Nederlands Forensisch Instituut
Ministerie van Justitie en Veiligheid

Informatieblad

Bitcoin

Inhoudsopgave

1. Inleiding

Bitcoin is de eerste decentrale digitale valuta, geïntroduceerd in 2008[1]. Bitcoins worden gebruikt als betaalmiddel voor criminele activiteiten, bijvoorbeeld in cybercrime (bijv. betalen van de afkoopsom bij ransomware) en illegale handel (bijv. handel in verdovende middelen of wapens). Ook worden ze steeds vaker gebruikt voor witwassen. In strafrechtelijke onderzoeken naar zulke activiteiten doen opsporingsdiensten onderzoek naar Bitcoin en rapporteren hierover in processen-verbaal.

Dit document geeft een algemene uitleg van Bitcoin, hoe hij werkt als een betaalmiddel en hoe adressen en transacties werken. Daarnaast wordt ook de onderliggende techniek uitgelegd, inclusief welke digitale sporen er zijn, de manier waarop (forensisch) onderzoek plaatsvindt en welke technieken kunnen worden gebruikt om traceerbaarheid van betaling tegen te gaan.

Dit informatieblad richt zich op Bitcoin. Hoewel het helpt voor het begrip van andere cryptovaluta, zijn de concepten en technieken niet één-op-één uitwisselbaar. Elke

[1] Nakamoto, Satoshi. *A peer-to-peer electronic cash system*, 2008. https://bitcoin.org/bitcoin.pdf. De ware identiteit van de auteur is niet bekend.

cryptovaluta heeft specifieke kenmerken, waardoor digitale sporen en onderzoek hiernaar anders werkt.

1.1. Leeswijzer

Dit informatieblad legt eerst in de sectie 2 conceptueel uit hoe Bitcoin voor de gebruiker als betaalmiddel werkt. Vervolgens lichten we in sectie 3 toe hoe een netwerk van computers betalingen controleert en beheert. Sectie 4 gaat dieper in op het beheren van Bitcoin, waarna we in sectie 5 de handel in Bitcoin toelichten. In de sectie 6 leggen we uit hoe een analyse van transacties inzicht kan geven in historisch betaalverkeer, en welke mogelijkheden er zijn om dat tegen te gaan. In sectie 7 lichten we tot slot toe welke sporen onderzocht kunnen worden op de apparaten van gebruikers.

2. Bitcoin als betaalmiddel

Betalen of betaald worden met Bitcoin (vaak afgekort als BTC) is vergelijkbaar met betalen of betaald worden met andere (digitale) betaalmethoden, zoals een bankoverschrijving. Het werkt alleen net even anders.

Om te betalen of betaald te kunnen worden met Bitcoin, is een *bitcoinwallet* nodig. Dit is een digitale portemonnee, vergelijkbaar met een bankrekening, die speciaal is ontworpen voor het beheren en verzenden van Bitcoin. Een gebruiker heeft in zijn wallet één of meer *bitcoinadressen*, vergelijkbaar met bankrekeningnummers, die bestaan uit lange reeksen met tekens zoals '1dEGELfGDH3PcfvGGbSJYtJ56KXTacP3K' of 'bc1qkszklnj37s9gfpvwry89fw3nvpyv87acyns4a7'.

Voor de gebruiker is het verrichten van een betaling met Bitcoin vaak een kwestie van een bitcoinadres intypen of kopiëren, een bedrag intoetsen en op de 'verstuur'-knop drukken. Achter de schermen gebeurt er in de tussentijd van alles. De wallet-software verwerkt de gegevens tot een betaling, een *bitcointransactie*. Deze transactie wordt naar het *bitcoinnetwerk* verzonden voor controle. Andere deelnemers op het netwerk controleren de transactie en leggen deze vast. Dit proces kan enige tijd in beslag nemen, afhankelijk van de drukte op het bitcoinnetwerk en de gekozen transactiekosten[2]. In tegenstelling tot traditionele valuta, is er dus geen centrale autoriteit (bijv. een bank of regering) die Bitcoin beheert of controleert. In een grootboek, genaamd de *blockchain*, worden betalingen (transacties) gecontroleerd en vastgelegd. Gelijkwaardige computers (*bitcoinnodes*) in het *bitcoinnetwerk* slaan een kopie van dit grootboek op en controleren voortdurend en volautomatisch de correctheid daarvan door communicatie met andere computers in dat netwerk.

2.1. Betalingen ontvangen

Met een wallet kan een gebruiker zelf nieuwe adressen aanmaken[3] om betalingen op te ontvangen. Zo kunnen in een wallet op meerdere adressen tegoeden ontstaan. Achter de schermen, in de blockchain, zijn deze tegoeden vastgelegd als *outputs* (uitvoer) van de bij de betalingen horende bitcointransacties. Iedere output vertegenwoordigt een hoeveelheid Bitcoin en is gekoppeld aan het bitcoinadres waarop betaald is. De tegoeden van de bitcoinadressen, dus de outputs die nog niet zijn uitgegeven, staan bekend als *unspent transaction outputs (UTXO)*. Het saldo van een wallet is de som van de waarden van alle UTXOs van de bij de wallet horende bitcoinadressen.

2.2. Met Bitcoin betalen

Deze outputs kunnen vervolgens worden gebruikt om mee te betalen. Iedere output (UTXO) kan maar één keer worden uitgegeven, dus maar één keer als input voor een nieuwe transactie worden gebruikt. Dit is technisch zo ingericht, om te voorkomen dat bitcointegoeden meerdere keren worden uitgegeven, ook wel double-spending genoemd.

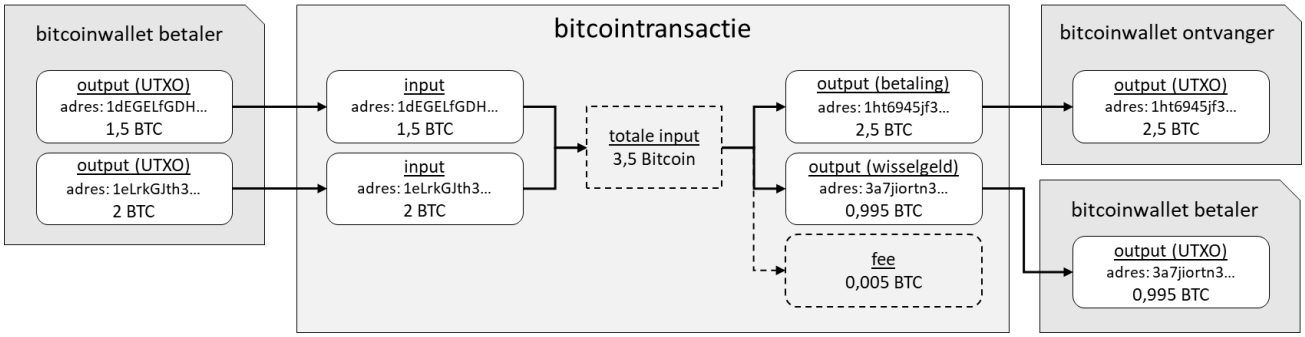
Voor een betaling kan de eigenaar van een wallet meerdere UTXOs in die wallet combineren, zie *Figuur 1*. Het maakt daarbij niet uit aan welk bitcoinadres ze gekoppeld zijn. Ze worden dan *inputs* (invoer) voor een volgende transactie. Iedere bitcointransactie heeft zo een aantal inputs en een aantal (nieuwe) outputs.

De inputs van een transactie vormen samen een bepaald bedrag aan Bitcoin. In de transactie wordt vastgelegd hoe dat bedrag wordt verdeeld onder de nieuwe outputs. Deze transacties worden na controle verzameld en vastgelegd in blokken op de Bitcoin-blockchain.

Omdat de waarden van UTXOs zelden precies optellen tot het bedrag dat de gebruiker wil betalen, is er bijna altijd sprake van wisselgeld. De wallet software kiest er in de meeste gevallen voor om het wisselgeld over te maken naar een nieuw adres in de wallet van de betaler, het wisselgeldadres of *change address*. De betaler krijgt dan dus

[2] De betaler kan bij iedere betaling zelf transactiekosten bepalen. Hoe hoger deze kosten zijn, hoe sneller de transactie wordt vastgelegd. Zie sectie 3 voor meer informatie.

[3] De manier waarop nieuwe adressen worden aangemaakt wordt bepaald door de wallet-software van de gebruiker. Zie sectie 4 voor meer informatie.



Figuur 1 bitcointransactie voor betaling van 2,5 BTC aan adres 1ht6945jf3...

een nieuwe output (UTXO) met de waarde van het wisselgeld, de *change output*. Aan de transactie zelf is niet te zien welke output het wisselgeld is en welke de betaling(en).

Zodra de transactie opgesteld is, wordt deze aan het netwerk aangeboden. De wallet software neemt contact op met één of meer bitcoinnodes en geeft de transactie door.

3. Het bitcoinnetwerk

Na het aanbieden van een bitcointransactie aan een bitcoinnode, stuurt de node de transactie door naar andere nodes, die het weer doorsturen naar andere nodes, totdat iedereen op het netwerk op de hoogte is van de transactie. De transactie komt nu in de *mempool* van de node, de lijst van transacties die wachten om opgenomen te worden in een blok (*block*).

Specifieke deelnemers, genaamd *miners*, verzamelen deze transacties en controleren de geldigheid ervan. Dit is ook het moment dat wordt gecontroleerd dat Bitcoin niet twee keer worden uitgegeven (*double spend*). Miners proberen een geldig block tot stand te brengen met de verzamelde transacties door een waarde in het block te variëren, de *nonce*. Dit proces vergt veel rekenkracht. De miner die als eerste een geldig block maakt door de juiste nonce te vinden, publiceert het block op het bitcoinnetwerk. Omdat het block een verwijzing bevat naar het controlegetal (*block hash*) van het block ervoor ontstaat hierdoor een keten van blokken, de *blockchain*. De andere miners in het bitcoinnetwerk proberen vervolgens een ander block te maken die op dit nieuwe block verder bouwt, om zo de blockchain langer te maken. Dit systeem staat bekend als *proof-of-work verification*. De langste keten blokken wordt gezien als de waarheid (*longest chain rule*).

Het bedrag dat door de transactie wordt uitgegeven (de outputs, inclusief wisselgeld) is vaak minder dan de waarde van de inputs. Het verschil, de transactiekosten, is een beloning (*fee*, zie Figuur 1) voor de miner die deze transactie opneemt in een block op de blockchain. Hoe hoger deze transactiekosten zijn, hoe interessanter voor een miner om de transactie in een block op te nemen.

Het kan voorkomen dat twee miners bijna tegelijk een nieuw block publiceren en dat een gedeelte van de miners doorwerkt op het ene block en een ander gedeelte op een ander block. Bitcoinsoftware geeft voorrang aan de langste keten. Wanneer één van de twee blokken de basis vormt voor weer een nieuw block, zullen alle miners doorwerken op dit nieuwste block. De transacties in het block waar niet op wordt verder gewerkt (*orphan block* of *stale block*) maken geen deel meer uit van de blockchain en vallen terug in de mempool.[4] Miners zullen ze vervolgens opnemen in een nieuw block.

3.1. Confirmations

Het aantal blocks dat aan de blockchain is toegevoegd ná het block waarin de transactie is opgenomen, staat bekend als het aantal bevestigingen (*confirmations*). Het is een maat voor hoe vast de transactie is verankerd in de blockchain. Alle transacties in een recent toegevoegd block hebben één confirmation. Als hierop wordt verder gewerkt en er wordt nog een block toegevoegd, dan hebben de transacties twee confirmations, enzovoorts. Pas bij een minimaal aantal confirmations, wat enige tijd kan duren, wordt een betaling als definitief beschouwd. Verschillende diensten gebruiken hiervoor verschillende minima.

3.2. Aanvallen op de blockchain

Als een node een block aanbiedt waar een transactie in zit met een output (UTXO) die al is gepubliceerd in een eerder block op de blockchain, dan wordt dat direct door het netwerk gedetecteerd en wordt het nieuwe block verworpen.

Om een Bitcoin (UTXO) toch twee keer uit te kunnen geven, moet een aanvaller eerst een betaling doen en dan, wanneer de aanvaller hier goederen of diensten voor heeft ontvangen, de betaling ongedaan maken. Daarna kunnen de UTXOs nogmaals uitgegeven worden.

[4] Ze vallen terug in de mempool zolang het geldige transacties zijn in de op dat moment langste keten. Anders worden ze verworpen.

Zoals eerder toegelicht, wordt de langste keten blokken gezien als de waarheid. Om de eerdere betaling uit de blockchain te halen, moet de aanvaller een nieuwe keten maken die aansluit in de blockchain vóór het block met de eerdere betaling én die langer is dan de op dat moment langste keten. Dit moet nog steeds een geldige blockchain zijn, waarin alle transacties met de juiste private sleutels ondertekend zijn. De aanvaller kan dus geen geld van derden uitgeven.

Om dit voor elkaar te krijgen, moet de aanvaller over meer rekenkracht beschikken dan alle andere miners bij elkaar, ofwel meer dan de helft van de totale rekenkracht. Daarom staat dit bekend als een 51% *aanval*.

Er is overigens nog nooit een 51% aanval uitgevoerd op Bitcoin. Door de grote en diverse groep miners is een dergelijke aanval op Bitcoin op dit moment erg lastig voor te stellen. Andere, kleinere cryptovaluta zijn in het verleden wel slachtoffer geworden van een 51% aanval.

4. Bitcoinwallets

Een gebruiker gebruikt een bitcoinwallet om te betalen en om zijn of haar saldo op te vragen.

Custodial en non-custodial wallets
Bitcointegoeden kunnen ook worden ondergebracht bij een dienstverlener. De tegoeden staan dan niet in een aparte bitcoinwallet van de gebruiker, maar worden door de dienstverlener beheerd. In een apart systeem wordt bijgehouden welk tegoed bij welke gebruiker (account) hoort. Dit staat bekend als een *custodial wallet*. Deze systemen zijn veel makkelijker in het gebruik dan 'echte' (*non-custodial*) bitcoinwallets, maar de gebruiker is dan wel afhankelijk van de dienstverlener.

De wallet software van de gebruiker geeft toegang tot de beschikbare outputs (UTXOs) die horen bij de bitcoinadressen die met de wallet worden beheerd. Als de gebruiker een betaling wil verrichten, dan zoekt de wallet-software UTXOs bij elkaar die optellen tot een bedrag dat gelijk of hoger is aan het over te maken bedrag. Deze UTXOs vormen de inputs van de nieuwe voor de betaling te maken transactie. De outputs van de nieuwe transacties zijn het adres of de adressen waar de betaling naartoe gaat en eventueel een wisselgeldadres.

Verschillende wallets hanteren verschillende strategieën voor het selecteren van de te combineren UTXOs. In het algemeen wordt gekozen om minder verschillende bitcoinadressen te combineren, want dit levert kleinere transacties op en daarmee ook kleinere transactiekosten. Daarnaast probeert wallet software om heel kleine outputs (als wisselgeld) te voorkomen, omdat het gebruiken van deze UTXOs een latere transactie meer kost dan ze waard zijn. Dit wordt ook wel *bitcoindust* genoemd.

4.1. Bitcoinadressen en cryptografische sleutelparen

Om een output (UTXO) uit te geven, moet de gebruiker bewijzen dat hij de eigenaar/beheerder is van het bitcoinadres van de UTXO. Dat doet hij of zij door de transactie digitaal te ondertekenen.

Om dit technisch goed te regelen, zijn alle bitcoinadressen afgeleid van *cryptografische sleutelparen* die door de wallet software worden beheerd.

Cryptografische sleutelparen
Cryptografische sleutelparen bestaan uit twee bij elkaar horende sleutels: een *publieke sleutel* die voor iedereen toegankelijk is en een goed beschermde *private sleutel* van de eigenaar van het sleutelpaar. Als je gegevens met de ene sleutel versleutelt ("op slot doet"), dan kun je die met de andere sleutel ontsleutelen ("van slot halen"). Gegevens versleutelen met de private sleutel is te vergelijken met een digitale handtekening van de eigenaar. Iedereen kan namelijk controleren of de bijbehorende publieke sleutel past en daarmee dus vaststellen dat de gegevens van de eigenaar van de bijbehorende private sleutel af komen. Gegevens versleutelen met de publieke sleutel, wat iedereen kan doen, zorgt ervoor dat alleen de eigenaar van de private sleutel de gegevens kan ontsleutelen. Als afzender weet je dan zeker dat niemand anders de gegevens kan inzien.

De sleutelparen voor Bitcoin hebben een vergelijkbare, maar net andere functie. Een bitcoinadres is afgeleid van de publieke sleutel. Dit werkt maar één kant op: Iedereen kan van een publieke sleutel een bitcoinadres afleiden, maar van een adres kun je niet terug naar de publieke sleutel. De private sleutels werken zoals hierboven beschreven en worden gebruikt om transacties te ondertekenen. Met de publieke sleutel kunnen andere deelnemers controleren dat degene die de transactie ondertekent ook de eigenaar is van het adres.

De betaler kan bij het opstellen van een transactie UTXOs van een of meerdere bitcoinadressen gebruiken als inputs. Deze transactie wordt digitaal ondertekend met de private sleutels van alle verschillende bitcoinadressen van die UTXOs.

4.1.1. Bitcoinadressen (sleutelparen) genereren

De oudere generaties wallets genereerden willekeurige adressen om Bitcoin te ontvangen en voor het wisselgeld. Dit maakte het lastig om reservekopieën te maken van

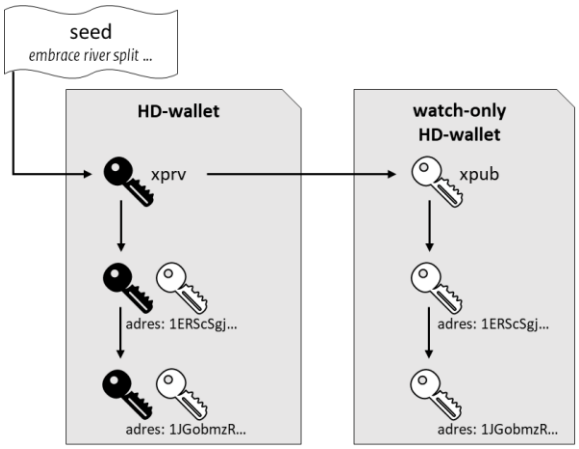
wallets en om wallets tegelijkertijd op verschillende plekken te gebruiken.

Daarom zijn *deterministische wallets* geïntroduceerd. Bij het aanmaken van zulke wallet wordt vaak een initialiseringszin gebruikt, ook wel *seed*, *recovery seed*, *seed phrase* of *mnemonic phrase* genoemd. Dat is een reeks van 12 tot 24 eenvoudige (vaak Engelse) woorden die de gebruiker op een stukje papier schrijft of digitaal opslaat, bijvoorbeeld:

> *embrace river split burden mouse slender slow diet loyal ocean network whisper source firm local*

Deze seed wordt door de wallet gebruikt voor het genereren van bitcoinadressen (sleutelparen), zie Figuur 2. Als de gebruiker toegang tot zijn of haar wallet kwijtraakt, kunnen alle sleutels in de wallet worden hersteld door deze woorden in te voeren in de wallet software. Omdat de wallet deterministisch is, reproduceert de wallet met deze ingevoerde seed opnieuw alle originele sleutelparen. De seed geeft hiermee dus toegang tot alle tegoeden die beschikbaar zijn op alle bitcoinadressen in de wallet.

Hiërarchische deterministische wallets (ook bekend als HD-Wallet, gestandaardiseerd als BIP-0032[5]) kunnen gegenereerde private sleutels gebruiken om meer sleutelparen (en dus meer bitcoinadressen) te genereren. Zo'n private sleutel staat bekend als een *extended private key*, of *xprv* sleutel. Bij elke *xprv* sleutel hoort een *extended public key*, of *xpub* sleutel. Dat is een publieke sleutel die de adressen die horen bij de xprv sleutel kan afleiden, maar zelf geen transacties kan maken. Met de xpub sleutel kunnen tegoed (en transacties) van de wallet worden ingezien, maar niet worden uitgegeven. Deze worden bijvoorbeeld gebruikt



Figuur 2 Voorbeeld afleiding adressen en sleutels uit seed

om snel tegoeden in te kunnen zien, zonder de private sleutel op een apparaat op te moeten slaan. Het is dus geen publieke sleutel die iedereen kan en mag inzien. Gebruikers kunnen deze wel delen zodat anderen tegoeden kunnen inzien maar niet uitgeven. Wallets op basis van zulke xpub sleutels worden *watch-only wallets* genoemd.

4.2. Soorten bitcoinwallets

De belangrijkste taak van een wallet is het veilig beheren van de cryptografische sleutelparen die horen bij de bitcoinadressen van de gebruikers. De term *bitcoinwallet* wordt dan ook vaak gebruikt als synoniem voor de verzameling van private sleutels van de bitcoinadressen waar de gebruiker beschikking over heeft.

De meeste wallets zijn softwarematige wallets, vergelijkbaar met software voor internet bankieren. Zo is er wallet-software voor gebruik op de desktopcomputer en er zijn wallet-apps voor gebruik op een mobiele telefoon. Dit kunnen custodial wallets zijn, waarbij de app toegang geeft tot een account bij een dienstverlener, of non-custodial wallets waarbij de app zelf de sleutels beheert en transacties opstelt en verstuurt. De meeste non-custodial wallet-software slaat de sleutelparen om veiligheidsredenen lokaal (op het apparaat) op in een bestand, dat vaak is beveiligd met een wachtwoord.

Er zijn ook *hardware wallets* te koop. Dit zijn apparaatjes ter grootte van een USB-stick, vaak met een schermpje, die de sleutelparen opslaan en transacties opstellen. De gebruiker voert een pincode in om de hardware wallet te ontgrendelen. Bekende merken van hardware wallets zijn Trezor en Ledger.

Een andere optie is om de private sleutels helemaal niet digitaal te bewaren, maar op papier. Dit heet een *paper wallet*. De eigenaar print de private sleutels op papier als een reeks tekens en/of als een QR-code. De gebruiker kan geld "op de wallet zetten" door Bitcoins te verzenden naar het bitcoinadres van de wallet. Om het tegoed van de wallet uit te geven, heeft de gebruiker de private sleutel nodig in de QR-code. Dit staat bekent als het "vegen" van een paper wallet (*sweeping*). Paper wallets worden vaak gebruikt voor lange termijn offline opslag van Bitcoin.

Mensen en organisaties die met grote hoeveelheden Bitcoins werken, hanteren vaak een *hot wallet/cold wallet systeem*. Werkkapitaal wordt opgeslagen in de *hot wallet*. De private sleutels van de hot wallets zijn direct online beschikbaar. Hierdoor kunnen er eenvoudig en

[5] BIP-0032 staat voor *Bitcoin Improvement Proposal* nummer 32. Een BIP beschrijft een voorstel voor een uitbreiding aan Bitcoin. De bitcoincommunity bepalen samen welke voorstellen wel en niet worden ondersteund en daarmee een standaard worden.

geautomatiseerd transacties vanuit deze wallet worden gedaan. Bitcoins die niet direct nodig zijn worden om veiligheidsredenen overgeboekt naar een wallet waarvan de private sleutels niet online zijn opgeslagen, de *cold wallet*.

Oorspronkelijk hielden bitcoinwallets een volledige kopie van de blockchain bij, zodat ze transacties konden controleren en nog niet uitgegeven outputs (UTXOs) konden opzoeken. Omdat deze blockchain inmiddels honderden gigabytes groot is, is dat niet praktisch, zeker niet voor incidenteel gebruik. Tegenwoordig zijn er dan ook *light clients* die via het internet gegevens uit de blockchain raadplegen.

5. Handelen met Bitcoin

Bitcoin heeft geen vaste waarde ten opzichte van traditionele valuta's zoals de Euro of de Amerikaanse dollar, maar varieert (vaak sterk) in waarde. Op online handelsplatformen (bitcoinexchanges) kunnen gebruikers onderling Bitcoin verhandelen van of naar andere (digitale) valuta. Gebruikers adverteren dan hun wens om te kopen of te verkopen. Het platform regelt de aan- en verkoop en vraagt meestal een percentage van de transactie als vergoeding voor de dienstverlening.

Bij de meeste exchanges kunnen de gebruikers ook tegoeden aanhouden in Bitcoin of andere (digitale) valuta. Deze tegoeden worden meestal niet opgeslagen in een bitcoinwallet, maar worden door de exchange beheerd namens de gebruiker. Ze zijn vergelijkbaar met een custodial wallet.

Er bestaan ook websites die alleen mensen met elkaar in contact brengen en niet de overdracht van de (digitale) valuta zelf regelen. Ondanks dat deze sites geen handelsmogelijkheden bieden, worden ze *peer-to-peer exchanges* genoemd.

6. Blockchainanalyse

De inhoud van het gedeeld grootboek in de blockchain is voor iedereen beschikbaar. Door deze gegevens te analyseren, kan informatie over de relatie tussen transacties en adressen worden afgeleid.

Figuur 3 toont een bitcointransactie zoals weergegeven op blockchair.com. Een van de twee ontvangende adressen is waarschijnlijk het wisselgeldadres. De pijltjes leiden tot eerdere en latere transacties. De eerste output heeft geen pijltje omdat deze output op het moment van het maken van de screenshot nog niet was uitgegeven.

Figuur 3 bitcontransactie zoals getoond door blockchain explorer

6.1. Clustering

Een bitcoinwallet beheert meerdere private sleutels en bevat dus ook meerdere bitcoinadressen. Dat deze adressen bij dezelfde wallet horen en dus samen worden beheerd, is niet zichtbaar voor buitenstaanders. *Clusteranalyse*, ook *clustering* genoemd, is een methode om op basis van de transacties in de blockchain een schatting te maken van welke adressen samen beheerd worden en dus bij dezelfde wallet horen.

Er zijn twee vuistregels die gebruikt worden bij het clusteren van adressen, beide op basis van inputs van transacties.

1. Adressen waarvan tegoeden samen worden uitgegeven horen bij een cluster. Dit is ook bekend als de co-spend regel, of in de wetenschappelijke literatuur, als de transitieve afsluiting (eng: *transitive closure*) van de netwerkgraaf van transactie-inputs.[6]

2. Transacties gebruiken geen overbodige inputs. Men betaalt in de winkel een aankoop van €15 niet met een briefje van €20 en eentje van €10. Vergelijkbaar zal wallet-software ook geen overbodige UTXO's (het briefje van €10) gebruiken. De analysesoftware gebruikt dit gedrag van wallet-software om een inschatting te maken welke output van een transactie de betaling is en welke het wisselgeld.

Het NFI heeft in meerdere strafzaken onderzoek gedaan naar de clustering van adressen door de (commerciële) blockchainanalyse-software Chainalysis. Door het herhaaldelijk toepassen van deze twee regels, kan het NFI de clustering afkomstig uit Chainalysis in alle onderzochte gevallen reproduceren.

Dit betekent niet dat de clustering een perfecte reconstructie geeft van de gebruikte wallets. Soms bevat de blockchain niet genoeg informatie om een adres in verband te kunnen brengen met een cluster. Adressen die alleen Bitcoin hebben ontvangen, maar nooit hebben uitgegeven, kunnen

[6] M. Jourdan, S. Blandin, L. Wynter and P. Deshpande, *Characterizing Entities in the Bitcoin Blockchain*, 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 2018, pp. 55-62, doi: 10.1109/ICDMW.2018.00016.

bijvoorbeeld niet door toepassing van de co-spend regel worden geclusterd.

6.2. Tagging

Clustering geeft geen inzicht in de daadwerkelijke beheerder (persoon of dienst) van een bitcoinadres. Op basis van alleen de blockchain kan deze vraag niet worden beantwoord.

Gespecialiseerde bedrijven proberen de beheerder van adressen te achterhalen. Dit heet *tagging* of *labeling*. Hiervoor combineren ze gegevens uit de blockchain met gegevens uit open bronnen zoals het internet of darkweb. Ook maken ze gebruik van clustering, waarbij adressen worden geclusterd en volledige clusters worden getagd op basis van individuele adressen in de clusters.

Het NFI heeft geen systematisch onderzoek uitgevoerd naar de betrouwbaarheid van de tags die worden toegekend door analysesoftware. Wel heeft het NFI in ongeveer tien strafzaken onderzoek gedaan naar tagging door Chainalysis, op basis van andere sporen zoals bevestigingsmails van verschillende exchanges. Ook heeft het NFI referentie-experimenten gedaan, waarbij een aantal transacties zijn uitgevoerd met specifieke exchanges, die vervolgens zijn opgezocht met Chainalysis.

Uit dit onderzoek blijkt dat adressen die horen bij diensten goed worden getagd, of niet worden getagd. Door de relatief kleine steekproef is echter niet uit te sluiten dat foute tags voorkomen. Ook komen sommige diensten helemaal niet voor als tags in Chainalysis.

6.3. Bitcoinmixers

Er zijn meerdere manieren om de traceerbaarheid van Bitcoins moeilijker of zelf onmogelijk te maken. Dit gebeurt door meerdere transacties (van meerdere gebruikers naar meerdere ontvangende partijen) te vermengen, ook wel *mixing* genoemd.

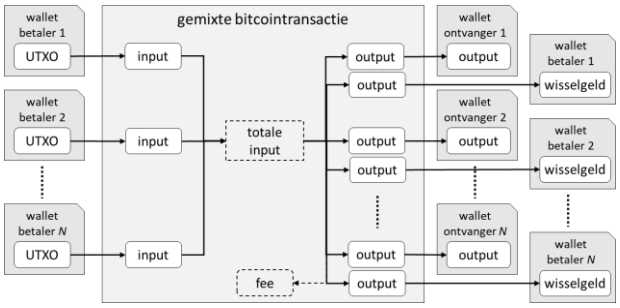
Een manier om te mixen is door het gebruik van online mixerdiensten. De gebruiker meldt aan de mixerdienst dat hij een bepaald bedrag wil overmaken naar een bepaald adres. De mixerdienst genereert een nieuw adres en vraagt de gebruiker om het bedrag (plus de kosten voor het gebruik van de mixerdienst) over te maken naar dat nieuwe adres. Als dat is gebeurd, maakt de mixerdienst vanuit een ander adres de bitcoins over naar het adres van de ontvangende partij. Deze transacties zijn hierdoor niet direct via de blockchain aan elkaar te koppelen. De betalingen vinden plaats met (vermengde) tegoeden van andere gebruikers en de eigen tegoeden van de mixerdienst.

Bij mixing betaalt de betaler vanuit zijn wallet (*bronwallet*) aan de mixer. Mixers hebben daarom geen effect op de clustering van de bronwallets. Mixers hebben ook geen invloed op de clustering van de ontvangers van de gemixte transacties omdat outputs niet gebruikt worden voor clustering.

Als alternatief kunnen meerdere partijen bij elkaar worden gebracht en worden hun betalingen vermengd in één enkele transactie: de inputs en outputs van de losse betalingen worden in één transactie samengenomen. Hierdoor is niet meer na te gaan wie een betaling aan welk adres heeft gedaan. Dit staat bekend als *peer-to-peer mixing*. Het bekendste protocol daarvoor heet *CoinJoin*. Er zijn ook *mixing wallets*. Dit zijn bitcoinwallets waarin peer-to-peer mixing functionaliteit is ingebouwd.

Sommige peer-to-peer mixers maken gebruik van transactiepatronen die goed te herkennen zijn in de blockchain. Deze patronen kunnen worden gebruikt voor tagging.

Het is mogelijk om rechtstreeks vanuit een non-custodial wallet deel te nemen aan een peer-to-peer gemixte transactie (zie *Figuur 4*), ofwel omdat de wallet hier ondersteuning voor biedt of omdat de gebruikers samen de transactie handmatig opstellen en samen ondertekenen. Clustersoftware kan hier verkeerde conclusies uit trekken en de bronwallets samenvoegen. Dit treft alleen de wallets die betrokken zijn bij de betreffende peer-to-peer gemixte transactie.



Figuur 4 Peer-to-peer gemixte transactie

6.4. Transactietijden

Bitcoin is peer-to-peer. Er is geen centrale eenheid die bijhoudt wat wanneer gebeurt. Een transactie doorloopt verschillende stappen op verschillende momenten en kan daarbij meerdere (verschillende) tijdregistraties opleveren. Het mechanisme van de blockchain opereert relatief langzaam, het groeperen van transacties in een block duurt meerdere minuten. De definitieve bevestiging vindt plaats na enkele confirmations, wat in de praktijk tot een uur kan duren. Het heeft daarom heeft het geen zin om te spreken over één transactietijd.

Dit eerste tijdregistratie van een transactie is het moment dat de transactie wordt aangeboden op het bitcoinnetwerk en dus in de mempool van de miners terechtkomt (zie boven). Dit moment is niet voor alle miners exact gelijk. Blockchain websites zoals blockchain.com geven via de transactie explorer inzicht in deze transactietijd. Verschillende block explorer websites kunnen verschillende tijden laten zien omdat de transactie tijd nodig heeft om door verschillende deelnemers in het netwerk te bereiken.

Iedere transactie op de blockchain is (door de miner van dat block) opgenomen in een block. Het block zelf heeft ook een tijdregistratie. Deze tijd geeft de miner van het block op bij het versturen van het block. Andere nodes voeren (eenvoudige) controles uit op deze tijdregistratie.

7. Digitale gebruikerssporen

Het gebruik van wallet-software laat mogelijk digitale sporen achter op gegevensdragers en apparaten van de gebruiker.

7.1. Lokale (non-custodial) wallet-software

Het gebruik van een lokale (non-custodial) wallet-software laat verschillende digitale sporen achter. Dit kan de wallet-software zelf zijn, of bestanden waarin de gegevens (sleutelparen, outputs, transacties) in de wallet worden vastgelegd. Zulke wallet-bestanden zijn te herkennen aan de bestandslocatie, bestandsextensie, inhoud en bestandsnaam (bijv. wallet.dat, default_wallet, etc.)

Het aantreffen van een wallet-bestand betekent niet automatisch dat er dan ook over de bitcointegoeden kan worden beschikt. Vaak zijn de private sleutels (die nodig zijn voor het aanmaken van nieuwe transacties) versleuteld met een wachtwoord. Soms zijn de private sleutels helemaal niet aanwezig, en kan de wallet alleen worden gebruikt om transacties en tegoeden te bekijken (*watch-only wallet*).

7.2. Custodial wallets

Als een gebruiker beschikt over een custodial wallet, zijn de bitcointegoeden ondergebracht bij een dienstverlener. Om zo'n wallet te benaderen, is een account nodig bij die dienstverlener. Bij het gebruik van zo'n wallet-accounts via het web blijven digitale sporen achter in de browser, zoals registraties in de internetgeschiedenis van de gebruiker, browsercookies, lokale gegevensopslag van de browser, enzovoorts. Ook wanneer het wallet-account wordt benaderd via een (mobiele) applicatie, blijven daar sporen van gebruik achter.

7.3. Exchanges

Ook het gebruik van exchanges voor digitale valuta kan digitale sporen opleveren. Zo is het mogelijk e-mails van de exchanges te vinden, of internetgeschiedenis waar de website van een exchange wordt bezocht. Ook kan met blockchainanalysesoftware worden vastgesteld dat er overboekingen naar adressen van exchanges zijn gedaan.

7.4. Bitcoinadressen

Het vinden van een bitcoinadres hoeft niet te betekenen dat iemand eigenaar is van het adres, of dat iemand bij een transactie met dit adres betrokken is. Alle bitcoinadressen die gebruikt zijn, zijn publiek. Wat de vondst van een bitcoinadres betekent, hangt dus sterk af van de context waarin die wordt aangetroffen. Als er bijvoorbeeld een indicatie is dat iemand een bitcoinadres kent voordat er een transactie mee is gedaan kan dit wel duiden op eigenaarschap of voorkennis over een (voorgenomen) transactie.

7.5. Seed phrases

De eerdergenoemde seed phrases kunnen door gebruikers in verschillende vormen bewaard worden. Zo kan een gebruiker kiezen een seed phrase over te nemen in een notitie, of er een foto van maken. Doordat de woorden in seed phrases worden gekozen uit vooraf opgestelde lijsten, kunnen ze in digitaal beslag herkend worden. Het reproduceren van de correcte sleutels uit de seed phrase vergt kennis over hoe verschillende wallet software hiermee omgaat. De opsporingsdiensten en het NFI beschikken hiervoor over de benodigde kennis en software.

Op papier bewaarde seed phrases en paper wallets kunnen ook bij een fysieke zoeking worden gevonden. Als een paper wallet achterblijft op een computer, bijvoorbeeld als een verwijderd pdf-bestand, kan deze ook herkend worden in het digitaal beslag.

Voor algemene vragen kunt u contact opnemen met de Frontdesk, telefoon (070) 888 68 88. Voor inhoudelijke vragen kunt u contact opnemen met het onderzoeksgebied Forensische data-analyse van de afdeling Digitale en Biometrisch sporen.

telefoon (070) 888 6666.

Nederlands Forensisch Instituut

Ministerie van Justitie en Veiligheid

Postbus 24044 | 2490 AA Den Haag

Telefoon (070) 888 66 66

www.forensischinstituut.nl

januari 2024