# BLOCKCHAIN

Blockchain is een transparant, decentraal, online (programmeerbaar) register. In het geval van Bitcoin ziet computerrekenkracht toe op de juistheid van het register(aanpassingen). Alle deelnemende computers strijden om het eerst een aanpassing (nieuwe block) goed te keuren. Zo wordt onderzocht of de aanpassing conform de historiek en de regels van de ketting gebeurt. De winnaar ontvangt een stukje bitcoin als vergoeding. Omdat heel de wereld decentraal en transparant online kan meekijken kan fraude met de ketting uitgesloten worden. Dit principe noemt men proof of work. Alleen als 51% van de rekenkracht bewust wil frauderen, kan dit theoretisch gebeuren en kan een niet-conforme aanpassing plaatsvinden. De hele wereld zal dit echter weten (ook omdat de chronologie niet meer kan kloppen) en de fraudeurs zullen er dus niet mee wegkomen. Desgevallend scheuren de anderen zich af in een harde fork. Mogelijks verliezen de fraudeurs hun investering indien dit in het protocol voorzien is.

Bitcoin kan aanzien worden als digitaal goud, ook omdat er slechts een vaste hoeveelheid van bestaat. Je kan je paswoord evenwel verliezen of je account kan gehackt worden. Dit laatste kan niet gebeuren bij fysiek goud. Cryptomunten koppelen aan fysiek goud lijkt ons inziens ook gedoemd omdat een centrale autoriteit dan moet toezien op die koppeling. Hierdoor ben je niet meer zeker dat je als de nood hoog is effectief je verwachte goud ontvangt.

Het probleem met proof of work is dat dit heel veel energie vraagt. Schattingen over het energieverbruik om bitcoin te onderhouden lopen op tot het totale electriciteitsverbruik van een land als Nederland. Een bijkomend probleem is dat het lang kan duren alvorens alle berekeningen en checks zijn gebeurd en dus ook lang duurt om een transactie goed te keuren. Als oplossing is Cardano gekomen. Dit is de snelle bitcoin die werkt met proof of stake en de anonimiteit garandeert door met een UTxo verificatie programma te werken. Toepassingen hiervan zijn bijvoorbeeld een database van universiteitsdiploma's.

Anderen werken nu ook met proof of stake. De bezitters van de munt die de blockchain onderhoudt of valideert, krijgen daarvoor een kleine vergoeding. Ethereum is zo een voorbeeld. Validatie van de Ethereum blockchain gaat veel sneller en verbruikt bijna geen energie. De bezitters moeten wel bereid zijn om hun munt Ether in te zetten in het proces en bij fouten kunnen zij hun inzet verliezen. (De ontwikkelaars bepaalden hoeveel Ether er jaarlijks moet bijkomen om een redelijke vergoeding te betalen aan hen die de veiligheid van de blockchain garanderen.) Ook hier kan de 51% aanval plaatsvinden. De grootste individuele staking pool is Lido met circa 30% marktaandeel. Theoretisch zou Lido dus samen met enkele andere staking pools zo een aanval kunnen inzetten. Zij zouden dan ook vele tientallen validators, die het eigenlijke werk doen en met wie de staking pools hun vergoeding ( circa 10 % van de staking vergoeding) doorgaans op 50/50 basis delen, moeten omkopen. De hele wereld zal dit hier echter ook weten en de fraudeurs zullen er dus niet mee wegkomen. Bovendien wordt binnen de ethereum gemeenschap nagedacht om staking pools te beperken tot circa 33%. LDO, de munt achter Lido, zou je dus als een aandeel in het bedrijf Lido kunnen beschouwen. Het keert (nu nog) geen dividend uit maar de winsten accumuleren daar wel.

Ethereum is open source en kan dus relatief eenvoudig gecopieerd worden. Dit noemt men een hard fork. Door de netwerkeffecten heeft dit geen zin. De developers zullen blijven waar iedereen zit en de meest (d)apps zijn. Ingeval van fraude, zoals hierboven beschreven, kan dit wel zin hebben. Niemand bezit een blockchain. Het is een sociaal contract dat evolueert door de massa's.

Door zijn grote schaal en zijn gebruikte protocol zou Ethereum dus wel eens het perfecte vehikel kunnen worden voor CBDC. Geïnteresseerden kunnen een basisinkomen in Ether bekomen en de overheid kan dit gedragsafhankelijk maken. Het adres van de burger is gemakkelijk terug te vinden, omdat ethereum als een accounting programma werkt (Cardano daarentegen werkt als verificatie programma UTxo en het bijkomend bezit zit decentraal), en zijn bezit dus ook. Cardano kan terughalen hoe dit bezit tot stand is gekomen en welke Cardano (ANA) wordt uitgegeven. Bij Ethereum is dit laatste moeilijker. Voor de overheid maakt dit niet uit, want zij bepalen de regels en kunnen een ethereum account desgevallend afsluiten bij ongewenst gedrag. Ethereum kan dus gebruikt worden om crypto fiat munten te lanceren. Cardano lijkt meer gebouwd om een crypto goud standaard te lanceren of een niet-corrumpeerbare database op te zetten. Zo zou het ook kunnen gebruikt worden om free speech te garanderen in berichten. Censuur kan zo uitgesloten worden omdat er geen centraal toezicht meer is. Zo kan ook muziek gedistribueerd worden zonder poortwachters uit de muziekindustrie. Cardano is performanter dan Ether maar heeft minder netwerkeffecten.

Ethereum kan ook gebruikt worden voor smart contracts met data die on-chain zijn. Deze supercomputer zou wel eens nuttig kunnen worden voor het bedrijfsleven en zijn munt zou wel eens het privégeld van de toekomst kunnen worden. Chainlink koppelt data off-chain aan data on-chain en kan zo smart contracts laten uitvoeren zonder dat er een centrale autoriteit of rechtbank nodig is om ze te laten uitvoeren of afdwingen. Zo kan een verzekeringsmaatschappij overgaan tot betaling van een landbouwer wanneer diverse betrouwbare leveranciers van temperatuurdata vaststellen dat de temperatuur op een akker boven bijvoorbeeld 50°C is gegaan. Zo kunnen insecticidedrones uitvliegen indien bijvoorbeeld slakken op gewassen worden vastgesteld middels camera's. Van LINK zijn ook slechts een beperkt aantal tokens beschikbaar.

Non-interactieve Zero-Knowledge roll-ups, zoals Polygon en ZKSync, gaan dan weer een belangrijke rol spelen bij het echt opschalen van Ethereum. Ze maken een parallelle Ehereum equivalente chain mogelijk. Er zullen er tientallen ontstaan. Zo blijft voor ontwikkelaars alles hetzelfde en kunnen deze subchains een kleine blok toevoegen met miljoenen transacties waarvan alleen meegedeeld wordt dat de inhoud juist is. Ook hier spelen publieke, transparante algoritmen een rol zodat proofer en verifier elk een bepaald algoritme draaien waarvan de uitkomst enerzijds bevestigt dat de inhoud juist is en anderzijds dat de inhoud gekend is zonder dat de verifier weet wat de inhoud is. Bovendien weet niemand anders met zekerheid of er een bewijs geleverd is of het in scene gezet is door proofer en verifier. Alleen de betrokkenen weten dit. Een intuïtief voorbeeld is de speciale grot van Alibaba in lusvorm. Toepassingen zijn hier bijvoorbeeld geheime stemmingen, anonimiseren van financiële transacties.

Quant, dat draait op Ethereum, is dan weer ver in het bouwen van infrastructuur voor central bank digital currencies,

Ethereum kan ook gebruikt worden om activa te vermarkten. Je kan een (stuk van) (digitaal) kunstwerk verkopen of aandelen in een bepaald bedrijf naar de markt brengen zonder centrale beursautoriteit. Je kan eigenaars van vastgoed registreren en huurders verplicht via blockchain laten reserveren zodat overheid in alle transparantie belasting kan heffen.

Gaming competities en een bijhorende ranglijst kan ook via blockchain gebeuren.

Aktes bij notarissen is een andere mogelijke toepassing.

Blockchains kunnen ook helpen om terug een echt vrije en eerlijke concurrentie te creëren waar de wijsheid van alle economische actoren (ook de kleine) de uiteindelijke uitkomst bepaalt.

Joost Olbrechts

Karakter Invest 2022