

Wat is Bitcoin?

Bitcoin is een alternatief voor fiatvaluta - dat wil zeggen, echt geld. Het is een soort digitaal geld dat gebruik maakt van versleutelingstechnieken die zowel het overschrijven van gelden als de aanmaak van nieuwe bitcoins regelen. Bitcoin werkt onafhankelijk van de centrale bankautoriteiten en kent geen regelgevend of bestuurlijk orgaan. De integriteit van het systeem wordt in stand gehouden door personen of groepen, "miners" geheten, die tot taak hebben het bestaan van gelden te verifiëren middels complexe wiskundige berekeningen. Transacties vinden plaats binnen een peer-to-peer netwerk - zonder gebruikmaking van een tussenpersoon, zoals een financiële instelling.

Een bitcoinadres, ook wel een "public address" (openbaar adres) genoemd, bestaat uit 25-36 alfanumerieke en hoofdlettergevoelige karakters en begint met een één (1) of een drie (3). Deze adressen versturen en ontvangen bitcoins. Iedere transactie wordt verwerkt in een **blockchain**, een vrij toegankelijk openbaar grootboek dat de geschiedenis bijhoudt van alle geverifieerde transacties. Bitcoin transacties zijn **onomkeerbaar**. Als de gelden eenmaal zijn verstuurd, is er geen mechanisme waarmee ze terug kunnen worden gehaald. **Exchangers** (wisselaars) zijn de schakel naar het formele financiële systeem door fiat valuta om te zetten naar virtuele valuta en vice versa.

Om bitcoins te versturen, moet iemand tekenen met een privésleutel, een cryptografische handtekening waarmee wordt bewezen dat de persoon met de sleutel het recht heeft om bitcoins te versturen. Privésleutels staan opgeslagen op een computer als er gebruik

wordt gemaakt van een software wallet of op een aparte server als er gebruik wordt gemaakt van een web wallet. Ze kunnen ook worden opgeslagen op usb-sticks, versleutelde hardware, mobiele telefoon applicaties, of zelfs handmatig worden genoteerd en opgeslagen op een veilige plek.

Wereldwijd wordt bitcoin als valuta gebruikt in zowel legale als criminele financiële transacties. Het is het primaire betaalmiddel dat bij illegale transacties op het Dark Web wordt gebruikt, alhoewel er ook andere cryptovaluta op deze sites worden gebruikt. Bitcoin kan worden gebruikt om fastfood te kopen op thuisbezorgd.nl en producten aan te schaffen diverse webwinkels. Tenslotte, kunnen bitcoins worden verkregen door middel van transacties op zogenaamde bitcoinpinautomaten waarin contant geld wordt omgewisseld voor bitcoin en vice versa.

Hoe ziet een Bitcoin adres er uit

Bitcoin adressen bestaan altijd uit 25-36 hoofdlettergevoelige alfanumerieke karakters.

Voorbeeld:

1FtAaz5xIHUXrCNLbtMDqcw6o5GNn4xqX

Signalen voor gebruik van virtuele valuta door een verdachte

Er zijn meerdere signalen die er op kunnen duiden dat een verdachte gebruik maakt van bitcoin, zoals:

- De aanwezigheid van een .wallet bestand of software wallets op de computer van de verdachte.
- De browsergeschiedenis:
 - bezoeken aan wisselaars (Zie bij "Bekende Wisselaars" voor verdere bijzonderheden)
 - bezoeken aan sites die iets te maken hebben met het gebruik van virtuele valuta (Blockchain.info, CoinDesk, CryptoCoin News, CoinTelegraph, enz.).
 - bezoeken aan verkopers die virtuele valuta accepteren (vooral online Dark Markets).
 - bezoeken aan fora waar bitcoin of andere virtuele valuta worden besproken.
- Mobiele applicaties, zoals wallet providers, (Blockchain.info, Bitcoin Flapper, Bitcoin Billionaire), of wisseldiensten (ShapeShift, Coinbase, zTrader, enz.).
- Berichten op Social Media betreffende het gebruik van virtuele valuta of andere criminele activiteiten.
- Bankafschriften met betalingen aan of door wisselaars (transacties binnen het officiële bankiersysteem kunnen aanleiding zijn voor een melding Verdachte Transacties).

Waar moet op worden gelet bij een onderzoek

Wallet software – deze software wordt gebruikt voor het beheer van bitcoin op een apparaat. Als wordt vastgesteld dat er sprake is van wallet software, is het waarschijnlijk dat een verdachte zich bezig houdt met bitcoin transacties. Veelvoorkomende wallet software is onder andere Armory, Breadwallet, Electrum, GreenAddress, Multibit, en Mycelium (zie de icoontjes hieronder). Wallet software kan zowel op computers als op mobiele apparaten worden aangetroffen.



Het gebruik van een Tor Browser – Tor browsers verhullen de identiteit van gebruikers door het versleutelen en tunnelen van gegevensverkeer door wereldwijde relay-netwerken, waardoor opzettelijk IP-adressen worden verborgen. Cookies en de internetgeschiedenis worden niet opgeslagen wanneer er gebruik wordt gemaakt van Tor browsers. Bezoek aan Dark Markets op het Dark Web – Dit zijn verborgen websites waarmee gebruikers anoniem goederen en diensten kunnen aankopen – vooral illegale goederen, waaronder drugs, wapens of gegevens van gestolen credit cards. Websites op het Tor Dark Web eindigen op ".onion" (in plaats van het gebruikelijke ".com/.nl" op het open web).



Veelvoorkomende markten op het Dark Web zijn op dit moment: Dream Market en Wall Street Market, hoewel er nog veel meer zijn. Geprinte of Elektronische QR Codes – QR codes kunnen openbare en privé cryptosleutels bevatten die nodig zijn om toegang te krijgen tot bitcoin en leiden naar een specifiek adres. QR codes worden gebruikt in papieren wallets die meestal niet digitaal worden opgeslagen. Let ook op het gebruik van zogenaamde bitcoin debitcards, die worden gebruikt om bitcoins en andere cryptocurrency om te zetten naar fiat valuta. Enkele bekende aanbieders zijn: Wagecan, Cryptopay en Xapo.



Bekende Wisselaars

Bitcoin wisselaars zijn het doorgeefluik voor het omzetten van cryptovaluta in fiat valuta. Net als traditionele financiële instellingen verzamelen wisselaars in veel rechtsgebieden identificerende gegevens over hun klanten op het moment dat er een rekening wordt geopend. Veelal wordt van onderstaande wisselaars gebruik gemaakt binnen de bitcoin gemeenschap:

- Bitfinex
- Bitstamp
- Circle
- Coinbase
- Kraken
- Local Bitcoins
- Poloniex
- Xapo



Wat te doen met een onvolledig bitcoinadres

Een bitcoinadres moet leesbaar en nauwkeurig worden overgenomen, inclusief een juist gebruik van hoofdletters. Adressen zijn hoofdlettergevoelig en zelfs één afwijkend karakter kan het al onmogelijk maken het adres te identificeren. In geval van een gedeeltelijk bitcoinadres is het echter mogelijk door middel van de auto-complete optie in de verschillende tracing tools het volledige adres te achterhalen. De beste optie hiervoor biedt BlockSeer.com. WalletExplorer.com identificeert ook adressen op basis van een aantal beginkarakters, bekend als "firstbits".

Informatie

Bekijk op Intranet de pagina van de Vakgroep Virtuele Valuta. In deze vakgroep is een expert uit elke eenheid vertegenwoordigd.

<https://kort.politie.local/vakgroepvirtuelevaluta>



Soort valuta

Kenmerken van de valuta	
Bitcoin	25-36 karakters beginnend met een 1 (één) of een 3
Dash	34 karakters beginnend met een X
Dogecoin	34 karakters beginnend met de letter D
Ethereum	42 karakters beginnend met 0x
Litecoin	33 karakters beginnend met de letter L, 3 of M
Monero	Een 'raw' adres heeft 95 karakters beginnend met een 4
Ripple	34 karakters beginnend met de letter r



Kenmerken van Cryptovaluta: Gids voor Rechercheurs

Vakgroep Virtuele Valuta

<https://kort.politie.local/vakgroepvirtuelevaluta>