BITCOIN
EN
CRYPTOCURRENCY

R.M. van Schaik

Schrijver: R.M. van Schaik

Coverontwerp: BVS

ISBN: 9789465541181

Voorwoord

Het plan om een radicale, utopische, decentrale, grenzeloze en censuurbestendige vrije munt in omloop te brengen, is een kleine twee deccennia later onherkenbaar veranderd.De handel in Bitcoin of andere crypto wordt tegenwoordig strikt gereguleerd door kaders zoals MiCA, MiCAR, de CLARITY Act en DAC8. Tegelijkertijd is het technologielandschap complexer geworden; u kunt vandaag de dag simpelweg niet meer succesvol handelen zonder op de hoogte te zijn van Web3, Stacks, de 'DeFi-uitdaging' en gedecentraliseerde exchanges (DEX). Waar beleggers vroeger moesten navigeren tussen obscure websites, is er nu een Europees kader met vergunningplichtige platforms en strikte consumentenbescherming.Wie vandaag de dag actief wil zijn met Bitcoin, het analyseren van innovatieve altcoins, of het begrijpen van de onderliggende blockchain-technologie, moet deze nieuwe spelregels kennen en er terdege rekening mee houden. Overheden en toezichthouders zijn scherper dan ooit. Fiscale verplichtingen, zoals het correct opgeven van uw digitale bezittingen bij de Belastingdienst en strenge nieuwe rapportageregels zijn inmiddels de absolute standaard geworden.Met dit boek bieden wij u houvast in dit dynamische en soms overweldigende landschap. We duiken diep in het juridische en fiscale speelveld, waarbij we kijken welke betrouwbare exchanges er zijn en hoe u uw crypto optimaal beveiligt. Daarnaast leggen we uit wat de ingevoerde regels concreet betekenen voor u als belegger én voor de cryptobedrijven die uw geld beheren.

Het mysterie Satoshi Nakamoto

Aan de basis van het Bitcoin-netwerk ligt een van de grootste mysteries van de moderne digitale geschiedenis: de identiteit van de anonieme bedenker, Satoshi Nakamoto. Hoewel de publicatie van het whitepaper in 2008 en de softwarelancering in 2009 de wereld permanent veranderden, verdween Nakamoto rond 2011 spoorloos uit de publieke sfeer.

Sindsdien is de jacht op de ware identiteit achter dit pseudoniem een onuitputtelijke bron van speculatie, rechtszaken en hoaxes gebleken. Sommige hardnekkige geruchten wijzen in de richting van tech-miljardair Elon Musk als het mogelijke alter ego, maar concreet bewijs hiervoor ontbreekt tot op de dag van vandaag volledig.

Een van de meest spraakmakende figuren in deze zoektocht is de Australische computerwetenschapper Craig Wright. Jarenlang claimde hij met veel vertoon de man achter Satoshi Nakamoto te zijn, een bewering die aanvankelijk werd ondersteund door documenten die na een inval van de Australische belastingdienst bij zijn huurhuis in Sydney opdoken.

De juridische werkelijkheid bleek echter onbarmhartig. Na een slepende internationale rechtszaak oordeelde de Britse High Court dat de claims van Wright berusten op grootschalige vervalsingen.

De rechter stelde onomstotelijk vast dat Wright noch de auteur is van het whitepaper, noch de ontwikkelaar van de oorspronkelijke Bitcoin-software.

Daarmee werd zijn jarenlange bekentenis definitief ontmaskerd als een van de grootste hoaxes binnen de crypto-industrie.Terwijl de claims van Wright juridisch werden begraven, richtte de schijnwerper zich recentelijk op een andere prominente pionier.

The New York Times publiceerde een uitgebreid onderzoeksrapport waarin de Britse cryptograaf Adam Back naar voren wordt geschoven als de meest waarschijnlijke man achter het pseudoniem.

De krant baseert deze conclusie hoofdzakelijk op een diepgaande computeranalyse van zijn specifieke taalgebruik en schrijfstijl, en wijst op e-mails en publieke verklaringen van Back die onderling inconsistent zouden zijn. Hoewel de Amerikaanse kwaliteitskrant geen sluitend, hard bewijs kan overleggen, is de connectie historisch gezien niet vreemd.

Back was in een uiterst vroeg stadium betrokken bij het project; hij is immers de uitvinder van Hashcash, het fundamentele proof-of-work algoritme dat door Bitcoin wordt gebruikt om transacties te valideren.

Tegenwoordig is Back nog altijd een van de meest invloedrijke figuren binnen de cryptosector. Hij opereert als CEO van het prominente Bitcoin-technologiebedrijf Blockstream en nam onlangs tevens de leiding op zich als CEO van de Bitcoin Standard Treasury Company (BSTR), een miljardenfonds dat agressief bitcoins opkoopt om deze naar de traditionele aandelenbeurzen te brengen. Zelf blijft de Britse cryptograaf de beweringen van The New York Times resoluut ontkennen.

Volgens Back is er louter sprake van confirmation bias en zijn de gelijkenissen in stijl en visie puur toevallig, simpelweg omdat hij en Satoshi Nakamoto destijds exact dezelfde academische en cryptografische interesses deelden.

Back houdt vol dat hij zelf ook niet weet wie de ware identiteit van de bedenker is, waardoor het grootste geheim van de digitale financiële wereld vooralsnog veilig blijft in de schaduw van de blockchain.

De fundamenten en evolutie van BitcoinBitcoin is in de basis een uniek stukje digitale code dat geheel of gedeeltelijk digitaal kan worden overgedragen. Wanneer u een betaling doet, wordt deze direct doorgegeven aan een wereldwijd netwerk van gebruikers die de specifieke Bitcoin-software draaien. Feitelijk functioneert de onderliggende blockchain hierbij als een digitaal, gemeenschappelijk en openbaar grootboek voor alle registraties en transacties van eigendom.

Binnen dit netwerk staan alle transacties onomkeerbaar geregistreerd, inclusief de exacte datum en de tijd van de overdracht. De algehele beveiliging, het onderhoud en het beheer van dit systeem geschieden volledig autonoom via geavanceerde algoritmes en cryptografie. De makers en instandhouders van zo'n chain, ook wel miners genoemd, worden voor het inzetten van hun rekenkracht automatisch beloond met nieuw gegenereerde Bitcoin.De juridische status van de munt heeft internationaal de nodige fundamenten gekregen.

In de Verenigde Staten werd Bitcoin door een federale rechter officieel gekwalificeerd als een wettig betaalmiddel, een vonnis dat een eerdere cruciale gerechtelijke uitspraak uit 2014 herbevestigde. Toch is de verhouding met toezichthouders altijd complex gebleven.

De Financial Stability Oversight Council ,waarin het ministerie van Financiën, de Federal Reserve en de Securities and Exchange Commission (SEC) zijn vertegenwoordigd, uitte jarenlang grote zorgen dat de toenemende populariteit van Bitcoin de algemene financiële stabiliteit in gevaar zou kunnen brengen. Hoewel de SEC vanwege deze risico's jarenlang weigerde toestemming te geven voor een Exchange Traded Fund (ETF) die de spotprijs van Bitcoin volgt, wijzigde dit beleid begin 2024 definitief met de historische goedkeuring van de eerste spot ETF's.

Bitcoin is in zijn huidige opzet dan ook onbruikbaar als digitale munt voor dagelijkse transacties; het functioneert puur als een speculatief instrument op de kapitaalmarkt, afgeschermd door de gereguleerde ETF-schillen van Wall Street.Sinds de lancering begin 2009, toen de munt nog slechts een fractie van een cent waard was, heeft Bitcoin een ongekende transformatie doorgemaakt.

De totale cryptomarkt is inmiddels de grens van 350 miljard dollar ver gepasseerd en schommelt anno 2026 rond de 2,2 biljoen dollar, waarmee het tot de grootste activa ter wereld behoort. In deze relatief korte levensduur is het een van de meest winstgevende beleggingsproducten ooit geworden, al ging dit gepaard met extreme volatiliteit.

Zo daalde de koers begin 2021 fors door de verwachting dat de Amerikaanse centrale bank de rente sneller zou verhogen om de hoge inflatie te beteugelen.

De markt kreeg daarnaast zware klappen te verwerken door het ineenstorten, de acute liquiditeitsproblemen en de grootschalige fraude rondom de cryptobeurs FTX, inclusief de destijds mislukte overname door Binance.

Naast macro-economische factoren speelt geopolitiek een doorslaggevende rol in het netwerk. Jarenlang waren Chinese bedrijven verantwoordelijk voor ruim driekwart van alle gegenereerde Bitcoins, hoofdzakelijk omdat zij profiteerden van de spotkope energie in het land.

Deze dominantie betekende destijds dat China een flinke vinger in de pap had in de discussies over de technologische toekomst van Bitcoin.

Hoewel er in China sinds 2021 een streng en officieel verbod geldt op cryptocurrencies, bleek zelfs een gedeeltelijke legalisatie naderhand niet genoeg om de ban volledig effectief te maken.

De drijvende kracht achter de kapitaalstroom blijft hardnekkig; de actieve investeerders binnen deze regio zijn namelijk niet alleen reguliere Chinese burgers, maar met name Chinezen in zeer invloedrijke politieke en zakelijke posities.

Netwerklimieten, de 'Blocksize Wars' en geopolitieke dreigingen

De snel groeiende populariteit van Bitcoin en de explosieve toename van het aantal transacties legden al in een vroeg stadium de fundamentele grenzen van de onderliggende netwerkinfrastructuur bloot. Bitcoin-transacties worden door miners gebundeld en verwerkt in opeenvolgende 'blocks'. Deze blocks zijn in feite digitale bestanden die samen een onveranderlijk, chronologisch archief vormen. Telkens wanneer een block compleet is en cryptografisch aan de keten wordt vergrendeld, ontstaat er in het netwerk ruimte voor een volgend block. Eenmaal gevormd, kan zo'n bestand nooit meer worden aangepast, veranderd of verwijderd. Binnen het oorspronkelijke Bitcoin Core-systeem gold echter een harde, softwarematige limiet: de omvang van een block was strikt begrensd op 1 Megabyte (MB). Naarmate het netwerk intensiever werd gebruikt, waarbij op piekmomenten de capaciteit volledig werd opgesoupeerd, rees de vraag hoe Bitcoin in de toekomst miljoenen dagelijkse gebruikers kon gaan faciliteren zonder dat het systeem volledig zou vastlopen.De zoektocht naar een oplossing voor dit schaalbaarheidsprobleem hield de cryptogemeenschap jarenlang in een wurggreep en leidde tot diepe interne verdeeldheid. Een fundamentele aanpassing van de netwerksoftware door middel van grotere blocks (bijvoorbeeld van 1 MB naar 2 MB of meer) vereiste namelijk aanzienlijk krachtigere hardware van de miners. Critici vreesden dat hierdoor de drempel voor deelname te hoog zou worden, wat de toegankelijkheid en de decentralisatie van het netwerk ernstig zou aantasten.

Een vroege, radicale poging om deze limiet te doorbreken werd ondernomen door een groep ontwikkelaars onder leiding van Gavin Andresen en Mike Hearn, een voormalig software-engineer van Google. Zij introduceerden een alternatieve softwareversie onder de naam Bitcoin XT. Het doel was om de harde grens van 1 MB op te heffen; vanaf januari 2017 zouden de blocks direct worden vergroot naar 2 MB, waarna de omvang ervan elke twee jaar automatisch zou verdubbelen tot een limiet van circa 8,9 MB. Grote architectonische wijzigingen als deze moeten binnen het open-source protocol formeel worden ingediend in de vorm van een Bitcoin Improvement Proposal (BIP).

De adoptie van zo'n voorstel hangt volledig af van de miners, die hun stem uitbrengen door de nieuwe programmacode al dan niet op hun computers te installeren.Voor het slagen van Bitcoin XT was een overweldigende meerderheid van 75 procent van de rekenkracht vereist. Omdat oudere mining-computers niet zomaar met het nieuwe, variabele protocol overweg konden, stonden miners voor een disruptieve keuze: twee systemen naast elkaar draaien of het risico lopen om volledig buiten de boot te vallen. De angst dat deze splitsing de definitieve nekslag voor Bitcoin zou betekenen, veroorzaakte in de zomer van 2015 een tijdelijke flash crash op de beurzen. Uiteindelijk wees de markt de software van Bitcoin XT resoluut af en weigerden de nodes de upgrade te accepteren, waarna een gedesillusioneerde Mike Hearn de cryptowereld definitief achter zich liet.

Toch bleef de noodzaak voor modernisering onverminderd groot, wat leidde tot verschillende alternatieve scenario's en felle debatten rondom concepten als Bitcoin Unlimited, SegWit2x en BIP148.Om de transacties sneller te kunnen verwerken zonder de blockgrootte direct fysiek te verdubbelen, werd uiteindelijk gekozen voor een softwarematige optimalisatie via het voorstel BIP141, beter bekend als Segregated Witness (SegWit).

SegWit2x kwam op in mei toen de Digital Currency Group (DCG) een artikel publiceerde genaamd “Bitcoin Scaling Agreement At Consensus 2017.” Volgens het artikel ondersteunen de gebruikers een paralelle upgrade gebaseerd op het Segwit2Mb voorstel met een behoud van 80% van de reeds gecreëerde munt met een activering van een 2 MB harde splitsing (fork) binnen zes maanden.

Mike Belshe, Wences Casares, Jihan Wu, Jeff Garzik, Peter Smith and Erik Voorhees waren de grondleggers. Volgens het artikel wordt het nieuwe systeem gesteund door 56 bitcoin bedrijven in 21 landen, 83.28% van de hashing kracht (miners), SegWit2x is inmiddels afgeblazen.

Door de activatie van SegWit werden de handtekeninggegevens losgekoppeld van de transactiedata. Hierdoor konden betalingsopdrachten veel efficiënter worden gecomprimeerd, waardoor er simpelweg aanzienlijk meer transacties in één traditioneel betalingsblock pasten.

Wanneer een consensus over dergelijke software-updates uitblijft, resulteert dit onvermijdelijk in een zogeheten hard fork: een onomkeerbare splitsing van de blockchain waarbij een geheel nieuwe, concurrerende munt ontstaat.

Een historisch sleutelmoment vond plaats op 3 augustus 2017, toen ontevreden groeperingen zich afsplitsen en de munt Bitcoin Cash (BCH) lanceerden. Speculanten en handelaren doken via grote valutaplatforms zoals Bitfinex en Bittrex direct op de nieuwe asset, al bleek de markt uiterst volatiel; amper een dag na de lancering verloor Bitcoin Cash alweer dertig procent van haar waarde.

Een vergelijkbare dynamiek herhaalde zich met de introductie van Bitcoin Gold (BTG). Deze afsplitsing werd eveneens via een hard fork operationeel gemaakt.

Het mechanisme achter zo'n splitsing creëerde telkens een unieke marktdynamiek: iedereen die op het moment van de fork in het bezit was van Bitcoin en de controle had over zijn eigen privésleutels of een ondersteunende webwallet, ontving automatisch een gelijke hoeveelheid van de nieuwe valuta.

Deze belofte van 'gratis geld' zorgde destijds voor een enorme kapitaalstroom. Actieve bezitters leverden massaal hun reguliere alternatieve munten (altcoins) in om extra Bitcoins te vergaren en zo optimaal te speculeren op de uitkomst van de splitsing, wat de koers van de originele Bitcoin in die periodes tot recordhoogtes opstuwde.Voor de gemiddelde Nederlandse belegger is de toegang tot deze markt inmiddels sterk geprofessionaliseerd.

BIP148

Ondertussen beoogde BIP148 een aanvullende “zachtere” oplossing die 1 augustus 2017 zou starten. Het zachtere systeem zou moeten worden versterkt door de zogenaamde full nodes (computer). The UASF is ontworpen om de bestaande SegWit MASF (miner activated soft fork) te starten waarbij ook de miners moeten instemmen. Door Segwit2x en BIP148 na elkaar te starten zou stabiliteit gewaarborgd worden.

Waar men vroeger aangewezen was op ingewikkelde buitenlandse platformen, kan Bitcoin tegenwoordig rechtstreeks worden aangekocht via gespecialiseerde online dealers en brokers, waarbij de betaling eenvoudig en direct wordt afgehandeld via vertrouwde methoden zoals iDEAL of een creditcard.Wie echter puur wil speculeren op de felle prijsbewegingen zonder de digitale munten daadwerkelijk zelf te hoeven bezitten, te beveiligen of over te boeken, wijkt vaak uit naar een zogeheten CFD-broker. Door gebruik te maken van dit Contract for Difference (CFD) wordt er belegd in een financieel derivaat dat de onderliggende koers volgt.

Dankzij het ingebouwde hefboomeffect van zo'n CFD-product wordt elke stijging of daling van de Bitcoin-koers met een vooraf bepaalde factor versterkt. Dit biedt kansen op exponentiële winsten bij een juiste voorspelling, maar stelt de onervaren belegger tegelijkertijd bloot aan het acute risico op het verlies van de volledige inzet bij een plotselinge trendbreuk.

Ondanks deze vergaande commercialisering en beursproducten, blijft de onderliggende structuur van Bitcoin kwetsbaar voor zowel interne monopolies als externe geopolitieke agressie.

Een grote existentiële dreiging voor de decentralisatie openbaarde zich toen de gigantische miningpool GHash op een zeker moment meer dan vijftig procent van de totale computerkracht van het netwerk in handen kreeg.

Een dergelijke centralisatie geeft één enkele partij theoretisch een monopoliepositie, waarmee zij kwaadwillende macht kunnen uitoefenen op het systeem door transacties te blokkeren of terug te draaien.

Daarnaast is Bitcoin aan de buitengrens het doelwit geworden van staatsactoren. In Noord-Korea worden bitcoins door het regime in Pyongyang op grote schaal gegenereerd met behulp van speciaal ontwikkelde software.

Bovendien worden internationale handelsplatformen systematisch en agressief gehackt door Noord-Koreaanse staatshackers om buitenlandse valuta te stelen en zo de internationale economische sancties tegen het land te omzeilen.

Het bewijst dat de strijd om Bitcoin zich allang niet meer alleen afspeelt op de tekentafels van softwareontwikkelaars, maar dat het netwerk permanent blootstaat aan de wetten van de mondiale machtspolitiek en cyberoorlogen.

Schaarste, kritiek en de quantumuitdaging

In de nacht van 19 op 20 april 2024 vond een cruciaal evenement plaats in het Bitcoin-netwerk: de beloning voor miners werd voor de vierde keer in de geschiedenis gehalveerd. Zo'n 'halving' vindt automatisch plaats na elke 210.000 gemijnde blokken, wat in de praktijk ongeveer vier jaar duurt.

Dit mechanisme garandeert de absolute schaarste van de munt, aangezien er in totaal nooit meer dan 21 miljoen bitcoins in omloop kunnen worden gebracht.

Ondanks deze ingebouwde schaarste blijven traditionele financiële instellingen sceptisch. Onderzoekers van de Europese Centrale Bank (ECB) tonen zich herhaaldelijk uitermate negatief over Bitcoin en stellen dat de digitale munt fundamenteel geen enkele waarde vertegenwoordigt.

Daarnaast ligt de munt constant onder een vergrootglas vanwege de ecologische voetafdruk; het wereldwijde 'minen' van Bitcoin kost op jaarbasis immers evenveel elektriciteit als het totale verbruik van alle huishoudens in landen als Griekenland of Australië.Naast de discussie over energieverbruik en economische waarde, dient zich aan de technologische horizon een nieuwe uitdaging aan: de quantumdreiging. Analisten schatten dat de cryptosector nog ongeveer drie tot vijf jaar heeft om zich voor te bereiden op de overstap naar quantum-resistente oplossingen.

Quantumcomputers werken fundamenteel anders dan de klassieke computers die we nu kennen. In plaats van traditionele bits maken zij gebruik van qubits, waardoor zij in staat zijn om gigantische hoeveelheden complexe berekeningen tegelijkertijd uit te voeren.

Hoewel dit een beheersbare technologische uitdaging is, betekent het wel dat deze computers in de toekomst de cryptografische systemen zouden kunnen doorbreken die vandaag de dag nog als onkraakbaar worden beschouwd.

Omdat de recente technologische vooruitgang de verwachte tijdlijn voor deze dreiging heeft verkort, staat het onderwerp inmiddels weer volop in de schijnwerpers. Het risico van deze quantumrevolutie is echter niet gelijk verdeeld over het Bitcoin-netwerk, waardoor niet elke bitcoin in dezelfde mate is blootgesteld aan een toekomstige quantumaanval. De grootste kwetsbaarheid ligt bij de zogeheten legacy wallets. Dit zijn oudere walletstructuren die beduidend minder bescherming bieden dan moderne varianten.

Specifiek de vroege P2PK-adressen (Pay-to-Public-Key), waarbij de publieke sleutels permanent zichtbaar zijn op de blockchain, vormen een risicogebied. In dit specifieke segment bevindt zich naar schatting ongeveer 1,7 miljoen Bitcoin, waaronder de circa 1,1 miljoen bitcoins die worden toegeschreven aan de mysterieuze oprichter Satoshi Nakamoto.

Ook adressen waarvan de publieke sleutel al een keer op het netwerk is getoond, of adressen waarbinnen sleutels onveilig worden hergebruikt, lopen een groter risico.

Dit betekent dat de quantumdreiging in eerste instantie vooral impact heeft op deze oudere, statische coins en specifieke adresstructuren, en niet direct op de veiligheid van het volledige netwerk.

Het miningproces zelf is bijvoorbeeld geen groot zwak punt. De SHA-256-hashing die voor het minen wordt gebruikt, lijkt volgens experts niet op dezelfde manier vatbaar voor quantumaanvallen als de walletbeveiliging.

De discussie binnen de community richt zich daarom voorlopig hoofdzakelijk op veilige opslag en modern adresbeheer, in plaats van op het functioneren van de blockchain als geheel.Bitcoin beschikt zodoende over voldoende tijd en organisatorische slagkracht om zich tijdig aan te passen. Dankzij het open-source karakter van het protocol kunnen ontwikkelaars en de bredere community de software tijdig upgraden en overstappen op quantum-resistente cryptografische standaarden voordat de dreiging kritiek wordt.

De conclusie is dan ook dat de quantumdreiging weliswaar serieus moet worden genomen, maar niet moet worden overdreven; het is een technisch probleem dat met de juiste en tijdige aanpassingen volledig beheersbaar blijft.

Extreme volatiliteit

De extreme beweeglijkheid van de cryptomarkt werd in de opeenvolgende jaren herhaaldelijk bewezen. Na eerdere crises beleefde de markt in 2025 een ongekende opmars, grotendeels aangejaagd door een groeiende vraag van beursgenoteerde bedrijven die strategisch digitale tokens op hun balans bleven opbouwen.

Medio augustus 2025 noteerde Bitcoin al een waarde van ruim 124.480 dollar, een opwaartse trend die zich doorzette tot een historische recordhoogte van 125.245 dollar begin oktober. De absolute piek werd uiteindelijk in november 2025 bereikt, toen de munt een astronomische recordstand van 126.000 dollar aantikte.

Vanaf dat moment sloeg het marktsentiment echter abrupt om en startte een langdurige correctie.De ommekeer zette definitief in halverwege oktober, waarna de koers eind november 2025 hard terugviel tot ongeveer 86.900 dollar.

Toegenomen geopolitieke spanningen tussen de Verenigde Staten en China, gecombineerd met een brede afwaardering van oververhitte AI-aandelen op de traditionele beurzen, zorgden voor grote onrust onder investeerders. Binnen een tijdsbestek van slechts enkele uren verdampte de volledige jaarwinst toen de koers met zeven procent kelderde. In de vroege ochtenduren werd een dieptepunt van 85.600 dollar bereikt.

Deze korte maar heftige crash werd veroorzaakt door een kettingreactie van automatische liquidaties van long-posities tijdens een moment van lage handelsactiviteit, waarbij in totaal voor 471 miljoen euro aan posities werd weggevaagd. De stijgende Japanse rente fungeerde hierbij als katalysator, omdat dit de kans vergrootte dat de Bank of Japan haar langdurige beleid van goedkoop geld radicaal zou verkrappen.

Hoewel de koers medio december nog kortstondig opklom naar 89.700 dollar door een belangrijk steunniveau tussen de 83.000 en 85.000 dollar, bleek de verkoopdruk aan het begin van het nieuwe jaar onhoudbaar.

Januari 2026 luidde de vierde opeenvolgende maand met koersverlies in. De langste verliesreeks voor Bitcoin sinds 2018. De waarde zakte die maand met bijna 11 procent tot onder de 76.000 dollar, wat destijds een daling van 40 procent betekende ten opzichte van de piek in november.

De neerwaartse spiraal versnelde in februari 2026, toen de koers achtereenvolgens onder de grens van 70.000 dollar zakte en op 23 februari zelfs wegzakte naar een dieptepunt van 56.168 dollar.

Daarmee beleefde Bitcoin zijn slechtste maand sinds de zomer van 2022, waarbij de waarde van de cryptomunt in feite was gehalveerd ten opzichte van het recordniveau.

Richting het voorjaar van 2026 bleef de markt uiterst fragiel en gevoelig voor mondiaal nieuws. Hoewel de koers eind maart 2026 weer enigszins herstelde naar zo'n 66.690 dollar, werd er direct daarna opnieuw 128 miljard dollar aan marktwaarde uit de totale cryptomarkt weggevaagd na berichten over militaire aanvallen op Iran.

Begin april 2026 reageerde de markt wederom negatief op scherpe geopolitieke uitlatingen van Donald Trump over Iran, waardoor de koers binnen een dag met 2,5 procent daalde tot ongeveer 66.500 dollar.

Deze opeenvolging van gebeurtenissen onderstreept dat Bitcoin in een volwassen markt weliswaar institutioneel wordt geadopteerd, maar tegelijkertijd functioneert als de ultieme seismograaf voor macro-economische en geopolitieke wereldwijd schokken.

De koesr lag 20 augustus 2026 weer rond de 70.000 dollar na stappen van de Amerikaanse minister van Financiën Scott Bessent om de Amerikaanse obligatierentes te verlagen. De koers steeg zelfs even tot boven de 72.000 dollar, het hoogste niveau sinds begin juni. Ook andere cryptomunten gingen mee omhoog. Ze stegen mee met risicovolle beleggingen nadat Washington met plannen kwam om meer langer lopende Amerikaanse staatsleningen terug te kopen. Trump had een ontmoeting met kopstukken van bedrijven als Coinbase, Payward en Blockchain.com. Dit wakkerde het optimisme aan dat de zogeheten Clarity Act er binnenkort toch gaat komen. Die wet voor de regulering van de cryptomarkt werd onlangs op het laatste moment toch niet in stemming gebracht in de Senaat.

De integratie van cryptovaluta in het traditionele financiële systeem laat inmiddels duidelijke sporen na bij zowel beursgenoteerde bedrijven als centrale banken.

MicroStrategy, dat inmiddels zijn naam heeft ingekort tot Strategy, was destijds een van de absolute pioniers die Bitcoin opnam in de strategische bedrijfsreserves. Het concern heeft in de loop der jaren een gigantische positie opgebouwd en bezit inmiddels meer dan 72 miljard dollar aan Bitcoin.

Toch bewijst de dynamiek rondom het aandeel Strategy hoe volatiel deze markt blijft; ondanks de eerdere recordkoersen van de onderliggende munt, verloor het aandeel sinds de piek in juli bijna twintig procent van zijn waarde.

Een vergelijkbaar patroon was zichtbaar bij de Japanse hotelketen Metaplanet. Als prominente houder van circa 2,2 miljard dollar aan Bitcoin zag deze keten haar eigen aandelenkoers sinds medio juni met ongeveer vijftig procent dalen.Tegelijkertijd bereikte de adoptie een historische mijlpaal binnen de muren van overheidsinstituten.

De Tsjechische Nationale Bank (CNB) schreef geschiedenis als de eerste centrale bank wereldwijd die besloot om Bitcoins en andere cryptomunten aan te kopen.

De CNB lanceerde hiertoe een testportefeuille ter waarde van 1 miljoen dollar, strategisch gevuld met Bitcoin, een aan de Amerikaanse dollar gekoppelde stablecoin en een getokeniseerde deposit. Om geopolitieke en binnenlands-politieke spanningen te vermijden, werden de aankopen bewust via een gereguleerde exchange buiten de officiële reserves om gedaan. Het primaire doel van dit project, dat over twee tot drie jaar geëvalueerd zal worden, is het opdoen van praktische ervaring met blockchain-technologie voor toekomstige betalingen en investeringen. Hoewel Tsjechië EU-lid is, maakt het geen deel uit van de eurozone, wat de bank meer operationele vrijheid gaf voor dit passieve experiment. In navolging van dit Europese initiatief maakte ook de centrale bank van Taiwan plannen bekend voor een soortgelijk Bitcoin-proefproject.

Naast deze institutionele groei toont de praktijk aan dat de arm van de wet steeds langer wordt in de digitale ruimte. In de grootste crypto-inbeslagname uit de Amerikaanse geschiedenis hebben de autoriteiten van de Verenigde Staten en het Verenigd Koninkrijk voor ruim 15 miljard dollar aan Bitcoin geconfisqueerd. Het ging hierbij om maar liefst 127.000 bitcoins die toebehoorden aan een omvangrijke internationale oplichtersbende onder leiding van de Brits-Cambodjaanse Chen Zhi. Via het malafide bedrijf Prince Group werden slachtoffers wereldwijd verleid om vermogen te investeren in crypto onder de valse belofte van gegarandeerde winsten. In werkelijkheid werd de inleg misbruikt voor excessieve luxe-uitgaven.

De organisatie maakte op grote schaal gebruik van callcenters waar dwangarbeid plaatsvond en stuurde duizenden nepaccounts op sociale media aan om slachtoffers te manipuleren. Chen Zhi, die wordt verdacht van grootschalige fraude en witwassen, riskeert inmiddels een gevangenisstraf van maximaal veertig jaar.

Dat gestolen crypto niet langer definitief onvindbaar is, bewijst ook de zaak rond Bo Shen, mede-oprichter van durfkapitaalbedrijf Fenbushi Capital. Hij loofde een aanzienlijke beloning uit van tien tot twintig procent van het totale bedrag, wat kan oplopen tot miljoenen dollars, voor cruciale informatie die leidt tot het herstel van ongeveer 42 miljoen dollar aan digitale activa. Dit fortuin verdween destijds uit zijn persoonlijke wallet na een hack en bestond specifiek uit 38,2 million dollar in de stablecoin USDC, 1.607 Ethereum, 720.000 USDT en ruim 4 Bitcoin.

Hoewel de buit destijds via exchanges en cryptodiensten zoals ChangeNow en SideShift werd weggesluisd om het spoor te wissen, hebben blockchain-analysten zoals ZachXBT en Taylor “Tayvano” Monahan recentelijk al 1,2 miljoen dollar weten veilig te stellen.Uit onderzoek van cybersecuritybureau SlowMist bleek dat de diefstal vermoedelijk werd veroorzaakt door een gelekte seed phrase, de unieke reeks back-upwoorden die volledige controle geeft over een wallet.

Waar de opsporingsmogelijkheden destijds beperkt waren, maakt de sector vandaag de dag gebruik van geavanceerde analysetools en kunstmatige intelligentie om complexe geldstromen dwars door verschillende blockchains te traceren en patronen te herkennen.Hoewel het terughalen van gestolen crypto een complexe uitdaging blijft, laat deze heropende zaak zien dat de technologische evolutie aan de kant van de opsporingsdiensten en blockchain-forensici de overhand begint te krijgen.Dat de noodzaak voor streng toezicht en betere beveiliging geen theoretische kwestie is, bewijzen de harde cijfers over diefstal en fraude binnen de sector. In 2023 werd er wereldwijd voor ongeveer 1 miljard dollar aan crypto gestolen. Volgens gezaghebbende securityrapporten ging er in die specifieke maand 26 miljoen dollar verloren aan zogeheten exit scams, waarbij projectontwikkelaars er plotseling met het geld van investeerders vandoor gingen, 6,4 miljoen dollar aan manipulatie via flash loans en ruim 13,5 miljoen dollar aan directe exploits, waarbij cybercriminelen misbruik maakten van kwetsbaarheden in de programmacode van smart contracts.

De geschiedenis van grootschalige cryptodiefstal kent echter nog diepere wortels die de markt destijds op haar grondvesten lieten schudden.

Een van de meest beruchte vroege cyberaanvallen vond plaats op 5 juli 2016, toen de destijds toonaangevende bitcoinbeurs Bitfinex werd gehackt.

Aanvallers wisten toen maar liefst 119.756 bitcoins buit te maken, wat destijds een nominale waarde vertegenwoordigde van zo'n 62 miljoen euro. De onmiddellijke paniek op de markten zorgde ervoor dat de Bitcoin-koers destijds in korte tijd kelderde van 650 dollar naar 540 dollar per munt.

Bitfinex maakte destijds nota bene gebruik van een geavanceerd beveiligingssysteem met meerdere digitale handtekeningen (multi-signature wallets). Dit systeem had het ongeautoriseerd overmaken van dergelijke immense hoeveelheden coins feitelijk moeten blokkeren, maar door een cruciale fout in de configuratie functioneerde deze barrière niet.

De combinatie van hacks, strenger toezicht en operationele misstappen heeft er in de loop der jaren toe geleid dat veel vroege platformen de deuren moesten sluiten. Een sprekend voorbeeld hiervan is het eerdere echec rondom Bittrex.