

Hoofdstuk #7

Hoe gebruik ik bitcoin?

7.0 Inleiding

7.1 Bitcoin verkrijgen en ruilen

7.1.1 P2P: persoonlijk in de echte wereld

7.1.2 P2P: online

7.1.3 Gecentraliseerde exchanges

7.2 Bitcoinwallets, een introductie

7.2.1 Self-custodial vs custodial wallets

7.2.2 Verschillende typen bitcoinwallets

7.2.3 Open-source vs closed-source

Activiteit: evaluatie van bitcoinwallets

7.3 Een mobiele bitcoinwallet instellen

Activiteit: een bitcoinwallet opzetten/herstellen

7.4 Transacties ontvangen en versturen

Activiteit: bitcointransacties in de praktijk

7.5 Sparen in bitcoin

7.6 Don't trust, verify

Hoe gebruik ik bitcoin?

7.0 Inleiding

Waarom zou iemand nergeld in plaats van centralebankgeld vertrouwen? Nerds brachten jullie het internet. Banken brachten je de grote depressie.

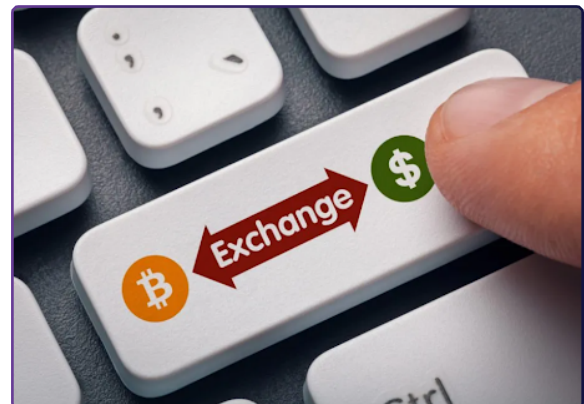
Andreas M. Antonopoulos

Nu we beter begrijpen wat bitcoin is en waar het voor dient, is het tijd om te leren hoe je het in de praktijk kunt gebruiken. In dit hoofdstuk begeleiden we je stap voor stap door het proces van het verkrijgen van bitcoin, verkennen we de verschillende soorten wallets die beschikbaar zijn, helpen we je bij het opzetten van je eigen bitcoinwallet en oefenen we zelfs met het versturen en volgen van een bitcointransactie op het netwerk. Het is tijd om je kennis toe te passen.

7.1 Bitcoin verkrijgen en ruilen

Er zijn veel manieren om bitcoin te verwerven en te spenderen. Je kunt bijvoorbeeld:

- betaald krijgen in bitcoin in ruil voor je werk, en ermee betalen voor producten en diensten van anderen. (Meer hierover in hoofdstuk 8)
- bitcoin minen (meer daarover in hoofdstuk 9)
- met iemand persoonlijk je fiatgeld omruilen voor bitcoin, of andersom.
- je fiatgeld online omwisselen voor bitcoin, of andersom



Hieronder zullen we het omwisselen van fiatgeld voor bitcoin en vice versa bespreken, zowel via persoonlijke transacties als online methoden, omdat dit de meest voorkomende opties zijn.

7.1.1 Peer-to-peer: persoonlijk in de echte wereld

Bij peer-to-peer (P2P) aan- of verkooptransacties van bitcoin ruil je fiatgeld (of een ander goed of dienst) direct voor bitcoin met een ander individu, zonder tussenkomst van een bank of een andere partij.

Beide partijen bepalen samen het wisselbedrag en de koers. De ene persoon levert het fiatgeld, de andere draagt de bitcoin over en de transactie is afgerond. Hoewel het gemakkelijker is om peer-to-peer transacties fysiek uit te voeren door de andere persoon rechtstreeks in de echte wereld te ontmoeten, kun je dit dankzij het internet ook vrijwel overal doen.



7.1.2 Peer-to-Peer: online

Maak kennis met peer-to-peer platformen, waar kopers en verkopers van bitcoin elkaar ontmoeten om rechtstreeks transacties met elkaar uit te voeren zonder tussenpersonen.

Bij zulke platformen hoef je niemand je informatie of geld toe te vertrouwen, je kunt andere peers ontmoeten en rechtstreeks met hen handelen.



Op de meeste peer-to-peer platformen moeten peers een deel van het geld in “escrow” plaatsen om er zeker van te zijn dat ze hun deel van de deal nakomen. Escrow betekent dat het geld tijdelijk op een veilige plaats wordt vastgezet, in beheer van het platform. Als een van de partijen niet meewerkt met de deal, krijgt de ander zijn vastgezette bedrag terug. Het is als een vertrouwde vriend die de spullen bewaart tot aan de afgesproken voorwaarden is voldaan

7.1.3 Gecentraliseerde exchanges

Het gebruik van gecentraliseerde exchanges is voor velen de gemakkelijkste manier om bitcoin te kopen en verkopen, maar het brengt ook aanzienlijke nadelen met zich mee. Gecentraliseerde exchanges zijn bedrijven die klanten toestaan om bitcoin direct via hen te kopen en verkopen. Aan dit gemak hangt echter een prijskaartje.



Gecentraliseerd

Afwegingen bij gecentraliseerde exchanges

Het is belangrijk om te weten dat als je bitcoin koopt via een gecentraliseerde exchange, je vaak persoonlijke informatie moet verstrekken en je identiteit moet verifiëren. Dit creëert een risico op identiteitsdiefstal en stelt je persoonlijke informatie bloot aan potentiële bedreigingen. Bovendien bewaren gecentraliseerde exchanges je bitcoin, wat betekent dat je geen controle hebt over je geld totdat je het bij hen opneemt.

Erger nog, gecentraliseerde exchanges kunnen het geld van gebruikers verduisteren of meer bitcoin uitlenen dan ze aan reserves hebben, totdat ze instorten. Ja, net als banken! Maar in de bitcoinwereld is er geen centrale bank die frauduleuze banken kan redden door meer geld bij te drukken, want bitcoin kan niet worden bijgedrukt!

Hoe gebruik ik bitcoin?

7.2 Bitcoinwallets, een introductie

In tegenstelling tot fysiek geld zijn bitcoins niet daadwerkelijk aanwezig in een bitcoinwallet. Ze leven in het gedistribueerde kasboek (ledger) dat het bitcoinnetwerk voortdurend verifieert en beveiligt. Dus hoe kun je dan bitcoin bezitten?

Je bent pas eigenaar van je bitcoin als je de private keys (privésleutels) bezit waarmee je transacties kunt ondertekenen, want met deze private keys kan je het eigendom van jouw bitcoin aan iemand anders overdragen. Dit is het versturen van bitcoin.

Laten we, met dat in gedachten, eens kijken naar 2 concepten die we beschrijven als we de term "wallet" gebruiken:



- Een master private key (wat lijkt op een wachtwoord) waarmee je public keys (publieke sleutels) genereert die je met anderen kan delen om bitcoins te ontvangen en versturen.
- De mobiele of desktop-interface waarmee je kunt communiceren met het bitcoinnetwerk om je bitcoinsaldo op te vragen, transacties te versturen of ontvangen, en om ze te presenteren aan het netwerk. In de volgende paragraaf worden verschillende soorten wallets beschreven, samen met hun voor- en nadelen.

7.2.1 Self-custodial vs custodial wallets

Voordat we ingaan op de details van de verschillende soorten bitcoinwallets en hun kenmerken, maken we een belangrijk onderscheid tussen self-custodial en custodial wallets. Self-custodial wil zeggen dat de gebruiker de private keys bezit en dus dat de bitcoin echt zijn/haar bezit is. Bij een custodial wallet bezit een derde partij de bitcoin. De onderstaande tabel benoemt de voordelen en risico's van elk type wallet.

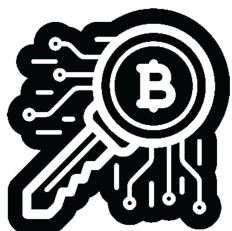
Wallet type	Wie beheert mijn bitcoin?	Voordelen	Risico's
Self-custodial wallets	De gebruiker	Volledige controle over tegoeden en transacties, geen goedkeuringsproces of bevrozing van rekeningen mogelijk, geen controle door bedrijven of overheden, beschermd tegen willekeurige inbeslagname, alsof je je geld thuis bewaart.	Geen herstel als de herstelzin verloren gaat, minder klantenondersteuning, de volledige verantwoordelijkheid ligt bij de gebruiker.
Custodial wallets	Een derde partij	Eenvoudig herstel als de toegang verloren is gegaan, eenvoudigere klantenondersteuning	Tegoeden zijn altijd verbonden met het internet en dus kwetsbaarder voor hacking en inbreuken. Beheerders kunnen rekeningen bevriezen.

Bij een self-custodial wallet (ook wel non-custodial genoemd) ben jij de enige met de sleutels van de wallet en heb je daarmee de volledige controle. Bij een custodial wallet heeft iemand anders de sleutels in bezit en heeft men toegang tot de inhoud van je wallet.

- Self-custody is alsof je je eigen bank bent. Transacties zijn niet onderworpen aan controle door een overheid of bedrijf, maar het betekent ook dat je de volledige verantwoordelijkheid draagt voor het veilig houden van je bitcoin.
- Self-custody zorgt ervoor dat anderen je bitcoin niet in beslag kunnen nemen zonder je medewerking.
- Self-custody geeft gemoedsrust in tijden van onzekerheid, omdat je weet dat je bitcoin veilig is.

Het is belangrijk om het juiste type wallet te kiezen voor je persoonlijke behoeften. Soms vinden mensen het moeilijk om onderscheid te maken tussen een self-custodial of een custodial wallet. Deze tabel laat de verschillen in het installatieproces zien.

Wallet type	Stap 1: kies een wallet	Stap 2: installeer de wallet	Stap 3: maak een nieuwe wallet	Stap 4: beveilig je herstelzin	Stap 5: gebruik je wallet
Self custodial wallets	Kies een self-custodial walletaanbieder	Volg de instructies van de walletaanbieder	Genereer een herstelzin (seed phrase) en ten minste één private key	Bewaar de herstelzin (seed phrase) op een veilige locatie	Gebruik je wallet om bitcoin te ontvangen en te versturen
Custodial wallets	Kies een custodial walletaanbieder	Volg de instructies van de walletaanbieder	Maak een account aan bij de walletaanbieder	n.v.t. (de walletaanbieder beheert immers de private keys)	Gebruik je wallet om bitcoin te ontvangen en te versturen



"Not your keys, not your coins" is een populair gezegde onder bitcoinbezitters. Het verwijst naar het idee dat, als je geen directe controle hebt over de private keys die gekoppeld zijn aan je bitcoinwallet, je niet echt de eigenaar bent van die bitcoin.

Wie toegang krijgt tot je private keys wordt eigenaar van je bitcoin. Daarom is het van het grootste belang om ze te beschermen en ze weg te houden van nieuwsgierige ogen! We zullen later in het boek een paar manieren bespreken waarop je dat kunt doen.

In het vervolg hebben we het alleen nog over self-custodial wallets, waarbij je zelf eigenaar bent van de sleutels en waarbij je zelf de volledige controle hebt over je bitcoin.

Maak je geen zorgen als het ingewikkeld wordt of als je niet alles begrijpt. Dit is een reis en je zult meer begrijpen naarmate je bitcoin meer gaat gebruiken!

Hoe gebruik ik bitcoin?

7.2.2 Verschillende typen bitcoinwallets

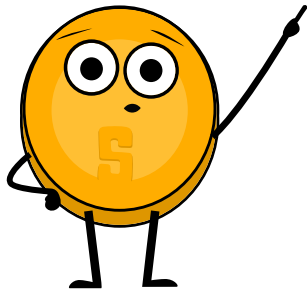
Afhankelijk van waar je private key is gemaakt en opgeslagen, gebruiken we vaak verschillende namen om bitcoinwallets te beschrijven.

Als de sleutels worden opgeslagen op je smartphone, noemen we het een "mobile wallet". Als ze veilig worden opgeslagen op een speciaal apparaat, dan noemen we het een "hardware wallet". Als de sleutel alleen op papier wordt opgeslagen, dan noemen we het een "paper wallet".

De verschillende namen die we aan bitcoinwallets geven, zijn afhankelijk van hoe ze gebruikt worden:

Wallet type	Beschrijving	Voordelen	Nadelen	Wanneer te gebruiken?
Online wallet	Een wallet die toegankelijk is via een webbrowser.	Toegankelijk vanaf elk apparaat met internet. Gemakkelijk te gebruiken.	Minder veilig. Kan worden gehackt.	Iemand die vaak bij zijn wallet moet en daar niet veel waarde in opslaat.
Mobile wallet	Een wallet die op een mobiel apparaat wordt geïnstalleerd.	Gemakkelijk. Overal toegankelijk	Kan verloren gaan als het apparaat zoekraakt, wordt gestolen of wordt gehackt.	Iemand die onderweg transacties moet doen en daar niet veel waarde in opslaat.
Desktop wallet	Een wallet die op een desktop computer wordt geïnstalleerd.	Veiliger dan online wallets. Kan ook offline worden gebruikt.	Kan worden gehackt als de computer is geïnfecteerd met malware.	Iemand die een grote hoeveelheid bitcoin wil opslaan en zich comfortabel voelt met een desktopcomputer.
Hardware wallet	Een fysiek apparaat dat bitcoin opslaat zonder verbonden te zijn met het internet.	Heel veilig. Kan ook offline worden gebruikt.	Bitcoin kan verloren gaan als het apparaat verloren gaat of wordt gestolen.	Iemand die een grote hoeveelheid bitcoin wil opslaan en bereid is te betalen voor de extra veiligheid van een hardware wallet.
Paper wallet	Een fysieke registratie van de private en public keys van een bitcoinwallet.	Heel veilig. Kan ook offline worden gebruikt.	Kan verloren gaan of gestolen worden als de fysieke registratie verloren gaat of gestolen wordt.	Iemand die een grote hoeveelheid bitcoin wil opslaan en extra voorzorgsmaatregelen wil nemen om de veiligheid te garanderen.







Omdat de keys (sleutels) van het ene apparaat naar het andere verplaatst kunnen worden, is de "status" van je bitcoinwallet niet definitief. Als ik bijvoorbeeld de keys van mijn bitcoinwallet genereer op een computer en ze later upload naar mijn telefoon, dan wordt de "desktop wallet" een "mobiele wallet".



Als het gaat om het opslaan van je bitcoin, gaat het er niet alleen om wie er controle over heeft - er zijn ook veel andere risico's waar je rekening mee moet houden. Daarom is het belangrijk om een opslagoplossing te vinden die zowel veilig als handig is.

Als je de afwegingen van de verschillende soorten wallets analyseert, zul je ontdekken dat er geen ideale wallet is die aan alle behoeften voldoet.

Bij het kiezen van een bitcoinwallet moet je hier rekening mee houden:

-  **Beveiliging:** zorg ervoor dat de wallet sterke beveiligingsmaatregelen heeft, zoals 2-Factor authenticatie en een veilig wachtwoordbeleid.
-  **Privacy:** onderzoek of de wallet je toestaat anoniem te blijven, of dat er persoonlijke informatie nodig is om een account aan te maken.
-  **Gebruiksgemak:** kies een wallet die makkelijk te gebruiken is, vooral als je nieuw bent met bitcoin.
-  **Compatibiliteit:** controleer of de wallet compatibel is met je apparaat en besturingssysteem.
-  **Fees:** vergelijk de kosten die verschillende wallets in rekening brengen. Waar krijg je de beste deal?
-  **Reputatie:** onderzoek de reputatie van de wallet en de makers om een idee te krijgen van de betrouwbaarheid.
-  **Controle:** sommige wallets geven je meer controle over je private keys, wat een veiligheidsvoordeel kan zijn.

Bedenk of je een wallet wilt die je volledige controle geeft, of eentje die gebruiksvriendelijker is maar misschien wat minder controle biedt.

7.2.3 Open-source vs closed-source

Een andere belangrijke factor om in gedachten te houden bij het kiezen van een bitcoinwallet is de keuze tussen open-source of closed-source.

Open-source code is erg belangrijk, omdat het de gemeenschap in staat stelt de broncode van de wallet te inspecteren en door te gaan met de ontwikkeling van het project, mocht het team stoppen.

Hoe gebruik ik bitcoin?



Net zoals dat de code van bitcoin volledig open is voor iedereen om te bekijken, te gebruiken en aan te passen, zou het ook een goede zaak zijn dat dit geldt voor de code van de wallet die je gebruikt om je bitcoin in op te slaan.

Activiteit - discussie in de klas en evaluatie van bitcoinwallets op bitcoin.org

Ga naar de volgende website:
<https://bitcoin.org/en/choose-your-wallet> en gebruik je nieuwe kennis van bitcoinwallets om de beste te kiezen op basis van de criteria die we vandaag hebben besproken.



7.3 Een mobiele bitcoinwallet instellen

Nu we bitcoinwallets en de verschillen ertussen beter begrijpen, gaan we kijken hoe we er een in de praktijk kunnen gebruiken. Voor dit voorbeeld maken we een mobiele wallet op onze smartphone.

Activiteit: een bitcoinwallet opzetten/herstellen

Als studenten geen mobiele telefoon hebben, geeft de docent er een te leen.

Oefening in de klas. Optie 1. Download een nieuwe wallet.



Je herstelzin

Je herstelzin wordt gebruikt om je account aan te maken en te herstellen

- | | | |
|-------------|-----------|-----------|
| 1. issue | 2. flame | 3. sample |
| 4. lyrics | 5. find | 6. vault |
| 7. announce | 8. banner | 9. cute |
| 10. damage | 11. sleep | 12. goat |

Sla aub deze 12 woorden veilig op. De volgorde is belangrijk. Deze herstelzin stelt je in staat je account te herstellen

Hoe maak je en gebruik je een bitcoinwallet.

- 1 Zoek naar de app in de App Store (iOS) of Google Play Store (Android).
- 2 Open de app en maak een nieuwe wallet aan. Nu zie je 12 of 24 woorden die de herstelzin vormen (ook wel een seed phrase genoemd). Zorg ervoor dat je deze opschrijft en op een veilige plek bewaart! Met deze herstelzin kun je indien nodig weer volledige toegang krijgen tot je bitcoins.

Onthoud dat als je deze reeks woorden verliest of vergeet, je geen toegang meer hebt tot je bitcoin als je de toegang tot je wallet verliest!

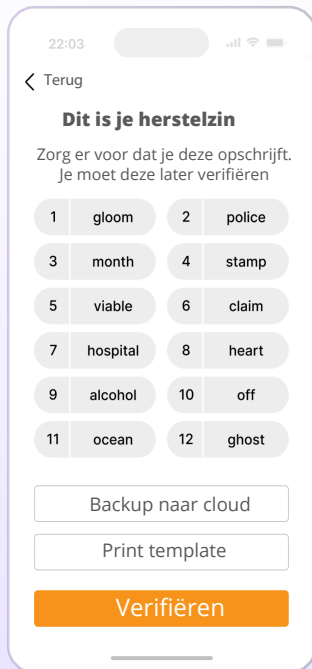
- 3 Je moet dan bevestigen dat je je herstelzin goed hebt opgeslagen. Om dit te doen, moet je opnieuw jouw herstelzin invoeren.
- 4 Als extra beveiligingsmaatregel kun je bij sommige wallets aanvullend nog een wachtwoord kiezen. Je private key en eerste bitcoinadres worden nu automatisch voor je aangemaakt door je wallet.

Je kunt bitcoinadres(sen) vergelijken met je e-mailadres - dit kan je delen met anderen zodat ze je bitcoin naar je kunnen sturen, of in het geval van een e-mailadres, een e-mail.

Je private key is vergelijkbaar met het wachtwoord van je e-mailaccount. Dit wil je met niemand delen omdat ze dan toegang krijgen tot je e-mail.

- 5 Nu kun je bitcoins ontvangen op je bitcoinadres. Met een self-custodial wallet kun je niet altijd direct bitcoin kopen met fiatgeld, dus moet je het misschien eerst kopen bij een exchange en dan overboeken naar je wallet.

Hoe gebruik ik bitcoin?



Oefening in de klas. Optie 2. Wallet herstellen (bij beperkte tijd).

Maak per student een wallet aan en voeg wat satoshis toe.

Geef elke student de herstelzin om deze wallet te herstellen.

Begeleid studenten stap voor stap:

- 1 Wanneer je je wallet voor het eerst start, zie je meestal meerdere methoden om een wallet aan te maken. We gaan nu een bestaande wallet herstellen middels een herstelzin. Tik op [importeer een bestaande wallet] Je ziet nu een introductiescherm, tik op [herstellen met herstelzin].
- 2 Voer de 12 of 24 woorden van de herstelzin één voor één in, in de juiste volgorde.
- 3 Klik op [verifiëren] om de invoer te controleren en daarna op [herstellen] om je wallet te herstellen.
- 4 Je ziet vervolgens "importeren succesvol" als de herstelzin succesvol is geïmporteerd. De wallet is nu hersteld.

7.4 Transacties ontvangen en versturen

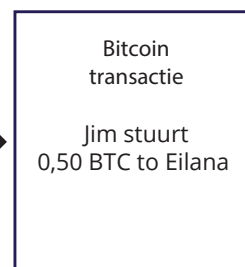
Een bitcointransactie is een eigendoms-overdracht van een bestaande hoeveelheid bitcoin naar een nieuwe eigenaar. Maar in plaats van daadwerkelijke munten over te dragen, werken alle nodes in het netwerk hun lokale kopie van het openbare kasboek bij om de verandering in eigendom weer te geven.

Bij het versturen van een bitcointransactie ondertekent de verzender een bericht dat alleen hij kan ondertekenen met zijn priv sleutel, waarmee hij aan het netwerk doorgeeft dat het eigendom van de bitcoin wordt overgedragen aan de ontvanger.

Dat wil zeggen dat de bitcoin nu wordt gekoppeld aan een adres vanwaar alleen de nieuwe eigenaar bitcoins kan versturen, waardoor hij of zij eigenaar wordt van de bitcoin.

Kasboek

Eigenaar	Waarde
Sam	2,50
Adam	3,00
Michael	6,00
Jim	1,50
Robert	2,00
Eliana	1,75
Daniel	5,25

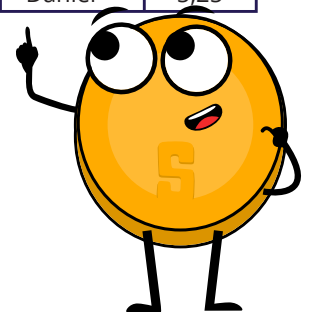


Kasboek

Eigenaar	Waarde
Sam	2,50
Adam	3,00
Michael	6,00
Jim	1,00
Robert	2,00
Eliana	2,25
Daniel	5,25

Nieuwe bitcointransacties worden ge ntieerd vanuit wallets over de hele wereld, maar er is geen centrale betalingsverwerker. In plaats daarvan concurreren miners over de hele wereld om transacties vast te leggen in het kasboek.

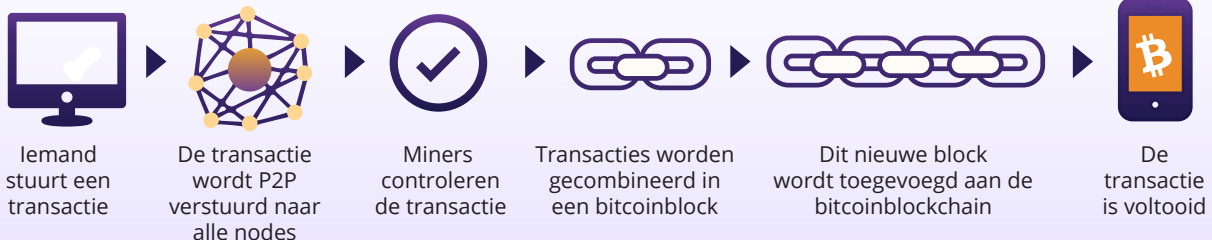
In bovenstaande voorbeeld maakt Jim 0,5 BTC over naar Eliana.



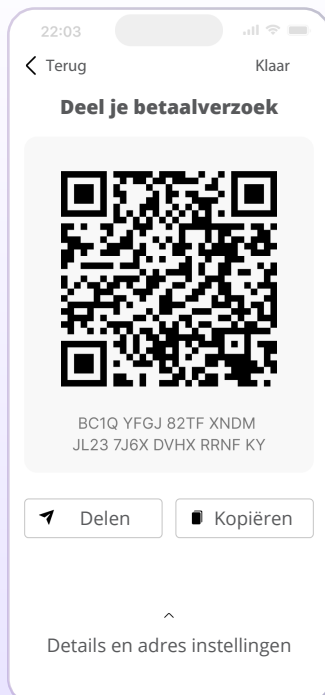
- 1 Eliana deelt haar bitcoinadres met Jim.
- 2 Jim gebruikt zijn wallet om de transactie aan te maken. Deze transactie bevat het bitcoinadres van Eliana, het bedrag (0,5 BTC) en een vergoeding voor de miner.
- 3 Na het ondertekenen van de transactie wordt deze naar het bitcoinnetwerk gestuurd waar deze wordt geverifieerd door de nodes. Nodes controleren de transactie op geldigheid en controleren of Jim genoeg bitcoin heeft. Als dat niet zo is, verwerpen ze de transactie onmiddellijk.
- 4 Zodra de transactie is geverifieerd, wordt deze door miners toegevoegd aan de blockchain en wordt de bitcoin overgemaakt naar het adres van Eliana.
- 5 Eliana kan dan haar private key gebruiken om toegang te krijgen tot de overgemaakte bitcoin in haar wallet.

Het is belangrijk om te weten dat transacties niet meer kunnen worden teruggedraaid.

Hoe een bitcointransactie werkt



Bitcointransacties ontvangen:



Om bitcoin te ontvangen, moet de afzender je bitcoinadres weten. Dit is een unieke reeks letters en cijfers die je wallet aanmaakt en is uniek op het bitcoinnetwerk. Je kunt je bitcoinadres vinden door in te loggen op je bitcoinwallet en te zoeken naar een optie om bitcoin te "Ontvangen" of "Versturen".

Je kan op verschillende manieren je bitcoinadres delen met de afzender:

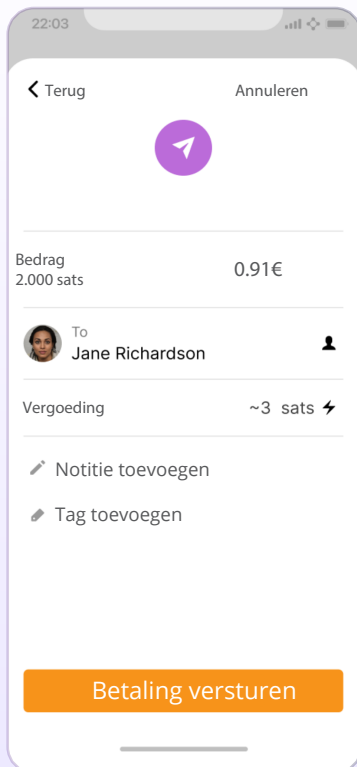
- 1 Kopieer en plak het adres: Je kunt het adres kopiëren door het te markeren en op "CTRL+C" op je toetsenbord te drukken, en het vervolgens te plakken via CTRL+V in een e-mail of bericht aan de afzender.
- 2 Deel een link naar je bitcoinwallet: Bij sommige bitcoinwallets kun je via een link je bitcoinadres delen met de verzender.
- 3 Deel een QR-code: Als de afzender een smartphone heeft met een bitcoinwallet app, kan hij de QR-code scannen om jouw bitcoinadres te krijgen.

Hoe gebruik ik bitcoin?

Zodra de verzender je bitcoinadres heeft, kan hij bitcoin naar je sturen door dit adres en het bedrag in te voeren en de transactie te starten. De bitcoin wordt dan naar je wallet gestuurd en is zichtbaar zodra de transactie is bevestigd op het bitcoinnetwerk. Dit duurt meestal een paar minuten, afhankelijk van de drukte op het bitcoinnetwerk.

Hieronder kijken we hoe het versturen van bitcointransacties via een wallet verloopt.

Bitcointransacties versturen:



Om bitcoin te versturen heb je een paar dingen nodig: een bitcoinwallet, het adres van de ontvanger en de hoeveelheid bitcoin.

- 1 Open je bitcoinwallet. Soms wordt er ter controle een SMS naar je telefoonnummer gestuurd met een code die je moet invoeren in het dialoogvenster. Als je Google 2FA hebt ingeschakeld, moet je de zescijferige code van de Google Authenticator app invoeren.
- 2 Kopieer het bitcoinadres van de ontvanger. Navigeer naar de functie "Versturen" of "Verzenden".
- 3 Plak het bitcoinadres van de ontvanger in het veld "Aan".
- 4 Voer het bedrag in dat je wilt versturen in het veld "Bedrag".
- 5 Controleer het adres van de ontvanger en het te versturen bedrag.
- 6 Voordat je op "Betaling versturen" klikt, raden we je aan om de transactiegegevens nog een keer te controleren om er zeker van te zijn dat je het juiste bedrag naar het juiste bitcoinadres stuurt.
- 7 Verstuur de transactie en wacht tot het bitcoinnetwerk de transactie bevestigt.

Nu weet je hoe je een self-custodial bitcoinwallet moet beoordelen, selecteren en gebruiken. Bitcoin versturen van de ene wallet naar de andere op het bitcoinnetwerk wordt een "on-chain-transactie" genoemd. Dit komt omdat de transactie plaatsvindt op de blockchain van het bitcoinnetwerk. On-chain-transacties zijn de veiligste manier om transacties te doen met bitcoin, maar de transacties zijn duurder en langzamer dan andere opties die we zullen bespreken in hoofdstuk 8.

Activiteit: bitcointransacties in de praktijk

Doel: de onderliggende concepten en mechanismen van peer-to-peer bitcointransacties begrijpen.

Hieronder een korte herinnering aan de hoofdrolspelers in een bitcointransactie:

- Afzenders en ontvangers zijn de partijen die transacties met elkaar willen doen.
- Nodes valideren transacties en slaan een volledige kopie van de blockchain op.
- Miners zijn verantwoordelijk voor het toevoegen van nieuwe transacties aan de blockchain.

In deze oefening krijg je een van de volgende rollen toegewezen: verzender, ontvanger, node of miner.

- 🌟 Verzenders zijn verantwoordelijk voor het maken en broadcasten van transacties.
- 🌟 Ontvangers zijn verantwoordelijk voor het ontvangen en verifiëren van transacties.
- 🌟 Nodes valideren de transacties door te controleren of de transactie geldig is.
- 🌟 Miners zijn verantwoordelijk voor het toevoegen van de transacties aan de blockchain.

Zowel nodes als ontvangers moeten transacties verifiëren

- 1 🌟 Een verzender: jij maakt een transactie aan.

Volg deze stappen om een transactie aan te maken: neem een transactienota en schrijf het aantal munten op dat je wilt versturen en de naam of initialen van de ontvanger. Onderteken het briefje met je naam of initialen, waarmee je een private key simuleert. Geef het transactiebriefje aan de ontvanger.

- 2 🌟 Een ontvanger: jij bent verantwoordelijk voor het verifiëren van de transacties.

- 🌟 Controleer op de transactienota of het juiste aantal munten en de naam of initialen van de ontvanger zijn geschreven.
- 🌟 Tel de ontvangen munten en vergelijk ze met het aantal munten dat op het briefje staat.
- 🌟 Als de munten overeenkomen, vink je het goedkeuringsvakje aan. Als de munten niet overeenkomen of als je twijfelt, wijs de transactie dan af.

Munten verstuurd	Verzender	Verzender handtekening	Ontvanger	Datum & tijd	Ontvanger goedkeuring

- 3 🌟 Een node: jij bent verantwoordelijk voor het verifiëren en valideren van de transacties.

- 🌟 Controleer of het adres van de afzender geldig is en of het adres van de ontvanger geldig is.
- 🌟 Controleer of de verzender genoeg munten heeft om de transactie te voltooien en of de transactie geen munten dubbel uitgeeft.

Munten verstuurd	Verzender	Verzender handtekening	Ontvanger	Datum & tijd	Node goedkeuring

Hoe gebruik ik bitcoin?

4 Een miner: jij bent verantwoordelijk voor het toevoegen van de transacties aan de blockchain.

- Controleer de transacties die zijn goedgekeurd door de ontvangers en gevalideerd door de nodes.
- Gooi de dobbelstenen en vergelijk de getallen met die van de andere miner. De miner met het kleinste getal voegt de transactie toe aan de blockchain.
- Voor je tijd, energie en moeite verdien je een punt. De miner met de meeste punten wint.

** Als een transactie eenmaal aan de blockchain is toegevoegd, kan deze niet meer worden veranderd of teruggedraaid.

5 Houd gedurende de activiteit je muntsaldo bij door de munten in je digitale wallet te tellen.

Munten verstuurd	Verzender	Verzender handtekening	Ontvanger	Datum & tijd	Goedkeuring

6 Bespreek de geleerde concepten met je klas.

7.5 Sparen in bitcoin

Bitcoin is een manier om je geld te beschermen tegen inflatie en, als je het goed doet, ook te beschermen tegen controle door iemand anders. Sparen in bitcoin is een middel om over de lange termijn waarde op te slaan en op te bouwen. Zoals je inmiddels begrijpt, is het soort geld dat je kiest om te sparen een van de belangrijkste beslissingen die je kunt nemen. Door verstandig te kiezen kun je een betere toekomst opbouwen voor jezelf en je naasten.



Gemoedsrust: Als bitcoin op de juiste manier wordt bewaard, is het de enige vorm van eigendom die niemand je kan afnemen



7.6 Don't trust, verify

Wat je ook doet in bitcoin, onthoud dit: "Don't Trust, Verify". Er zijn geen leiders in bitcoin. Je moet nooit blindelings iemands beweringen volgen. In plaats daarvan moet je altijd vragen stellen bij wat je verteld wordt en het voor jezelf verifiëren. Door dit mantra te volgen, bescherm je jezelf tegen het verliezen van je bitcoin. Dit geldt net zo goed voor beweringen als "dit is de volgende bitcoin", of voor "investeringsmogelijkheden" of beloften van "snelle en gemakkelijke winsten".

Samengevat heeft hoofdstuk 7 je de belangrijke vaardigheden gegeven om bitcoin in je dagelijks leven te gebruiken. Je hebt geleerd hoe je bitcoin op verschillende manieren kunt verkrijgen, ontvangen en versturen, en hoe je het veilig kunt bewaren met behulp van verschillende wallets.

Door je mobiele bitcoinwallet in te stellen en transacties met anderen uit te voeren, heb je nu praktijkervaring opgedaan om bitcoin vol vertrouwen dagelijks te gebruiken. Als je begrijpt dat bitcoin een manier is om geld te sparen en het idee van "Doe Je Eigen Onderzoek (DYOR) - Don't Trust, Verify" volgt, heb je nu controle over je geld.

In het volgende hoofdstuk verkennen we het lightningnetwerk. We bekijken hoe deze innovatieve technologie de manier verandert waarop mensen wereldwijd toegang hebben tot geld en hoe ze het gebruiken, van alledaagse transacties tot meer geavanceerde toepassingen. Je zult leren hoe het lightningnetwerk individuen, gemeenschappen en bedrijven in staat stelt om toegang te krijgen tot financiële diensten.