ISO bestand "Ubuntu 24.04"

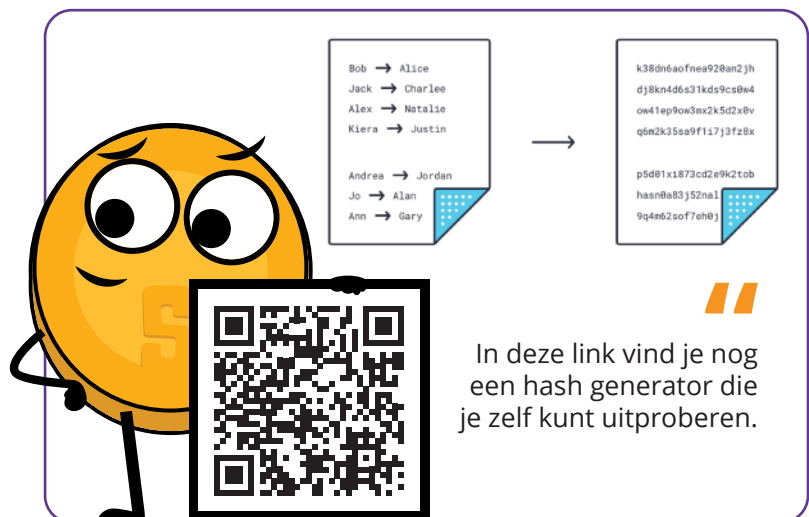
7b9f670c749f797a0f7481d61 9ce8807edac052c97e1 a0df3b130c95efae4765

Hashing kan ook gezien worden als een partituur die de essentie van een muziekstuk weergeeft. Net zoals dat een partituur een unieke weergave van een muziekstuk is, is een hashwaarde een unieke weergave van een stuk data. Door de partituur van een muziekstuk te vergelijken met de daadwerkelijke uitvoering, kan een muzikant bepalen of de uitvoering accuraat is. Op dezelfde manier kan het vergelijken van de hashwaarde bepalen of de gegevens tijdens de overdracht zijn gewijzigd.



Net zoals dat een kleine afwijking in een muziekuitvoering ervoor kan zorgen dat het vals klinkt, zal zelfs de kleinste verandering in de originele gegevens resulteren in een andere hashing waarde. Dit maakt hashing een krachtig hulpmiddel om de integriteit en authenticiteit van een bitcointransactie te garanderen.

Hashing van **public keys** wordt gebruikt om de veiligheid van informatie te verbeteren door deze om te zetten in een onleesbaar formaat met een vaste lengte. Bitcoin gebruikt de SHA-256 en Ripemd-160 algoritmen om openbare adressen te produceren. De resulterende output dient als een unieke identificatie voor de public key en helpt de integriteit en veiligheid van transacties die zijn opgeslagen in het kasboek te garanderen. Door de informatie op deze manier te versleutelen, wordt het voor onbevoegden moeilijker om toegang te krijgen tot de gegevens en ze te manipuleren.



- Deterministisch**
Dezelfde ingrediënten leveren altijd dezelfde smoothie op.
- Voorafbeeldingsbestendigheid**
Je kunt geen aardbeien meer maken van een smoothie door ze aan elkaar te lijmen.
- Correlatiebestendigheid**
Als je de ingrediënten een beetje verandert, krijg je een heel andere smoothie.
- Botsingbestendigheid**
Het is moeilijk om met andere ingrediënten precies dezelfde smoothie te maken.
- Snelheid en verifieerbaarheid**
Gooi fruit in de mixer. Het gaat snel en het resultaat is zeker een smoothie.

9.2 Het UTXO Model

UTXO - Unspent Transaction Output

| De uitvoer van nog niet-bestede transacties

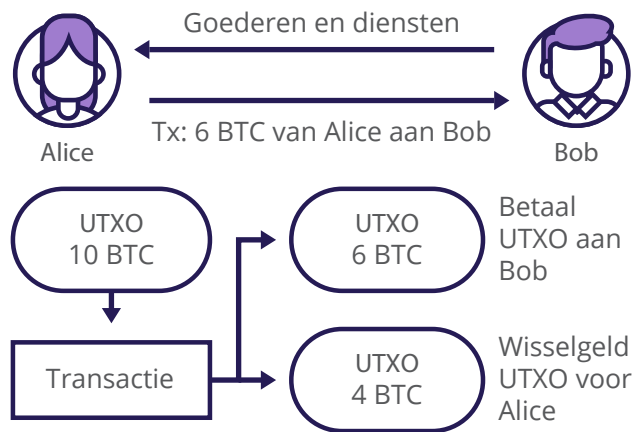


Een introductie tot de technische kant van bitcoin

Wat zijn UTXO's?

Bitcointransacties werken alsof je een groter stuk goud in kleinere stukjes breekt en deze kleinere stukjes zowel naar anderen als naar jezelf stuurt.

Je kunt UTXO's zien als bitcoin in verschillende stukjes, of als biljetten met verschillende waarden in je wallet. Als je een UTXO uitgeeft, wordt het omgezet in een nieuwe UTXO voor de ontvanger, en wat er over is wordt naar je teruggestuurd in een andere nieuwe UTXO die bekend staat als "het wisselgeld UTXO". Dit is net zoiets als wanneer je een biljet van €10 gebruikt om kopjes koffie te kopen voor €6. De winkelier houdt de €6 en geeft je €4 terug als wisselgeld.



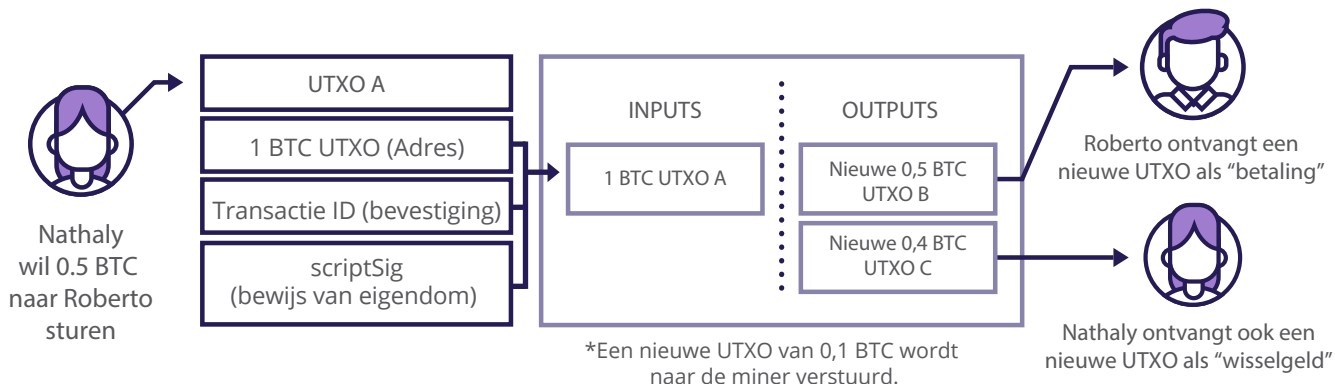
Als je bitcoin verstuurt, dan stuur je altijd het volledige bedrag van één (of meer) van je UTXO's in je wallet. Wat gebeurt er dan? Je stuurt een deel naar de ontvanger en je ontvangt het resterende bedrag terug als wisselgeld op een van de bitcoinadressen die je bezit. Het wisselgeld dat je terugkrijgt heet een UTXO (Unspent Transaction Output) en kan gebruikt worden als input voor een nieuwe toekomstige transactie.

Het saldo van je bitcoinwallet is de som van al je verschillende UTXO's. De som van je UTXO's is dus de som van de hoeveelheid bitcoin die je bezit.

Het is belangrijk om te weten dat je anderen niet op de hoogte moet stellen van je UTXO's, want als iemand je UTXO's kent, kan hij je bitcointransacties in het netwerk volgen en uiteindelijk weten hoeveel geld je bezit.



Samenvattend: elke keer dat je een transactie doet, gebruik je een of meerdere van je bestaande UTXO's om bitcoin uit te geven en worden er nieuwe UTXO's aangemaakt (voor zowel jou als de ontvanger).

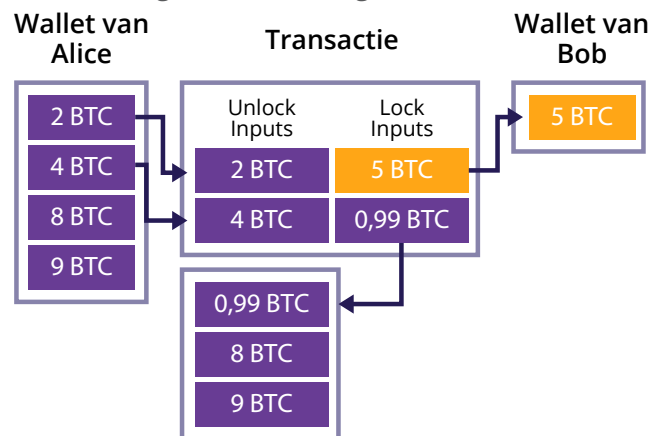


Bij elke transactie wordt de hoeveelheid bitcoin die wordt verzonden verdeeld in meerdere 'outputs', die elk worden gekoppeld aan een nieuw bitcoinadres (een nieuwe UTXO).

Als je naar iemand bitcoin verstuurt, gebruik je een of meerdere UTXO's als geldbron (input). Deze UTXO's worden, indien nodig, gecombineerd om nieuwe outputs te creëren die zowel aan de ontvanger van de transactie als aan jezelf zullen toebehoren. Deze nieuwe outputs, de UTXO's van de betaling zelf en van het wisselgeld, worden dan respectievelijk het eigendom van de ontvanger en dat van jou. Deze UTXO's kunnen dan worden gebruikt als tegoed in andere toekomstige transacties. Deze keten van UTXO's creëert een transparante en traceerbare geschiedenis van alle bitcointransacties in het bitcoinkasboek, vanaf het allereerste block (3 januari 2009).

Hier nog een voorbeeld van hoe dit werkt: als je 2 bitcoin wilt versturen maar je hebt alleen een UTXO van 5 bitcoin, dan wordt het verschil van 3 bitcoin naar je teruggestuurd als "wisselgeld". Dit wisselgeld is een nieuwe UTXO voor jou, en je kunt die nieuwe UTXO in een toekomstige transactie uitgeven.

- 1 Alice wil naar Bob 5 bitcoin sturen
- 2 Ze voegt twee van haar UTXO's samen tot 6 BTC
- 3 Van deze UTXO's, stuurt ze 5 BTC naar Bob, ontvangt ze 0,99 bitcoins "wisselgeld", en moet ze 0,01 BTC transactiekosten betalen.
- 4 Na de bevestiging wordt de transactie toegevoegd aan het bitcoinkasboek op alle bitcoinnodes



Stel dat Alice probeert om een van haar al uitgegeven UTXO's te gebruiken om een andere transactie te doen, dan wordt dit automatisch afgewezen door de nodes. Dit komt omdat de nodes een kopie van het bitcoinkasboek (en alle transacties) bijhouden, zodat ze gemakkelijk het saldo van de UTXO's van Alice kunnen controleren en kunnen bevestigen dat de transactie niet geldig is.

Hieronder zie je een screenshot van een echte transactie met slechts één invoer. In een ander geval kan het startsaldo echter de som zijn van meerdere UTXO's. Welke opmerkingen kun je maken als je naar de twee onderstaande transacties kijkt? Komen de inputs overeen met de outputs? Kun je de details van de transactie beschrijven? Is er een verband tussen de twee screenshots? En welke transactie vond als eerste plaats?



Een introductie tot de technische kant van bitcoin

9.3 Bitcoinnodes en miners nader bekeken

In dit gedeelte gaan we dieper in op twee zeer belangrijke onderdelen (en deelnemers) van het bitcoinnetwerk die voor het eerst werden geïntroduceerd in Hoofdstuk 6. We zullen kijken naar:



Bitcoinnodes:

Dit zijn poortwachters van het bitcoinnetwerk houden een kopie bij van het bitcoinkasboek, zorgen ervoor dat alle transacties geldig zijn en dat iedereen dezelfde regels volgt.

Door deze taak over nodes wereldwijd te verspreiden, blijft bitcoin beschermd tegen potentiële problemen. Bitcoinnodes helpen het systeem betrouwbaar te houden en trouw te blijven aan het gedecentraliseerde idee, waarbij geen enkele persoon of groep te veel macht heeft.



Bitcoinminers:

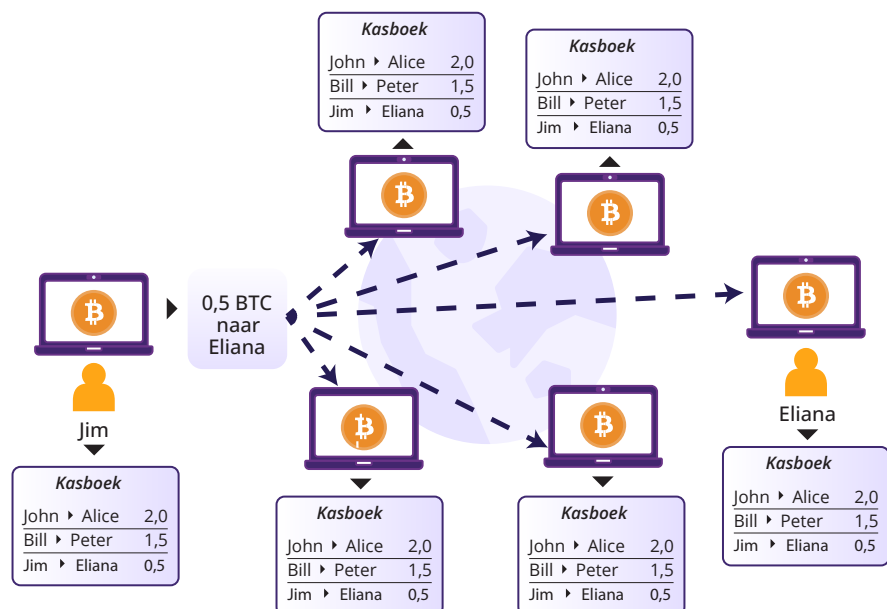
Dit zijn de architecten van de veiligheid en gebruiken krachtige computers en elektriciteit om transacties te controleren en te bevestigen, zodat het netwerk veilig gebruikt kan worden. Dit helpt het kasboek, of blockchain, bestand te maken tegen slechte actoren die de boel proberen te manipuleren.

Samen werken bitcoinnodes en -miners als een team om een gedecentraliseerd, veilig en sterk systeem in stand te houden - een nieuwe manier om met geld om te gaan waar mensen over de hele wereld op kunnen vertrouwen. Laten we deze rollen in meer detail bekijken om te begrijpen op welke manier ze bijdragen.

9.3.1 Wat is een bitcoinnode en hoe zet ik er een op?

Een bitcoinnode klinkt misschien technisch, maar het is gewoon een stukje software waarop een kopie van het bitcoinkasboek draait. Als je je eigen bitcoinnode draait, krijg je een stem in het vormgeven van de regels van het bitcoinnetwerk.

Stel je dit eens voor: als een groep mensen bitcoin probeert te veranderen, bijvoorbeeld door de totale hoeveelheid van bitcoin te veranderen, dan heb jij inspraak. Je kunt ervoor kiezen om de software van je node niet aan te passen aan het nieuwe systeem, wat hetzelfde is als stemmen voor de regels die jij wel ondersteunt.



Laten we ons een bitcoinnode voorstellen als een digitale verkeersagent met een aantal essentiële taken:

Poortwachters van de validatie:

1

Een bitcoinnode houdt een digitale kopie bij van de blockchain, wat een gedistribueerd kasboek is van alle bitcointransacties. Nodes over de hele wereld bewaren ditzelfde kasboek.

2

Communicatiehub:

Nodes verbinden zich met elkaar en creëren zo een uitgebreid communicatienetwerk. Ze delen informatie, vooral transacties die wachten om aan de blockchain te worden toegevoegd. Deze transacties worden opgeslagen in een digitale wachtkamer die "de mempool" wordt genoemd, tot een miner ze verwerkt in een block.

3

Kwaliteitschecker:

Elke toevoeging aan de blockchain wordt kritisch bekeken. Nodes controleren de geldigheid van transacties en wijzen ze af als ze niet voldoen aan de regels van het bitcoinnetwerk.

4

Blockchain Informant:

Andere software, zoals wallets, kunnen een node om informatie vragen over de blockchain, zoals bitcoin balansen. Nodes dienen hierbij als informatiehubs.

5

Nieuwe nodes verwelkomen:

Wanneer een nieuwe node zich wil aansluiten aan het netwerk, stellen al aangesloten nodes een kopie van de blockchain ter beschikking. De nieuwe node controleert onafhankelijk van de rest de geldigheid van elke transactie, wat een vertrouwensloos systeem benadrukt.

Activiteit: Bekijk een video over bitcoinnodes



Een van de opties om je eigen node te draaien is om de Bitcoin Core software te installeren en het wat tijd te geven om de hele blockchain te downloaden. Zodra dit proces voltooid is, kun je de software laten draaien, waarna er elke 10 minuten nieuwe blocks met transacties verschijnen. Je node controleert de geldigheid en voegt de nieuwe blocks toe aan je lokale kopie van de blockchain.

Bron:
Bitcoin Core
Software



Het runnen van een node biedt soevereiniteit en onafhankelijkheid. Je bent niet afhankelijk van anderen; het is je eigen verkeersagent. In tegenstelling tot je bitcoinwallet, die geen kopie van de blockchain heeft, zorgt een node voor zelfvoorziening. In plaats van anderen te vertrouwen wat betreft je bitcoinbezit (en de staat van het bitcoinnetwerk), kan je wallet met je persoonlijke node communiceren, waardoor je digitale ervaring veiliger en betrouwbaarder is.

9.3.2. Wat is een bitcoinminer en hoe werkt mining?

Het doel van mining is niet het creëren van nieuwe bitcoin. Dat is de stimulans. Mining is het mechanisme waarmee de veiligheid van bitcoin wordt gedecentraliseerd

Andreas M. Antonopoulos

Een introductie tot de technische kant van bitcoin

Miners verzamelen onbevestigde transacties, vormen een block en besteden energie om een waardevolle sleutel te vinden waarmee het block aan de blockchain kan worden toegevoegd. Deze investering van energie beveiligt het netwerk tegen kwaadwillende actoren.



Miners racen tegen elkaar om het volgende block aan de blockchain toe te voegen. Ze zoeken de "juiste block hash," die slim verborgen is tussen miljarden anderen. Stel je een enorme hooiberg voor, gevuld met miljoenen sleutels die elk een unieke hash van een block vertegenwoordigen. Het protocol heeft één specifieke sleutel gekozen die een waardevolle beloning vrijspelt. Miners doorzoeken de hooiberg en testen elke sleutel om te zien of deze in het slot past, maar slechts één gelukkige miner zal als eerste de perfecte match ontdekken.

Zodra een miner de juiste block hash heeft gevonden, deelt hij deze met het netwerk samen met het door hem aangemaakte block met nieuwe transacties. Andere miners verifiëren de oplossing om er zeker van te zijn dat het klopt. Als alles klopt, wordt het block toegevoegd aan de blockchain, waardoor een veilig en openbaar kasboek ontstaat.

Miners verdienen op twee manieren beloningen voor hun inspanningen:

- 1 Block rewards
- 2 Transactievergoedingen

Block rewards zijn nieuwe bitcoin die in omloop worden gebracht bij elk block dat aan de blockchain wordt toegevoegd. Transactievergoedingen zijn kleine bitcoinbetalingen die gebruikers doen om hun transacties prioriteit te geven en sneller verwerkt te laten worden door miners. Miners kunnen kiezen welke transacties ze opnemen in het block dat ze minen, waarbij ze meestal de voorkeur geven aan transacties met hogere transactiekosten.

Bitcoin halvings

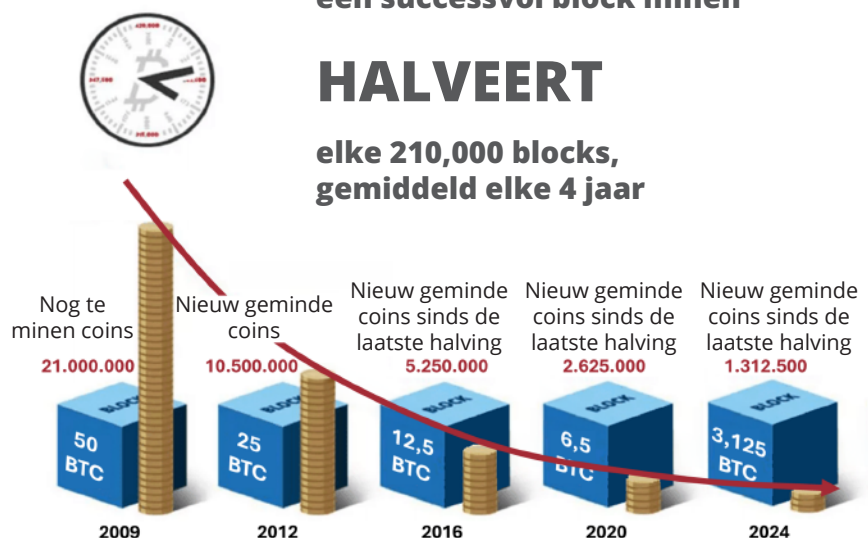
De bitcoin halving is cruciaal voor het behoud van de schaarste en waarde van bitcoin. Er bestaat een limiet van 21 miljoen bitcoins, die niet in één keer beschikbaar waren bij de lancering, maar geleidelijk vrijkomen. Satoshi Nakamoto ontwierp het ingenieuze systeem van de block reward om nieuwe bitcoins te verdelen zonder dat een centrale autoriteit dit kan manipuleren. In de begintagen van Bitcoin kregen miners een beloning van 50 bitcoins voor het minen van elk block, wat hen motiveerde om te investeren in krachtige apparatuur en de benodigde elektriciteit voor hun miningactiviteiten.

Om het netwerk stabiel te houden en het aanbod van nieuwe bitcoin onder controle te houden, wordt de block reward elke 210.000 blocks gehalveerd. Deze gebeurtenis, die "de halving" wordt genoemd, vermindert het aantal nieuwe bitcoin dat in omloop komt maar blijft miners motiveren om het netwerk te beschermen, en de decentralisatie in stand te houden. Historisch gezien hebben halvings geleid tot aanzienlijke prijsstijgingen op de bitcoinmarkt vanwege het verminderde aanbod van nieuwe bitcoins.

De beloning voor miners die een succesvol block minen

HALVEERT

elke 210,000 blocks,
gemiddeld elke 4 jaar

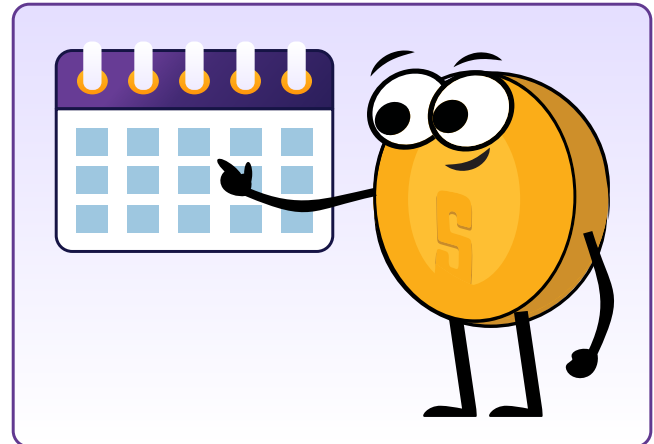


De omloopvoorraad (circulating supply) verwijst naar de totale hoeveelheid van een valuta die in circulatie is gebracht. Bij bitcoin is de omloopvoorraad het aantal munten dat is gemined en op een bepaald moment in omloop is, exclusief munten die voor altijd verloren zijn gegaan.



Na elke halving wordt door het protocol per block minder bitcoin in omloop gebracht, waardoor miners kleinere beloningen krijgen. Deze vermindering van de block reward betekent niet per se dat miners minder winst zullen maken, omdat ze ook transactiekosten kunnen verdienen voor het verifiëren van transacties en het toevoegen ervan aan de blockchain. Dit kan de vermindering van de block rewards compenseren.

Halvings zijn voorgeprogrammeerd in het bitcoinprotocol, waardoor het aanbodschaam van bitcoin voorspelbaar en transparant is

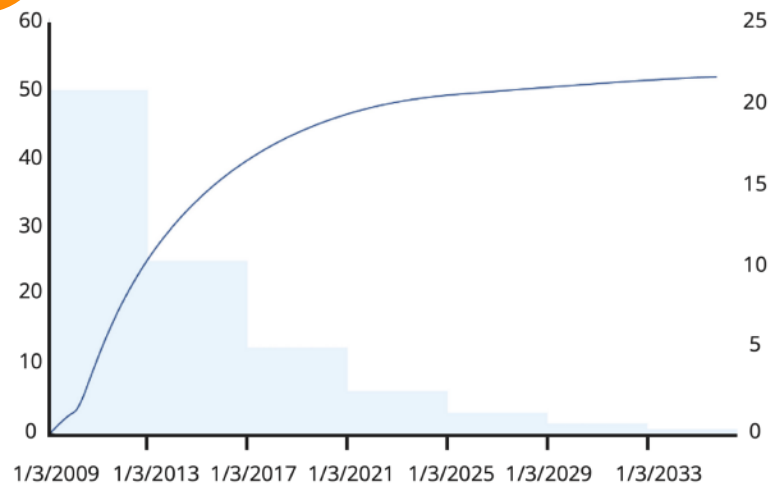


Het bitcoin aanbodschaam is het vooraf bepaalde en openbare plan voor het in omloop brengen van nieuwe bitcoin, ontworpen om de schaarste van bitcoin in de loop van de tijd te handhaven.



De volgende tabel geeft een overzicht van de komende halvings voor bitcoin, de verwachte datum van de volgende halvingsgebeurtenis, het blocknummer waarop de halvingsgebeurtenis zal plaatsvinden, de block rewards (per gemined block) vanaf die halvingsgebeurtenis en het percentage van de voorraad dat minimaal gemined zal zijn.

Het bitcoin aanbodschaam



Gebeurtenis	Verwachte datum	Block	Block Reward	Percentage gemined
Vierde halving	2024	840,000	3.125	96.875 %
Vijfde halving	2028	1,050,000	1.5625	98.4375 %
Zesde halving	2032	1,260,000	0.78125	99.21875 %

Een introductie tot de technische kant van bitcoin

Naarmate er meer bitcoin wordt gemined, zal de omloopvoorraad en het percentage van de totale voorraad dat gemined is, blijven toenemen totdat het totale aanbod van 21.000.000 is bereikt. Het afnemende aanbod van nieuwe coins, in combinatie met een stijgende vraag, kan de prijs van bitcoin (gemeten in euros) opdrijven. Dit is in het voordeel van vroege gebruikers (early adopters) en motiveert miners om door te gaan met het beveiligen van het netwerk en het inzetten van hun rekenkracht en middelen.

Percentage van de 21M geminde bitcoins



Wat is een geldige block hash in bitcoin?

In bitcoin is een geldige block hash als een speciale code die miners proberen te vinden. Het is een uniek nummer dat helpt bij het bijhouden van elk block in de blockchain, waarin informatie over transacties wordt opgeslagen. De blocks vormen zich in een keten, van het eerste (genesis block) tot het laatste block, waardoor een openbaar verslag ontstaat van alle transacties. Deze hashing van een block is cruciaal omdat het elk block koppelt aan het block ervoor, waardoor het voor iedereen mogelijk is om de geschiedenis van alle transacties te controleren. Het is een beetje zoals een vingerafdruk voor elk block, die ervoor zorgt dat de informatie correct en veilig is. Met andere woorden, de hash van het block is een manier om te bevestigen dat de gegevens in het block niet zijn veranderd.



Satoshi Nakamoto, de uitvinder van bitcoin, mineerde het eerste block, dat in totaal 50 bitcoins bevatte.

De race om een block te minen

Miners gaan een wedstrijd aan om de hash van het block te vinden die overeenkomt met het doel (een speciaal nummer) dat door het netwerk is ingesteld. De miner die als eerste met succes de juiste hash van het block ontdekt, krijgt de mogelijkheid om dat block aan de blockchain toe te voegen en het de bijbehorende hash ID te geven. Deze oplossing dient als validatie voor de authenticiteit van het block.



Mining kan vergeleken worden met een race waarbij het doel is om zo snel mogelijk de finish te bereiken. De moeilijkheid om de hash van het block te vinden, wordt periodiek aangepast, zodat elk block in ongeveer 10 minuten wordt gemined (om te compenseren voor een toe- of afnemend aantal miners). Dit mechanisme wordt de "difficulty adjustment" genoemd.



Laten we zeggen dat het doelgetal dat door het bitcoinprotocol is ingesteld 1000 is. De miners moeten dan hun rekenkracht en energie gebruiken om een block hash (een specifiek getal) te zoeken dat lager is dan 1000. De eerste miner die een block hash vindt dat lager is dan 1000 mag het nieuwe block toevoegen aan de blockchain en wordt beloond met bitcoin.

De moeilijkheidsgraad in bitcoinmining is een maat voor hoe moeilijk het is om een geldige hash van een block te vinden dat voldoet aan het doel dat het protocol heeft gesteld. De moeilijkheidsgraad wordt elke 2016 blocks aangepast, wat ongeveer elke twee weken is, om ervoor te zorgen dat blocks in een vast tempo aan de blockchain worden toegevoegd. Zonder deze difficulty adjustment zouden blocks steeds sneller gevonden worden naarmate meer miners naar de block hash gaan zoeken. De moeilijkheidsgraad wordt uitgedrukt als een getal en hoe hoger de moeilijkheidsgraad, hoe moeilijker het is om een geldige hash van een block te vinden.

Neem bijvoorbeeld deze twee verschillende hashes:

-  Hash 1: 0000A1mINgF0RbL0cK5wltHth3hAy5tAcK
Moeilijkheidsgraad: 1
-  Hash 2: 00000000A1mINgF0RbL0cK5wltHth3hAy5tAcK
Moeilijkheidsgraad: 2

In dit voorbeeld heeft Hash 2 een hogere moeilijkheidsgraad dan Hash 1, omdat het een langere hash is met meer nullen aan het begin. Het is moeilijker voor miners om Hash 2 te vinden omdat hun computers meer werk moeten verrichten.

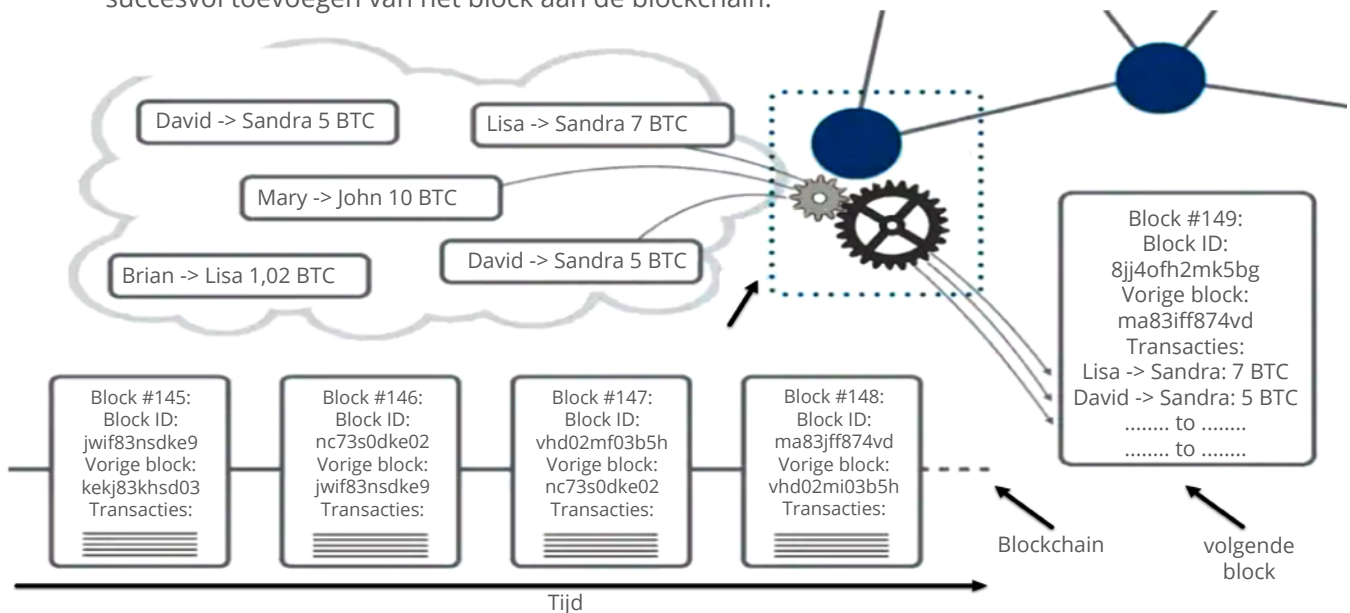
Door een geldige hash van een block te vinden, bewijst een miner dat hij het werk heeft gedaan dat nodig is om het nieuwe block aan de blockchain toe te voegen en krijgt hij een beloning in bitcoin, plus transactiekosten voor zijn inspanning. Deze methode die het bitcoinnetwerk gebruikt om transacties te valideren en nieuwe blocks aan de blockchain toe te voegen heet Proof-of-Work (PoW).

Een introductie tot de technische kant van bitcoin

PoW maakt bitcoin veilig door het moeilijk te maken voor iemand met kwade bedoelingen om de controle over te nemen, waardoor het bitcoinnetwerk veilig te gebruiken is.

Samengevat bestaan de taken van miners uit:

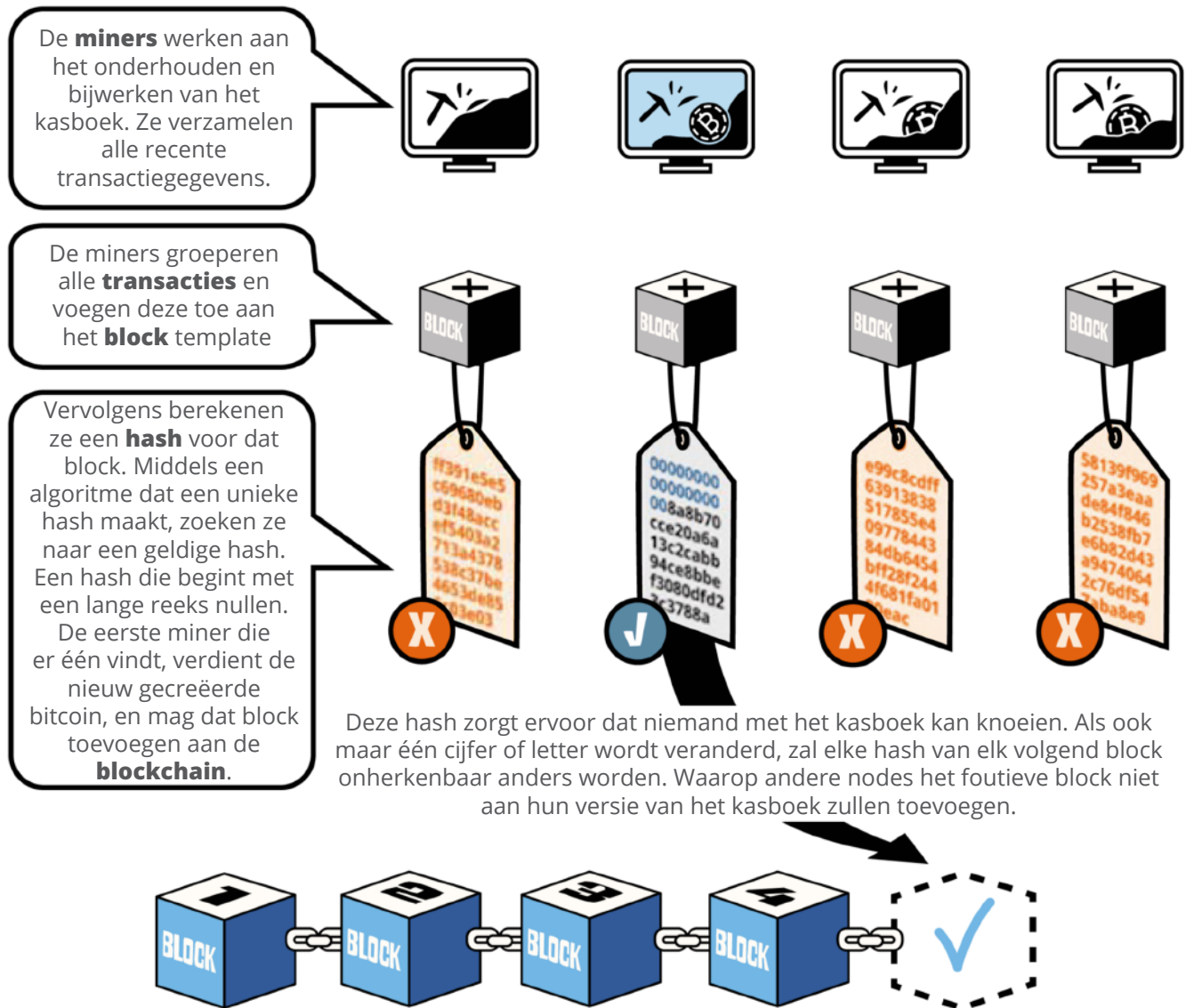
- 1 Het bundelen van transacties in blocks:
Nodes verifiëren nieuw aangemaakte transacties die wachten in de mempool. De miners selecteren een subset hiervan om op te nemen in een toekomstig te minen "block template".
- 2 Proof-of-Work:
Miners concurreren met elkaar om de geldige hash van het block te vinden.
- 3 Geldige blocks broadcasten:
Na het vinden van de geldige blockhash, zenden miners het nieuwe block uit naar het netwerk
- 4 Beloningen verdienen:
Tot slot ontvangen miners nieuw gecreëerde bitcoins (block subsidy) en transactiekosten voor het succesvol toevoegen van het block aan de blockchain.



Meerdere miners werken tegelijkertijd aan het creëren van nieuwe blocks. De eerste miner die een block hash ontdekt die voldoet aan de eisen van het netwerk, deelt dit met het netwerk. De andere miners controleren dan de transacties in het template block van die miner om er zeker van te zijn dat ze geldig zijn. Als de transacties inderdaad geldig zijn, wordt het block toegevoegd aan de blockchain. De andere blocks die op dat moment door de andere miners zijn gemaakt worden weggegooid. Dit proces helpt de consensus binnen het netwerk te behouden en voorkomt "dubbel uitgeven" van UTXO's.

Een template block is een block met een set transacties dat overwogen wordt om aan de blockchain toegevoegd te worden, maar nog niet toegevoegd is.





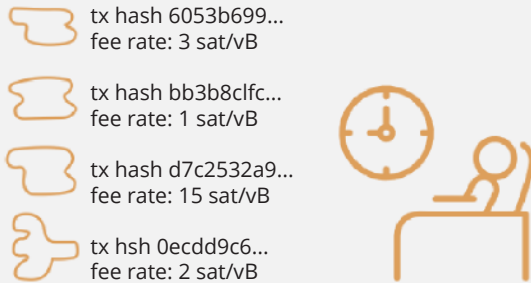
9.4 Wat is de mempool?

De "Mempool" of Memory Pool is als een wachtkamer voor transacties in het bitcoinnetwerk. Wanneer je een transactie doet, wordt deze eerst uitgezonden naar de mempool en kunnen miners besluiten of ze deze transactie toevoegen aan een nieuw block. Vervolgens controleren de bitcoinnodes of de transacties in dit nieuwe block voldoen aan de consensusregels.

Stel je voor dat je in de rij staat bij een restaurant en je naam wordt toegevoegd aan een lijst van mensen die staan te wachten. Als er een tafel vrijkomt, roept de gastheer je naam en geeft je een plaats. Op dezelfde manier komt een bitcointransactie in de mempool. De transactie wordt toegevoegd aan de blockchain wanneer een miner besluit deze op te nemen in een block.

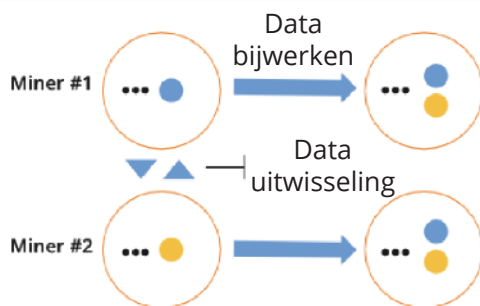
Een introductie tot de technische kant van bitcoin

In de **mempool** wachten transacties tot ze worden bevestigd in een block.



Wanneer een node een transactie ontvangt van een peer, moet deze eerst verifiëren of de transactie legitiem is.

Mempoolsynchronisatie stelt nodes in staat om hun transacties te delen met andere nodes door ze een bericht te versturen met een lijst van geverifieerde transacties in de mempool.



Het belangrijkste doel van een mempool is om:

1

Niet-bevestigde transacties door te geven



2

Miners transacties te geven om te minen.



De Accept To Memory Pool (ATMP) stelt nodes in staat om transacties te ontvangen, te valideren en toe te voegen aan hun mempool. Het controleert:

- Heb ik deze transactie al?
- Is er een conflict met een andere transactie in de mempool?
- Komen de ingaande en uitgaande hoeveelheid bitcoin overeen?
- Bewijzen de handtekeningen dat de vorige UTXO kan worden uitgegeven?
- Is de vergoeding (fee) hoog genoeg?

Hoe worden transacties geverifieerd en toegevoegd aan de mempool?

Wanneer nieuwe transacties worden verzonden naar het bitcoinnetwerk, verifiëren nodes deze transacties om er zeker van te zijn dat ze geldig zijn en dat het geld niet eerder is uitgegeven. Zodra deze transacties zijn geverifieerd, voegen de nodes ze toe aan hun mempool. Vervolgens delen de nodes de transacties met andere nodes om ze dubbel te controleren. Als de meerderheid van de nodes akkoord gaat, worden de transacties beschikbaar gesteld aan miners, die kunnen selecteren welke transacties ze opnemen in een block.

Soms komt het voor dat transacties niet bevestigd of geweigerd worden. Dit kan veroorzaakt worden door:

- 1 Te lage transactiekosten:
Transacties met een lage vergoeding worden mogelijk niet snel genoeg verwerkt, omdat miners geneigd zijn om de transacties met hogere vergoedingen eerder op te nemen in hun blocks.
- 2 Netwerkgestoei:
Bij een overbelast netwerk kan het bevestigen van transacties traag zijn, zelfs bij een hoge vergoeding.
- 3 Poging tot double spend:
Als een kwaadwillende een 'double spend' tracht uit te voeren, kan die transactie worden geweigerd.
- 4 Onjuiste of onvolledige gegevens:
Als een transactie onjuiste of onvolledige gegevens bevat, kan deze worden geweigerd.
- 5 Misvormde transactie:
Als een transactie incorrecte gegevens bevat, kan deze geweigerd worden door het netwerk.

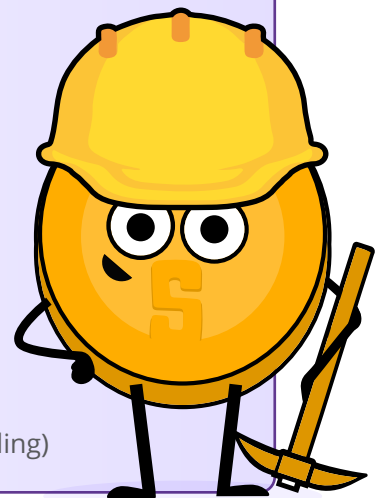
Om te voorkomen dat transacties worden geweigerd, is het aan te raden om een vergoeding aan te bieden die hoog genoeg is zodat de transactie tijdig wordt verwerkt. Controleer ook altijd minstens twee keer of alle gegevens in de transactie correct zijn voordat je deze verstuurt.

Activiteit: mempool

- 1 Scan de volgende QR code:
- 2 Bekijk de verschillende elementen die op de pagina worden weergegeven, waaronder de laatste blocks, bevestigde transacties, het aantal transacties, geheugengebruik en de geschatte waarde van het hele block. Beantwoord de vragen:



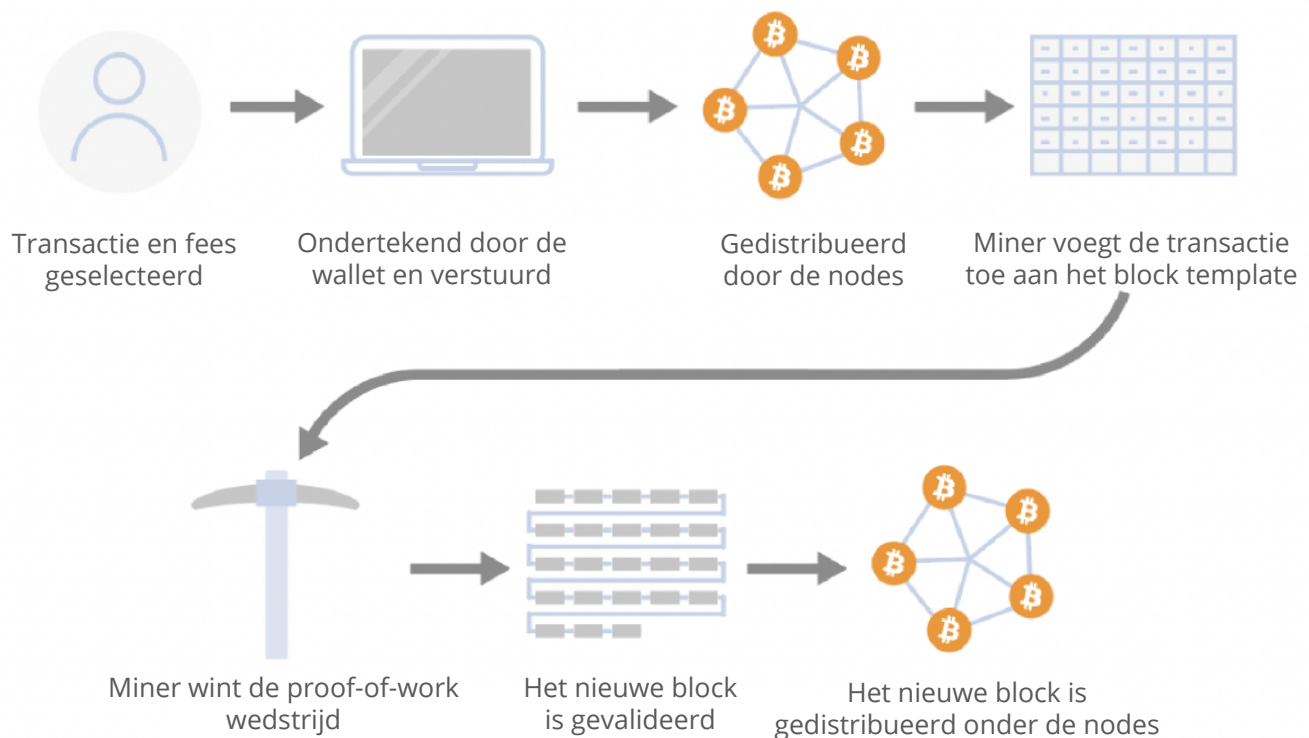
- ☀ Wat was het laatst geminede block?
- ☀ Hoeveel transacties zaten er in dat block?
- ☀ Wat is de totale waarde die in bitcoin wordt verhandeld?
- ☀ Wat was de grootte van het block in megabytes?
- ☀ Hoeveel bitcoin heeft de miner in totaal verdiend?
- ☀ Wat was de totale waarde van de vergoedingen die de miner ontving voor het toevoegen van de transacties aan het netwerk?
- ☀ Kies de transactie met de hoogste waarde.
Over hoeveel bitcoinadressen werd het bedrag verdeeld?
- ☀ Met hoeveel nullen begint de nonce van het block?
(De nonce is een willekeurig getal dat aan een block header wordt toegevoegd om een hash te maken die voldoet aan de moeilijkheidsdoelstelling)



Een introductie tot de technische kant van bitcoin

9.5 Hoe bitcointransacties van begin tot eind werken

- 1 Adam wil bitcoin naar Peter sturen. Hij kiest een van zijn UTXO's, maakt een transactie aan en voegt alle benodigde details toe, waaronder de hoeveelheid bitcoin die hij wil versturen, Peter's ontvangende adres en een bovengemiddeld bedrag aan transactiekosten.
- 2 Na een laatste controle of alle details kloppen, gebruikt Adam zijn private key om de transactie te ondertekenen.
- 3 Adam verzendt (broadcast) de transactie naar het bitcoinnetwerk



Van: Stevenot, Ted, "What is a bitcoinnode and how does one work?". *Unchained Capital*, 17, January, 2023, <https://unchained.com/blog/what-is-a-bitcoin-node/>

- 4 De nodes op het netwerk ontvangen de transactie en verifiëren de geldigheid ervan volgens de consensusregels (zoals de geldigheid van Adams handtekening en of hij voldoende bitcoin heeft om de transactie uit te voeren).
- 5 De transactie wordt als geldig gemarkeerd en de nodes propageren het naar andere nodes op het netwerk, waarna ze het toevoegen aan de mempool.
- 6 Omdat Adam een transactievergoeding (fee) heeft gekozen die hoog genoeg is, nemen bijna alle miners zijn transactie op in hun blocks.

7

Proof-of-work: miners proberen hun block te minen door de geldige hash van het block als eerste te vinden. Een van de miners vindt de hash en zendt zijn block uit naar het netwerk.

8

De nodes ontvangen het nieuwe block en verifiëren de geldigheid ervan. Dit houdt in dat alle transacties in het block worden gevalideerd en dat het proof-of-work wordt gecontroleerd.

9

De meerderheid van de nodes is het ermee eens dat het block geldig is en voegt het toe aan de blockchain. Peter ontvangt de bevestigde (confirmed) bitcoin op zijn ontvangstadres.

10

Naarmate er in het daaropvolgende uur meer blocks aan de blockchain worden toegevoegd, groeit het aantal bevestigingen van de transactie. Naarmate het aantal bevestigingen toeneemt, krijgt Peter meer vertrouwen dat het gelukt is en dat de transactie niet meer omkeerbaar is.

Samengevat ondertekent de verzender de transactie met zijn private key, de nodes verifiëren de transactie-UTXO's en de miners voegen de geverifieerde transactie toe aan de blockchain. De ontvanger heeft dan toegang tot de bitcoin met zijn of haar private key. Zodra een block is gemined, worden alle transacties die er deel van uitmaken als bevestigd beschouwd en de UTXO's die als inputs in deze transacties zijn gebruikt, worden als uitgegeven beschouwd en zullen niet opnieuw worden gebruikt.



In dit hoofdstuk heb je waardevolle inzichten gekregen over de fundamentele concepten van de werking van bitcoin. We hebben essentiële aspecten behandeld, van de basis van geld tot de technische kant van de bitcointechnologie. Laten we het nu allemaal samenvoegen in hoofdstuk 10, waarin we dieper ingaan op de belangrijke vraag: "Waarom bitcoin?"