Publicatie : AG Connect
Datum : 29 feb 2020
cm2 : 2.264
Pagina : 32
Advertentiewaarde : € 28.350,00
Regio : Nederland
Frequentie : 10x per jaar
Oplage : 8.000

SUPER SCIENCE

DAVID CHAUM

DAVID CHAUM IS DE GRONDLEGGER VAN DE BLOCKCHAIN-TECHNOLOGIE, PIONIER IN DIGITAAL GELD EN ZEER GEWAARDEERD CRYPTOGRAAF EN COMPUTERWETENSCHAPPER. HIJ RICHTTE DE INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH OP, EN BEGIN JAREN TACHTIG BIJ HET CENTRUM WISKUNDE & INFORMATICA (CWI) IN AMSTERDAM DE ONDERZOEKSGROEP CRYPTOLOGIE.

door Tanja de Vrede beeld Inge Hoogland

GRONDLEGGER VAN DE BLOCKCHAIN, DAVID CHAUM

30 jaar voorsprong op bitcoin

EEN BELANGRIJKE DRIJFVEER VOOR HEM WAS EN IS ZIJN OVERTUIGING DAT BURGERS HUN DIGITALE LEVENS ZO VEEL MOGELIJK BUITEN DE MACHTSSFEER VAN OVERHEDEN KONDEN LEIDEN. En wel door zo anoniem mogelijk op het internet te kunnen verkeren, dus zonder digitale sporen achter te laten. Dat resulteerde niet alleen in het bedrijf DigiCash, dat met eCash de bitcoin jaren vooruit was, maar ook in initiatieven om veilig digitaal te kunnen stemmen, onder meer voor de Raad van Europa en enkele Amerikaanse steden.

Al in 1982 legde David Chaum met het multiparty-computation protocol de fundamenten voor de blockchain vast in zijn dissertatie 'Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups'.

Hierbij leverde Chaum ook code om het protocol te implementeren. Met de toevoeging van Satoshi Nakamoto in 2008, die het probleem van mogelijk dubbele betalingen oplost met de introductie van nodes/proof of work, leverde dat de blockchaintechnologie op die gebruikt wordt voor de bitcoin.

ANONIEME COMMUNICATIE

Chaum legde met zijn publicaties in het begin van de jaren tachtig al de basis voor het onderzoek naar anonieme communicatie. In zijn dissertatie uit 1982 beschreef hij hoe opgeslagen en gecommuniceerde data beschermd kunnen blijven terwijl maar één klein mechanisme,

Publicatie : AG Connect
Datum : 29 feb 2020
cm2 : 2.264
Pagina : 32
Advertentiewaarde : € 28.350,00
Regio : Nederland
Frequentie : 10x per jaar
Oplage : 8.000

CRYPTOMUNT PRAXXIS: 'SNELLER EN KWANTUMVEILIG'

Chaum werkt in zijn eigen bedrijf Elixxir met rond de 40 medewerkers aan een nieuwe digitale munt, gebaseerd op blockchain uiteraard. Deze munt, Praxxis, is sneller dan bitcoin, waardoor hij beter geschikt zou zijn voor grote aantallen betalingen tegelijk. Daarnaast is hij ook bestand tegen mogelijke hacks met een kwantumcomputer. Chaum: "We werken met een zeer basale vorm van encryptie. Dat blijft veilig, ook bij aanvallen door kwantumcomputers, als je maar sleutels hebt die groot genoeg zijn. Dat is echt alles wat je hiervoor nodig hebt."

Van groot belang hierbij is Elixxir, een communicatietechnologie die de communicatie versleutelt en geen sporen en dus geen metadata achterlaat. Praxxis is zo veel sneller dan bitcoin doordat het met 'fractional endorsement' werkt, waardoor een transactie goedgekeurd kan worden zonder de complete blockchain daarbij te betrekken. Bij een bitcointransactie moet een mutatie wel aan de hele blockchain worden gemeld, en dat kost veel tijd. De digitale sporen ontbreken doordat elke transactie opgeknipt wordt in een groot aantal kleine tokens waarvan de herkomst niet wordt vermeld.

Publicatie : AG Connect
Datum : 29 feb 2020
cm2 : 2.264
Pagina : 32
Advertentiewaarde : € 28.350,00
Regio : Nederland
Frequentie : 10x per jaar
Oplage : 8.000

een zogeheten vault, ook echt fysiek beveiligd hoeft te zijn. Als die vault gecontroleerd en 'verzegeld' is, zal elke poging om die vault te openen ertoe leiden dat de informatie erin wordt vernietigd. Daardoor is de aanval nutteloos.

DE GROTE MAN

Nakamoto, waarvan eigenlijk niemand weet wie dat is, staat dan wellicht te boek als de grote man achter blockchain, maar inmiddels komt er steeds meer erkenning voor Chaums betekenis voor blockchain. Zo kreeg hij onlangs nog het Dijkstra Fellowship van het CWI toegekend. Want Chaum is ook voor het CWI van grote betekenis geweest. Hij was vanaf midden jaren tachtig verbonden aan het CWI in Amsterdam. Omdat hij zijn eigen bedrijf DigiCash startte en de mogelijke indruk van belangenverstrengeling wilde vermijden, maakte hij zich los van het CWI. Maar de wederzijdse waardering bleef. Chaum ontwikkelde diverse cryptografische protocollen, zoals blind signature, mix networks en het dining cryptographers protocol. Zijn onderzoeken in Berkeley en het CWI leverden vooral theoretische resultaten op. Praktisch heeft Chaum er nooit wat mee gedaan, benadrukt hij. "Er zijn wel mensen en organisaties geweest die het gebruikt hebben in simpele cases." Chaum richtte in 1990 DigiCash op, dat in Amsterdam was gevestigd, vlak bij het CWI. Tientallen jaren voor de bitcoin kwam hij al met een digitale munt: eCash. Hiermee konden kleine betalingen anoniem gedaan worden op internet. Hij was zijn tijd echter te ver vooruit, waardoor eCash niet goed van de grond kwam.

DE GROOTSTE THRILL VAN ZIJN LEVEN

David Chaum mag dan tientallen jaren geleden het fundament voor de blockchain hebben gelegd, veel erkenning heeft hij er tot nu toe niet voor gekregen, hoewel dat nu langzaamaan wel toeneemt. Van Nakamoto is hem niet bekend of die zijn werk kende en zich daarop heeft gebaseerd. In elk geval heeft hij daar "geen commentaar" op. "In mijn werk mist wel de PoW (proof of work). Maar die heb je alleen nodig voor bitcoin. En dat heeft IBM uitgevonden." En ook op de vragen of hij weet wie Nakamoto is en of hij dat misschien zelf is, antwoordt hij: "Geen commentaar".

Zijn dissertatieonderzoek deed Chaum aan de universiteit van Berkeley. Was er een eurekamoment?

"Nee, het was geen eurekamoment, maar het was wel verreweg de grootste thrill die ik ooit heb meegemaakt op wetenschappelijk gebied. Het was een serie resultaten waarmee we konden laten zien wat met multiparty computations aan 'algemene dingen' gebouwd kon worden. Het was het forefront in science!" "Eerlijk gezegd is goed kijken en onderzoeken een veel fundamenteler deel van het onderzoek geweest. Een kind van 5 begrijpt dat als je een opa hebt die je vertrouwt, jij hem al je geheimen kunt vertellen. Het belangrijkste daarbij is dat die opa een gedragscode heeft: hij vertelt je geheim niet door. Als je zo werkt, kun je elk probleem rondom informatiebeveiliging oplossen. Kinderen snappen dat; die zijn dol op geheimen. Het gaat er hier om dat je die vertrouwde persoon kunt vervangen door een mechanisme. Mijn carrière is gevuld met het doen van voorstellen voor zulke oplossingen. En een daarvan is de bitcoin."

Hoe kwam u van Berkeley bij het CWI in Amsterdam terecht?

"Dat kwam onder meer doordat daar veel onderzoek werd gedaan naar multiparty computations. Daarmee kon ik mijn theorieën verder uitbouwen, samen met de wetenschappers van het CWI. Maar we werden constant op de hielen gezeten door een team van het MIT. Zij deden onderzoek in dezelfde richting. Ze presenteerden tijdens dezelfde conferenties als wij en altijd met ongeveer dezelfde resultaten. Maar altijd net iets minder dan wij. We deden het steeds wat beter; wij kregen ook de prijzen en uitnodigingen om te publiceren."

Wat is van essentieel belang geweest qua faciliteiten binnen het CWI?

"Dat was de volledige academische vrijheid die wij hadden en de mogelijkheid om samen te werken met collega's van wereldklasse. Dat is echt niet vanzelfsprekend; we hoefden niet per se te publiceren of les te geven. Het CWI was toen honderd procent gefinancierd door NWO en we konden vrij onze gang gaan. Dat was geweldig. Als ik moest kiezen tussen werken in een academische wereld en in mijn eigen bedrijf, dan zou ik voor die academische wereld kiezen – als dat diezelfde academische wereld was van de jaren tachtig, want die ongebreidelde vrijheid is er niet meer. De invloed van de zakelijke wereld is erin geslopen en zorgde voor erosie van je academische vrijheid. Daardoor bewogen we steeds verder af van het pure onderzoek. Dat is niet per se slecht in het algemeen. Maar wel voor mij, want ik ben op mijn best als ik mijn eigen problemen kan kiezen en oplossen, en zelf mijn mensen kan kiezen."