Nexus: Een Peer-to-Peer Netwerk

4 juli 2017

Samenvatting

"Je verandert nooit dingen door de bestaande realiteit te bestrijden. Om iets te veranderen bouw je een nieuw model dat het bestaande model overbodig maakt"

R. Buckminster Fuller

Door de geschiedenis heen zijn we getuige geweest van veel veranderingen in onze cultuur, technologie en bestuur. Deze veranderingen worden gevoed door de noodzaak voor de verdere evolutie van de mensheid. Nu benadert de mensheid een nieuw cruciaal punt waarin we de manier van werken volledig moeten veranderen; daarom hebben we Nexus gebouwd. Peer-to-Peer-technologie is de ruggengraat van een wereldwijde op blockchain gebaseerde cryptocurrency vertegenwoordigd door de ticker: *NXS* die wereldwijd wordt verhandeld als alternatieve valuta met het vermogen om te concurreren met wereldeconomieën. Het Nexus framework maakt gebruik van een nieuw gedistribueerd database ontwerp, wiskundige algoritmes, gemeenschapsbestuur, op de grond gebaseerde mesh-netwerken en een *Low Earth Orbit* satelliet netwerk. Wij zijn Nexus, een connectie van mensen, ideeën en computers met als doel meer vrijheid te bieden. Welkom in de toekomst.

Inhoudsopgave

Geschreven door:

Colin Cantrell
Bryan Gmyrek, Ph.D.
Kierre Reeg

Met bijdragen van:

Keith Smith
Preston Smith
Jacynda Smith

Aangepast door:

Mara Michael

Vertaald door:

Glenn Bogaerts

"fides in stellis, virtus in numeris"

nexus: een verbinding of reeks van verbindingen die twee of meer dingen met elkaar verbinden.

Oxford Engels woordenboek

1 Inleiding

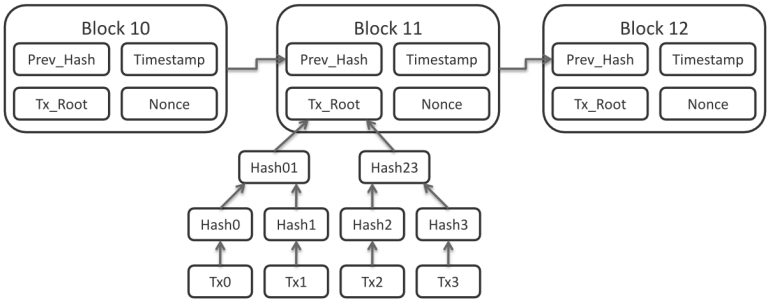
Peer-to-peer netwerken vormen de basis van digitale industrieën in de wereld. Dit ecosysteem blijft evolueren door innovators in de sector van open-source protocollen, zoals *Bitcoin, BitTorrent, TOR, and IPFS*. Het nut van deze netwerken heeft een steeds groter effect op mensen over de gehele wereld. Voor de eerste keer in de geschiedenis kan de overdracht van waarde plaats vinden zonder de noodzaak van tussenpersonen. Nu, bijna tien jaar na de release van Satoshi Nakamoto's *Bitcoin: een peer-to-peer elektronische valuta systeem* [1] dat debuteerde op een Cypher Punk e-maillijst in een tijd van economische crisis, er veel voordelen zijn gerealiseerd, waaronder maar niet beperkt tot: ***viz.*** verbeterde financiële zekerheid, emancipatie van gecentraliseerde banksystemen, en de mogelijkheden voor nieuwe toepassingen op blockchains. Er zijn echter vele uitdagingen geïdentificeerd zoals schaalbaarheid, consensus updates en overwegingen voor het post-quantum tijdperk dat zeer dichtbij is. Door oplossingen te bieden aan een aantal van deze geïdentificeerde problemen heeft Nexus het blockchain protocol verbeterd, waardoor een solide basis wordt gelegd voor de digitale economie van de toekomst.

1.1 Wat is Nexus?

Nexus is een verbinding, of reeks van verbindingen van computers, bedrijven en mensen die de focus leggen op het opzetten van nieuwe financiële toepassingen, technologieën, dienstverlening en soevereiniteit.

1.2 Wat is een blockchain?

Een blockchain is een gedecentraliseerde en onveranderlijke openbare database van transacties. De database is georganiseerd door een reeks van blokken met elkaar te verbinden. Elk blok bevat een aantal transacties. De blokken worden gerangschikt op tijd en aan elkaar gekoppeld met behulp van cryptografische hashes.[1][2] Het berekenen van deze hashes vergt enorme computerkracht.[3] Elke blok bevat de hash van het vorige blok: *op deze manier worden de blokken met elkaar gelinkt.*



De blokken worden in intervallen geproduceerd en vormen een ketting van verifieerbare blokken die de transactiegeschiedenis bevatten. Deze gegevens kunnen niet gewijzigd worden zonder het werk van de *voorgaande blokken* en *bevestigingen* opnieuw uit te voeren. Het eindresultaat is één enkele, onveranderlijke ketting van transacties gegroepeerd door middel van in tijd geordende blokken die zijn gedistribueerd en geverifieerd door alle nodes in het netwerk.

1.3 Hoe worden blokken gemaakt?

Blokken worden gemaakt in een gedistribueerd netwerk van mijnwerkers *(mensen die hun computers of speciale hardware in zetten om hashes te berekenen)* in een proces dat minen of in het nederlands mijnen wordt genoemd. Om het in mensentaal te zeggen, stel je voor dat veel mensen in

[1] "Een cryptografische hash-functie is een functie die een invoer (of 'bericht') neemt en een alfanumerieke tekenreeks van vast formaat oplevert. De string wordt de 'hash-waarde' genoemd"[11]

[2] Het concept van een cryptografische reeks blokken stamt uit de Ehrsam, Meyer, Smith en Tuchman's uitvinding van Cipher Block Chaining (CBC) in 1976 [3]. NB: dit is verschillend van *blockchain* die hier op verschillende manieren wordt besproken, vooral omdat het geen proof-of-work bevat.

[3] Dit wordt in het algemeen Proof-of-Work genoemd, maar omvat ook de innovatie van Sunny King: Proof-of-Stake [12].

een kamer zitten en gemotiveerd zijn om een prijs te winnen als ze de eerst zijn om de Rubik's puzzel op te lossen. De tegels van de Rubik's puzzel kunnen worden aanzien als transacties, waarbij een van de tegels de prijs *(mint)* vertegenwoordigt die de winnaar mag claimen als hij de puzzel als eerst heeft opgelost. Ze mogen slechts één willekeurige aanpassing doen per iteratie en worden beperkt door de snelheid van hun handen *(sommige zijn sneller dan andere)*. Uiteindelijk zal één speler eindigen met een opgeloste puzzel. Wanneer men de oplossing vindt, wordt deze aan de andere spelers in de ruimte getoond. Als de andere spelers onafhankelijk verifiëren dat de puzzel correct is opgelost, wordt de winnaar beloond met de prijs en begint een nieuwe ronde.

1.4 Zijn blockchains de oplossing?

Blockchains zijn noodzakelijker nu we ons bewust worden van de uitdagingen waar we voor staan in onze huidige samenleving. Door open te staan voor de uitdagingen worden we ons bewust van de beperkingen die legale monetaire systemen niet kunnen oplossen. We zien dat *blockchains* veel monetaire uitdagingen oplossen, zoals ongecontroleerde inflatie, centrale banken en vele anderen. Toch zijn ze slechts een deel van de oplossing voor onze huidige economische omstandigheden.

Kwantitatieve versoepeling of vrijer vertaald kwantitatieve geldverruiming is een vorm van directe geldschepping door een centrale bank, waarbij deze effecten (zoals staatsobligaties) aankoopt met voor dat doel gecreëerd geld.

Investopedia

De term *blockchain* moet niet verward worden met een versleutelde database (encryptie). De Dollar of Euro is in wezen een online virtuele valuta die gecodeerd is tussen banken die kan ingewisseld worden voor *papieren geld*. Dit maakt de Dollar of Euro echter niet tot een blockchain. Wat een blockchain tot een echte blockchain maakt, is een gedecentraliseerd publiek beschikbaar dagboek (ledger) zonder centrale autoriteit. Door een bepaald deel van een cryptocurrency te bezitten, bewijst u gedeeltelijk eigenaarschap in het financiële systeem.

1.5 De uitdagingen van geld

De toepassing en implementatie van alle monetaire systemen in de wereld is een van de grootste uitdagingen waar we vandaag de dag voor staan. Dit is te wijten aan de vele wereldwijde beleidslijnen die ontworpen zijn om centrale banken in staat te stellen valuta's te creëren als schulden met bijbehorende rente. Centrale banken hebben de mogelijkheid om de wereldeconomieën te beïnvloeden door de rentetarieven te veranderen, massa's geld te drukken *(ook bekend als inflatie of hyperinflatie)*, kwantitatieve versoepeling of door verschillende andere vormen van kredietcreatie. Er zijn veel historische voorbeelden van centrale autoriteiten die deze enorme macht misbruikt hebben en dit allemaal ten koste van mensen die van deze instellingen afhankelijk waren. Voorbeelden hiervan zijn de hyperinflatie die opliep tot 30,000% per maand in Duitsland na de eerste wereldoorlog, de Grote Recessie in Zimbabwe van het afgelopen decennium met bijna 79 miljard procent inflatie per maand en Hongarije na de tweede wereldoorlog, met inflatiecijfers van bijna *13,000,000,000,000%* per jaar. [4]

2 Nexus

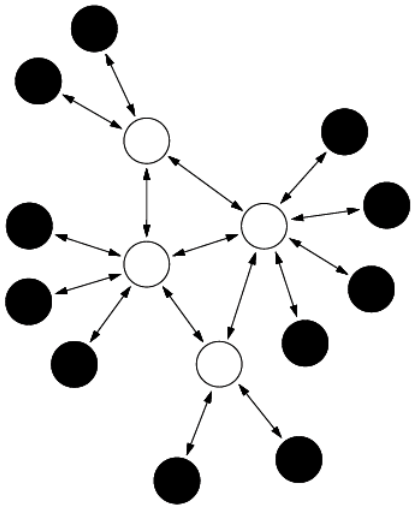
Bij het bieden van de fundamentele basis voor verandering en vrijheid moeten meerdere componenten overwogen worden. Het volgende is een korte schets van de hoofdcomponenten die de basis vormen van Nexus.

2.1 Hardware

Nexus onderzoekt en ontwikkelt drie soorten netwerken die samenwerken om een nieuw telecommunicatiesysteem te vormen. Deze worden beschreven in de onderstaande paragrafen.

[4] De geschatte 200% per dag inflatie komt overeen met ongeveer dertien miljard percenten jaar [2]

2.1.1 Mesh Netwerken



Een mesh netwerk is een netwerktopologie waarbij elk knooppunt gegevens doorgeeft. Alle netwerk knooppunten werken samen bij de distributie van gegevens in het netwerk [4].

Dit maakt de groei mogelijk voor netwerken op de aarde om gegevensuitwisseling in gelokaliseerde gebieden af te handelen.

Deze mesh netwerken op de aarde zelf zullen veel telecommunicatie problemen oplossen. Gespecialiseerde antennes kunnen door mensen aangekocht en bedient worden, waardoor er netwerken worden gevormd die eigendom zijn van de personen die het gebouwd hebben.

2.1.2 Cube Satellites

Cube satellites of in het nederlands mini satellieten in de vorm van een kubus maken deel uit van het mesh netwerk dat naarmate de groei de problemen met 'line of sight' en transcontinentale communicatie moeten overwinnen. Dit probleem kan worden opgelost met een geheel van satellieten die ontworpen zijn om de caching [5] laag te voorzien in de ruimte voor het mesh netwerk dat op zijn beurt gegevens uitwisselt met het mesh netwerk dat zich op de aarde bevindt.

2.1.3 Grondstations

Grondstations zorgen voor de satelliet *up en downlinks*. Deze zijn verantwoordelijk voor caching van gegevens op de aarde, het draaien van een nexus daemon en het definiëren van een route om gegevens door te sturen naar een geadresseerd eindpunt.

[5] Een cache (spreek uit: kesj of kasj, van het Engelse woord 'cache', voorraad of opslagplaats) is een opslagplaats waarin gegevens tijdelijk worden opgeslagen om sneller toegang tot deze data mogelijk te maken.[5]

2.2 Software

Er zijn veel soorten softwaretoepassingen die een integraal onderdeel zijn van de functionaliteit en efficiëntie van Nexus. De softwaresystemen worden voortdurend ontwikkeld en verbeterd naarmate Nexus groeit.

- **Daemon (achtergrond proces)**

  Nexus werkt op een low-level software applicatie die we de *"Nexus Daemon"* noemen. Verschillende instanties van deze softwaretoepassing communiceren met elkaar en vormen een peer-to-peer-netwerk. Ze wisselen gegevens uit in de vorm van transacties en beveiligen ze in een gedistribueerde database die een blockchain wordt genoemd.

- **Wallet (portemonnee)**

  Een command line en een grafische Qt versie van de Nexus wallet zijn momenteel beschikbaar [6] [10]. De nieuwe versie van de Nexus wallet zal een grafische toepassing van hoger niveau zijn die toegang biedt tot de functies van de *"Nexus Daemon"* via een HTML / JS-interface. De interface fungeert ook als modulair framework waarin modules kunnen worden ontwikkeld voor een betere gebruikerservaring.[6]

- **Library (bibliotheek)**

  De lower-level library bestaat uit drie delen, namelijk Crypto, Databank en Protocol. Ze vormen een basislaag van programmeer sjablonen die kunnen gebruikt worden om er complexere klassenstructuren bovenop te maken.

3 Specificaties

Dit gedeelte bevat details over de belangrijkste softwarecomponent van Nexus, de *"Nexus Daemon"*. Deze software component is de basis voor het Nexus netwerk en houdt rekening met juiste uitgaves, mining, trust en andere componenten van beveiliging en efficiëntie.

3.1 Hashing

Hashing is een cruciaal onderdeel van elke cryptocurrency. De recente SHA-1 botsing computatie die door Google werd ontdekt benadrukt de nood aan

[6] Dit is wordt actief ontwikkelt op het moment van dit schrijven.

veiligere hashes [21]. Een van de innovaties van Nexus is het gebruik van nieuwe hashing-functies met als doel een verbeterde beveiliging.

3.1.1 SHA-2

SHA-256 is lid van de SHA-2, een set van cryptografische hashfuncties.[7] Het is ontworpen door de National Security Agency (NSA) en in 2001 gepubliceerd [17]. SHA-256 wordt gebruikt in Bitcoin-mining en bij het maken van Bitcoin adressen [54].

3.1.2 SHA-3

Nexus gebruikt een nieuwer, veiliger hashing algoritme dan dat van Bitcoin. De SHA-3 [55] standaard was het resultaat van een wedstrijd [22] met als doel een alternatief voor SHA-2 op te leveren. Deze wedstrijd werd georganiseerd door het National Institute of Standards and Technology (NIST). De winnaar van deze wedstrijd werd in 2012 geselecteerd. Het nieuwe algoritme SHA-3 is een subset van de cryptografische familie Keccak [56].

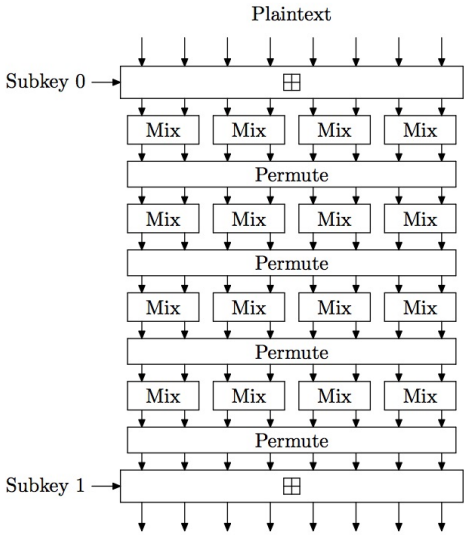
3.1.3 Skein

Het Skein-algoritme was de nummer twee in de NIST hashfunctie competitie [57]. Deze wordt ook gebruikt in Nexus in combinatie met SHA-3. Het voordeel van deze aanpak is een grotere diversiteit in veilige hashing functies die in Nexus worden gebruikt.

[7] SHA staat voor Secure Hashing Algorithm.

3.1.4 Skein-Keccak

Nexus hashing is opgebouwd uit twee veilige hashing algoritmen: Skein en Keccak [19]. Deze twee algoritmen worden gecombineerd om één enkele SK-1024 (Skein-Keccak 1024 bit) hash te vormen. Er zijn drie soorten uitvoer lengtes in Nexus hashing: SK-256, SK-512 en SK-1024. Publieke sleutels zijn gehashed met SK-256 om ze te beschermen tot ze worden gebruikt. Transacties worden gehashed met SK-512 terwijl SK-1024 wordt gebruikt voor de proof-of-work hash.



Figuur 1: Vier van de 72 ronden van het Threefish-512 blokcijfer dat in Skein gebruikt word [18].

3.1.5 Vergelijking van 256 bit en 1024 bit

Het volgende voorbeeld illustreert het verschil in grootte tussen een Nexus blok hash en een Bitcoin blok hash:

- Bitcoin Hash (256 bit)

  000000000000000000478710bb73175549d34893a375
  454df1af122c26a453d9b

- Nexus Hash (1024 bit)

  0000000001370e3764cffad92091c99b5beaf85f6fc
  edae66e77be9de6f0ce6e3d8b1da4b6581d35f3ff6c
  f359b10ab85c3b226f41cf864c979e8492f854c56d3
  0e329ffc012c338caa7f3c6197137afb1637adc0b2f
  22270990d0034c0ea0eae306ec28b7a565a1459896d
  69a1c20f9f63af6c5fd672d76c6c8934e8363a21

3.2 Uitgave

Emission of in het nederlands 'uitgifte'. In Bitcoin is een vaste hoeveelheid BTC beschikbaar als beloning voor mijnwerkers (miners) in elk blok. Dit bedrag halveert om de vier jaar, waardoor de inflatie van Bitcoin afneemt. Deze plotselinge verandering in de beloning per blok is echter een schok voor de markt. Mijnwerkers (miners) spenderen grote sommen geld aan apparatuur en personeel. Als de beloning per blok halveert, wordt hun winst gehalveerd. [8] Een dergelijke onzekerheid kan mogelijk een negatief effect hebben op de netwerkbeveiliging [26]. Nexus verbetert dit model door de beloning bij elk blok aan te passen. Gebruikmakend van de vergelijkingen voor exponentieel verval *(met een zorgvuldig gekozen constante k)*, (e^{-kt}), wordt elke minuut een aanbetaling in reserves gedaan. Het reserve bepaalt de beschikbare beloning voor mijnwerkers (miners).

De beschikbare hoeveelheid is op tijd vergrendeld en niet op de productie van blokken. Inconsistente blocks hebben geen effect op de beschikbare hoeveelheid. Dit maakt het mogelijk de beschikbare hoeveelheid nauwkeurig te berekenen op elk moment na een netwerk tijdslot.

3.2.1 Reserves

Een traditioneel waterreservoir bevat water dat door een stad kan worden gebruikt. De totale hoeveelheid water die de stad kan gebruiken, is beperkt op basis van de hoeveelheid water in het reservoir. Op vergelijkbare wijze bepaalt het reservesysteem van Nexus hoeveel NXS beschikbaar is voor mijnwerkers (miners) op een bepaald moment.

Er zijn drie reserves. De hoeveelheid NXS die in elke reserve wordt gestort, wordt wiskundig bepaald door *vervalvergelijkingen*.

$$\begin{aligned} V_d &= \quad 1 \cdot e^{-0.00000059 \cdot T_m} \quad +0.032 \\ V_a &= 10 \cdot e^{-0.00000055 \cdot T_m} \quad +1 \\ V_m &= 50 \cdot e^{-0.0000011 \cdot T_m} \quad +1 \end{aligned} \tag{1}$$

Waar T_m de tijd is in minuten en V_d, V_a, V_m zijn de reserve stortingen voor mijnwerkers (miners), ambassadeurs en ontwikkelaars.

[8] Deze winstdaling kan in theorie voorzien worden zodat mijnwerkers (miners) zich kunnen voorbereiden. Het is realistisch gezien moeilijk voor mijnwerkers (miners) om dit te verantwoorden in een snel veranderend systeem.

3.2.2 Beloningen

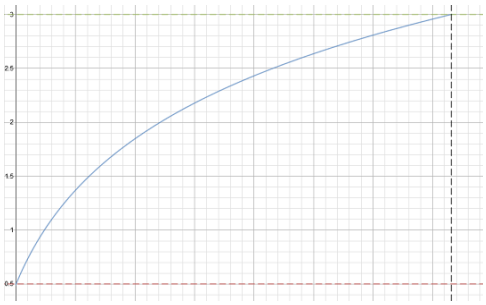
De beloningen worden berekend op basis van de reservewaarde. Dit voorkomt uitgave voorbij het streefniveau. Deze drie vergelijkingen beschrijven de intervallen waarin de blokbeloning V_b verandert op basis van reservewaarden V_m bij T_m door de T_m waarde uit vergelijkingen te comprimeren 1.

$$V_b = \begin{cases} \frac{T_a}{60} \cdot V_r, & T_m \leq 2.5 \\ 2.5 \cdot V_r, & 2.5 < T_m < 20 \\ 3.0 \cdot V_r, & T_m \geq 20 \end{cases} \tag{2}$$

Waar T_a de werkelijke tijd is, T_o de offset tijd is en T_t de doeltijd is.

3.2.3 Intrest of ook Rente (Minting)

Peer-to-peer-netwerken, zoals Bitcoin en Nexus, vereisen de ondersteuning van vele knooppunten over de hele wereld. Als er niet genoeg knooppunten zijn, lijden netwerk stabiliteit, decentralisatie, snelheid en beveiliging. Bitcoin zit met het probleem[9] waarbij iedereen wil dat meer mensen een peer-to-peer-wallet draaien, maar er is weinig stimulans om het effectief te doen. Nexus lost dit probleem op door mensen te belonen met nieuwe munten om hun portemonnee 24/7 beschikbaar te houden en als knooppunt in het netwerk te fungeren. Om het simpel te zeggen: als iemand de Nexus portemonnee op zijn computer installeert en er voldoende NXS insteekt, dan zullen ze af en toe een blok vinden en extra NXS verdienen.[10]



Figuur 2: Rentevoet Grafiek.

[9]Dit is een economisch probleem waarbij elk individu het meeste profijt probeert te trekken uit een bepaald middel[37].

[10] Dit is een manier om het netwerk te ondersteunen en Nexus te verdienen zonder kostbare en moeilijk te bedienen hardware en software voor het genereren van munten (minen).

Dit systeem beloont deelnemers naarmate hun bijdrage aan het netwerk. Als iemand blokken produceert door deze methode te gebruiken, groeit zijn of haar vertrouwens score. Bij een hogere vertrouwens score komt een hogere intrest (minting rate). De intrest (minting rate) R_m varieert van 0.5 % tot 3 %.

$$R_m = \frac{0.025 \cdot ln(\frac{9 \cdot a_t}{31449600} + 1)}{ln(10)} + 0.005 \tag{3}$$

Waar a_t de leeftijd is van uw vertrouwens score (het aantal seconden sinds de Genesis transactie waarbij de Trustkey werd genereerd).

3.3 Blok validatie

Er zijn drie manieren om een geldig Nexus blok te maken en nieuwe NXS te genereren. Er zijn twee proof-of-work kanalen en een kanaal met proof-of-holdings (bewijs van bewaring). De proof-of-work kanalen zijn het Prime Channel (Priemgetallen) en het Hashing Channel. In het Prime Channel zoeken mijnwerkers (miners) naar priemgetallen van 308 cijfers groot. In het hash channel, wordt de standaard Hashcash [20] werkwijze gebruikt door middel van het SK-1024 hashing algoritme. De twee proof-of-work-kanalen voorkomen dat er te veel blokken achter elkaar worden geproduceerd, waardoor een 51% aanvaller over beide kanalen wordt gedwongen.[11]

3.3.1 Priemfactoren

Het doel van het werk in het Prime Channel is een zoektocht naar priemfactoren [44].[12] Het vinden van deze priemfactoren is een proces van vallen en opstaan. Mijnwerkers (miners) moeten vele getallen proberen om er een te vinden die het begin is van een priemfactor [43, 38].

Het aantal priemgetallen in een priemfactor wordt de kettinglengte genoemd. [13] Een priemfactor met een langere ketting is moeilijker te vinden dan een met een kortere ketting. Het eerste priemgetal in de keten moet hoger zijn

[11] Reserves tussen Prime en Hash worden gelijk verdeeld, elk 50 %

[12] De cijfers die in deze zoekopdrachten worden gevonden, zijn eigenlijk waarschijnlijke priemgetallen [40]. Ze doorlopen de Fermat Prime test [41] op basis 2, 3 en 5.

[13] De "ketting"hier moet niet worden verward met de ketting in de blockchain.

dan de block hash en kleiner dan de block hash plus 2^{64}.[14] Als de eerste priemgetallen in het cluster aan deze criteria voldoen, wordt dit als een geldige oplossing beschouwd.

Een voordeel van het zoeken naar priemfactoren is dat er wordt aangenomen dat het resistent is tegen GPU-, FPGA- en ASIC-mining in tegenstelling tot hashing. Een andere voordeel is dat de door de mijnwerker (miners) geproduceerde gegevens nuttig zijn voor wiskundig onderzoek naar priemgetallen [42] [39]. De toepassingen van priemgetallen onderzoek kunnen verder reiken dan de wiskunde en de kwantumfysica [45]. Dit is een van de manieren waarop Nexus waarde toevoegt aan de wetenschap en de wereld.

3.3.2 Hashing

Het hashing channel maakt gebruik van *Hashcash* [20] proof-of-work. Mijnwerkers (miners) voeren code uit [7, 8] op GPU's in een poging een hash te vinden die aan een bepaalde moeilijkheidsgraad voldoet. Als ze geluk hebben, vinden ze een hash met minstens een bepaald aantal 0 bits in het begin. Dit betekent dat de hash wordt voorafgegaan door een aantal 0'en en een kleiner geheel getal is. Dit wordt een "gedeeltelijke botsing"genoemd. Dit is vergelijkbaar met de proof-of-work die Bitcoin gebruikt. Bitcoin gebruikt SHA-256 terwijl Nexus de nieuwere SHA-3 gebruikt in combinatie met Skein.

3.3.3 Stockeren

Proof-of-Holdings *(POH)* biedt een derde beveiligings kanaal. Een aanvaller zou 51 procent van de NXS voorziening nodig hebben om dit kanaal aan te vallen in combinatie met de hash- en prime-kanalen. Door deel te nemen aan dit systeem wordt je beloond voor het actief "bijhouden"van je munten, de beloning is uiteraard nieuwe munten. Dit betekent dat het netwerk gebruikers stimuleert om bij te dragen aan de beveiliging van het systeem. Dit zorgt voor een natuurlijke groei van het aanbod van munten in de loop van de tijd, wat zeer bevorderlijk zal zijn voor het netwerk, de economie en gebruikers.

[14] De block hash kan niet a priori worden bepaald voor toekomstige blokken omdat deze gebaseerd is op eerdere blok informatie. Daarom moet een mijnwerker (miner) het zoeken naar hun priemfactor opnieuw starten nadat elk nieuw blok is gevonden

In tegenstelling tot de huidige modellen van de Centrale Bank, gaat dit nieuwe aanbod munten rechtstreeks in handen van de gebruikers in plaats van te worden gefilterd door een fractioneel reserve systeem. Bovendien hebben deze nieuw geslagen munten geen schuld in verband met hun uitgifte en hoeven ze daarom nooit terug te worden betaald aan het systeem met bijbehorende rente, zoals het geval is met veel huidige valuta's. De wisselkoers is vastgesteld als een variabele rente tussen 0.5% en 3% om een kleine natuurlijke groei aan de munt voorraad toe te staan met als doel de economische mogelijkheden te vergroten.

3.4 Moeilijkheidsgraad (Difficulty)

De moeilijkheid om een blok te vinden, wordt bij elk nieuw blok aangepast. Het moeilijkheids algoritme dat Nexus gebruikt combineert gewogen gemiddelden voor de laatste n blokken. Een gewogen gemiddelde tijd, T_a wordt als volgt berekend:

$$T_a = \frac{\sum_{i=1}^{n} w{\cdot}i[T_b(H-n+i)-T_b(H-n+i-1)}{n} \tag{4}$$

Waar H huidige blok moeilijkheid is, T_b is de blok tijdsindicatie op een gegeven moeilijkheid, n is de blockchain diepte en w is een gewichts constante (momenteel ingesteld op 3).

Mod_d is de factor die wordt gebruikt om de moeilijkheidsgraad te wijzigen

$$Mod_d = \begin{cases} [1 - (Min_d \cdot T_o)] \cdot T_t, & \text{if } T_a \geq T_t \\ [1 + (Max_d \cdot T_o)] \cdot T_t, & \text{otherwise} \end{cases} \tag{5}$$

Waar T_t de streeftijd, T_o is de offset tijd, Min_d is de minimale moeilijkheidsgraad vermindering en Max_d is de maximale moeilijkheidsgraad verhoging.

> Het is een ondeugd om iedereen te vertrouwen, evenveel als een ondeugd om niemand te vertrouwen.
>
> *Seneca*

3.5 Vertrouwen (Trust)

Vertrouwen of Trust is een kern component van Nexus. Knooppunten (of zoals hierboven aangehaald deelnemers) die een gevestigd belang hebben in en ten goede komen aan het gehele netwerk door consistent deel te nemen, worden als betrouwbaarder beschouwd. Op dit moment wordt vertrouwen verdiend door Nexus in een portefeuille te houden en regelmatig geldige blokken te genereren. Dit verdiend vertrouwen wordt vastgelegd in de Nexus blockchain en is gekoppeld aan een vertrouwens code.

Toekomstig onderzoek en de ontwikkeling van Nexus zal zich concentreren op het op vele manieren gebruiken van het concept van vertrouwen. Met behulp van vertrouwen kan een nieuw beveiligingsmodel ontwikkeld worden. De kracht van de Nexus economie en de betrouwbaarheid ervan zal versterkt worden door de het vertrouwen tussen de vrijwillige interacties met individuen en groepen van individuen.

3.5.1 Gewicht (Weight)

Gewicht bepaalt de snelheid waarmee kan worden gezocht naar nieuwe vertrouwens blokken. Het komt in de vorm van twee verschillende gewichts variabelen: Blok gewicht (W_b) en Vertrouwen gewicht (W_t).

$$W_t = Min(17.5, \frac{16.5 \cdot ln(\frac{2 \cdot a_t}{2419200}) + 1}{ln(3)} + 1.0) \tag{6}$$

$$W_b = Min(20.0, \frac{19.0 \cdot ln(\frac{2 \cdot a_b}{86400}) + 1}{ln(3)} + 0.05) \tag{7}$$

Waar a_t de vertrouwens leeftijd is en a_b de leeftijd van de block.

3.5.2 Drempel (Threshold)

Er is een systeem ontwikkeld om een op tijd gebaseerd energie efficiënt vertrouwen systeem mogelijk te maken. Dit wordt geregeld door de Energie Efficiënte Drempel (Energy Efficiency Threshold) E_t.

$$E_t = \frac{100 \cdot T_a}{N_{once}} \tag{8}$$

De vereiste drempelwaarde R_t is

$$R_t = \frac{(50 - W_t - W_b) \cdot 1000}{C} \tag{9}$$

Waarbij C de totale NXS is in een vertrouwens transactie.

3.5.3 Vertrouwenssleutel (Genesis)

De genesis transactie is de eerste transactie van een vertrouwens sleutel. Deze bepaald de beginleeftijd van de vertrouwens sleutel en dient vervolgens om een referentie te krijgen over zijn huidige gewicht en de bijbehorende intrest. De hash van deze genesis transactie kan daarom worden gebruikt als invoer in toekomstige transacties om te verifiëren dat een vertrouwens blok gekoppeld is aan een bijbehorende genesis transactie.
De volgende vergelijking beschrijft het genesis gewicht dat vereist is om een drempelwaarde te bereiken die hoog genoeg is voor een genesis transactie te creëren met bijbehorend blok.[15]

$$W_g = Min(17.5, \frac{16.5 \cdot ln(\frac{2 \cdot a_c}{7257600}) + 1}{ln(3)} + 1.0) \tag{10}$$

Waarbij a_c de munt leeftijd is van de gebruikte munten.

3.5.4 Interval (Intervals)

Vertrouwens blokken kunnen niet met dezelfde vertrouwens sleutel worden gemaakt, tenzij het interval of het aantal blokken tussen hun laatste vertrouwens blok groter is dan $I_t \geq 6$.

3.6 Tijdsverschil (Clock Drift)

Clock drift verwijst naar verschillende gerelateerde verschijnselen waarbij een klok niet exact hetzelfde loopt als een referentie klok [9]. Dit wordt meestal opgelost door verbinding te maken met een centrale server en / of een atoomklok. Nexus lost dit op met een peer-to-peer tijdregistratiesysteem dat alle klokken op het netwerk gesynchroniseerd houdt met een universeel tijd protocol.

[15] Genesis transactie gewicht omvat niet het blok gewicht.

3.7 Beveiliging (Security)

Bitcoin en andere cryptocurrencies staan tot maximaal 2 uur klok afwijking in de toekomst toe, wat betekent dat blokken tot 2 uur voorbij de huidige netwerk tijd (in het Engels *timestamp*) kunnen gemaakt worden, waardoor potentiële aanvalsvectoren ontstaan. Nexus bestrijdt deze synchronisatie problemen niet met de mediaan doorheen de tijd, zoals Bitcoin dat doet, maar eerder met een Unified Time systeem dat op protocol niveau werkt, zodat alle Nexus klokken tot op de seconde gesynchroniseerd zijn.

3.8 Tijdslot (Time-Locks)

Omdat de klokken in het Nexus netwerk worden gesynchroniseerd kunnen nieuwe regels in het protocol worden geactiveerd op basis van tijd stempels (in het Engels *timestamp*) in plaats van bloknummers. Dit stelt netwerk-deelnemers in staat om consensus updates nauwkeuriger te activeren.

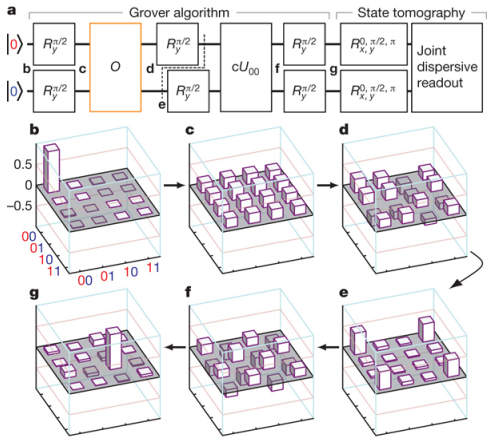
3.9 Controlepunten (Checkpoints)

Geautomatiseerde en gedecentraliseerde controlepunten worden elk uur gemaakt. Een controlepunt verhindert dat een blok die niet ontstaan is uit het laatste controlepunt ongeldig is. Dit voorkomt dat een aanvaller een alternatieve blockchain produceert die het vorige controlepunt vooraf gaat.

> Ik denk dat ik gerust kan zeggen dat niemand quantummechanica begrijpt.
>
> *Professor Richard Feynman, 1965*
> *Natuurkunde Nobelprijswinnaar*
> *[23]*

4 Post-quantum-overwegingen

4.1 Algoritme van Grover



Figuur 3: Het algoritme van Grover over twee Qubits

Het algoritme van Grover is een quantum algoritme dat werd bedacht door Lov Grover in Bell Labo. De samenvatting in Grover's theorie uit 1996 biedt een nuttige beschrijving: "Stel je een telefoongids voor met N namen gerangschikt in willekeurige volgorde. Om iemands telefoonnummer te vinden met een waarschijnlijkheid van de helft, zal elk klassiek algoritme ... een minimum van $N/2$ namen moeten bekijken. Qubits kunnen in een superpositie van toestanden zijn, wat betekent dat een qubit een 0 of een 1 kan zijn. Als gevolg hiervan kan het gewenste telefoonnummer alleen worden verkregen in $O(\sqrt{N})$ stappen [63]."

Het resultaat van een black box-functie kan worden gebruikt om[16] de invoer te bepalen. Dit betekent dat de meeste eenrichtings cryptografische hashfuncties gevoelig zijn voor dit algoritme. En inderdaad, het algoritme van Grover kan een 256-bits sleutel door middel van brute force via 2^{128} iteraties de input berekenen.

Het algoritme gaat door met het oproepen van $G\left[\frac{\pi}{4}\cdot 2^{\frac{k}{2}}\right]$ voor de verificatie van de subroutines. De grootste overhead in het algoritme van Grover is echter de kost van foutdetectie die klassiek moet worden uitgevoerd om de nauwkeurigheid van de qubits te garanderen (het overwinnen van kwantum ruis) en de twee subroutines van Grover iteratie te waarborgen.

De eerste subroutine van G probeert te beweren dat g : $\{0,1\}^k \rightarrow \{1,0\}$ alleen X op 1 toewijst als $f(x) = y$. De volgende subroutine wordt de *"Diffusion Operator"* genoemd en implementeert de transformatie van g om de

[16] Op een probabilistische manier.

Tabel 1: Vergelijking voor Grover zoekopdracht van SHA-256 en SHA3-256 [25, p. 18]

		SHA-256	**SHA3-256**
Grover	T-count	$1.27 \cdot 10^{44}$	$2.71 \cdot 10^{44}$
	T-depth	$3.76 \cdot 10^{43}$	$2.31 \cdot 10^{41}$
	Logical qubits	2402	3200
	Physical qubits	$1.39 \cdot 10^{7}$	$1.94 \cdot 10^{7}$
Distilleries	Qubits per Distillery	3600	3600
	Total Distilleries	1	294
	Code Distilleries	$\{33, 13, 7\}$	$\{33, 13, 7\}$
	Physical qubits	$5.54 \cdot 10^{5}$	$1.63 \cdot 10^{8}$
Total	Logical qubits	$2^{12.6}$	2^{20}
	Code Cycles	$2^{153.8}$	$2^{146.5}$
	Total Cost	$2^{166.4}$	$2^{166.5}$

kans te vergroten dat $f(x) = y$.

Zoals geïllustreerd in Tabel 1 resulteert het algoritme van Grover in een reductie van bijna 50% op de beveiliging geboden door one-way hashing functies tegen brute force aanvallen. Dit houdt in dat een hash, die twee keer zoveel bits heeft, gebruikt moet worden om hetzelfde niveau van beveiliging tegen brute force aanvallen te bereiken.

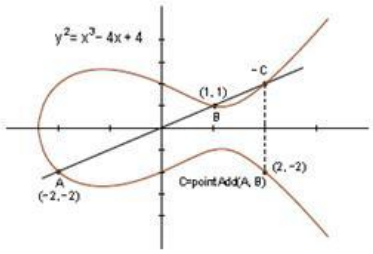
4.2 Elliptische Curve cryptografie

Elliptische curve cryptografie, in termen van klassiek computergebruik, behoudt hoge veiligheidsstandaarden met kleinere sleutelgrootten in vergelijking met RSA [59]. De volgende vergelijking kan worden gebruikt om een elliptische curve weer te geven:

$$y^2 = x^3 + ax + b \tag{11}$$

4.3 Curve groepen en velden

Figuur 4: Illustratie van een elliptische curve



In Nexus zijn de elliptische curve domein parameters gebaseerd op *sect571r1* [13]zoals gedefinieerd in de 'Standards for Efficient Cryptography 2: Recommended Elliptic Curve Domain Parameters' en deze worden gedefinieerd over een binair veld $\mathbb{F}_{2^m}$. De domein parameters die in de meeste andere digitale valuta's worden gebruikt, zijn gebaseerd op *secp256k1* [14]. Deze parameters zijn geassocieerd met een Kolbitz curve en worden gedefinieerd over een priem veld $\mathbb{F}_p$.

4.4 Private sleutels (Private Keys)

Een private key is een sleutel dat alleen aan de eigenaar van munten op een bepaald adres moet kennen. Als u een beveiligde private key wilt maken, moet u beginnen met een getal dat zo dicht mogelijk bij het echt willekeurige ligt.[17] Als iemand kan achterhalen wat de privésleutel is, kan hij of zij de munten verplaatsen naar een ander adres. Daarom is beveiliging van de private key zo belangrijk. U wilt niet dat iemand anders ontdekt wat uw 'geheime sleutel' is en u wilt niet dat zij het kunnen raden of bepalen met een complex algoritme op basis van openbare gegevens. Zowel Bitcoin als Nexus gebruiken grote getallen, zodat er bijna geen kans is dat iemand anders hetzelfde willekeurige nummer genereert en het onmogelijk is voor iedereen om alle nummers te proberen.[18] Bitcoin sleutels zijn 256 bits lang, terwijl de Nexus sleutels meer dan twee keer zo lang zijn namelijk 571 bits.

Bitcoin Private Key (256 bit)

5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF

Nexus Private Key (571 bit)

6Wuiv513R18o5cRpwNSCfT7xs9tniHHN5Lb3AMs58vkVxsQdL4atHTF
Vt5TNT9himnCMmnbjbCPxgxhSTDE5iAzCZ3LhJFm7L9rCFroYoqz

[17] Dit wordt afgehandeld door de Nexus portefeuille software - deze genereert private keys en bewaart ze.

[18] "Hoeveel nummers? Maak voor elke korrel zand op aarde een nieuwe aarde. Er zijn 26 miljard unieke Bitcoin adressen voor elke korrel zand op elk van die aardes. "[53] Omdat de sleutels in Nexus langer zijn, zijn er astronomisch meer mogelijke Nexus adressen.

4.5 Publieke sleutels (Public Keys)

Het is eenvoudig om een public key te bepalen van een private key, maar niet omgekeerd. Wanneer u een betaling van iemand vraagt, ontvangt u eerst een *Nexus address* van uw portemonnee. Dit adres is niet uw public key, dit wordt een publieke sleutel hash of *PKH* genoemd. Zoals de naam al aangeeft, is deze gemaakt door uw public key te hashen en deze te converteren naar Base58 codering. Dit betekent dat een aanvaller die eerst uw private key wil achterhalen uw public key moet bepalen via de *PKH*. Gelukkig is dit een onoverkomelijk probleem. Lopend onderzoek wijst uit dat dit zelfs quantum computers in de orde van honderd miljard jaar [49, 50] kan kosten om de publieke sleutel te achterhalen. De public key die is gekoppeld aan een *PKH* wordt niet onthuld totdat de munten zijn uitgegeven [28]. Daarom kan een hoog niveau tegen kwantum aanvallen eenvoudig worden bereikt door adressen niet opnieuw te gebruiken.

4.6 Algoritme van Shor

Het algoritme van Shor, vernoemd naar de Amerikaanse wiskundige Peter Shor die het in 1994 formuleerde, is een kwantum algoritme [46] voor het ontbinden in priemfactoren. Dit was een belangrijke prestatie omdat deze problemen geen klassieke polynomiale tijdoplossing hebben. Dit betekent dat ze, op een klassieke computer, op geen enkele hoeveelheid tijd kunnen worden opgelost. Dit kan weergegeven worden door n^k - bijvoorveeld n^2, n^3, etc.[19]

Het Elliptic Curve Discrete Logarithm Problem *(ECDLP)* is een speciaal onderdeel van *DLP* voor elliptische curves. Dit is een moeilijker probleem om klassiek op te lossen dan conventionele cryptografie die alleen op de *DLP* is gebaseerd.[47] Dit is het type probleem dat moet worden opgelost om de private key van de public key voor cryptocurrencies, zoals Bitcoin en Nexus, te bepalen.

4.7 Algoritme van Proos-Zalka

Het algoritme van Proos-Zalka was specifiek ontworpen om de *ECDLP* op te lossen over een priem veld $\mathbb{F}_p$ op een kwantumcomputer. De qubit vereiste

[19] In lekentaal betekent dit dat het vinden van een oplossing niet haalbaar is zolang er een voldoende groot getal wordt gebruikt.

voor het verbreken van de ECDLP over een priem veld van n bits is als volgt [47]

$$5 \cdot n + 8\sqrt{n} + 4\log_2 n + 10 \approx 6n \tag{12}$$

4.8 Kaye-Zalka Algorithm

De Kaye-Zalka revisie behandelt curven over het binaire veld $\mathbb{F}_{2^m}$. Dit specifieke veld maakt gebruik van binaire berekening om snellere verificatie op grotere sleutels mogelijk te maken. De vergelijking die de qubits modelleert die nodig zijn om een sleutel van $\mathbb{F}_{2^m}$ te verbreken, gaat als volgt [48].

$$2m + 7 \cdot logm + 7 + H \approx 2m \tag{13}$$

Waar H is gerelateerd aan de stop teller en volgorde van $log(m)$.

4.9 Het voordeel van langere sleutels

"De sleutellengte definieert de bovengrens van de beveiliging van een algoritme omdat de beveiliging van alle algoritmen kan worden geschonden door brute force aanvallen [59]."

Vanaf 2015 werd een minimale sleutellengte van 224 bits aanbevolen voor algoritmen voor elliptische curves [61]. Bitcoin sleutels zijn $256 - 224 = 32$ bits langer dan deze vereiste, terwijl de Nexus sleutels $571 - 224 = 347$ bits langer zijn. Volgens de National Security Agency "Elliptic Curve Public Key Cryptography met behulp van de 256-bit prime modulus elliptische curve zoals gespecificeerd in FIPS-186-2 en SHA-256 zijn geschikt voor het beschermen van geclassificeerde informatie tot het "geheime" niveau. Gebruik van de 384-bits primaire modulus elliptische curve en SHA-384 zijn nodig voor de bescherming van "topgeheime" informatie [60]."

Brute Force Resistent

De Large Bitcoin Collider [58] is een project dat Bitcoin door middel van brute force probeert aan te vallen. Deelnemers aan dit project genereren zoveel mogelijk openbare Bitcoin adressen door eerst een willekeurig getal in een bepaald bereik te kiezen. Ze vinden zelden een openbaar adres dat Bitcoin bevat, maar moest men bij toeval toch een adres vinden dan kunnen

de aanwezige Bitcoins gestolen worden.[20]

De sleutellengte definieert de bovengrens van de beveiliging van een algoritme [59] tegen aanvallen met brute force. Nexus gebruikt aanzienlijk grotere 571-bits sleutels dan de 256-bits sleutels van Bitcoin en wordt daarom verondersteld beter bestand te zijn tegen deze aanvallen.

In elk geval zegt Rico - de pseudonieme hoofdrol van de LBC: "Het vinden van een P2PKH[21]-botsing [een cryptografische methode voor het maken van Bitcoin adressen] zou waarschijnlijk het einde betekenen van P2PKH maar niet van Bitcoin,"... "Bitcoin zou evolueren met een nieuw soort adressen. Zeer zeker zou het hierdoor niet 'sterven'."[58] Dit benadrukt een van de manieren waarop Nexus waarde teruggeeft aan het Bitcoin ecosysteem. Door verschillende elliptische curve parameters en verschillende hash algoritmen te gebruiken, maakt Nexus de weg voor mogelijke toekomstige uitbreidingen van Bitcoin. In plaats van alleen alternatieven te onderzoeken of te bespreken, heeft Nexus ze op een live blockchain getest.

Langere oplossingstijd (Longer Solution Time)

Het kost meer tijd voor een quantum computer om de *ECDLP* op te lossen als de sleutel langer is. Er wordt voorspeld dat de looptijden in orde van $O(n^2)$ tot $O(n^3)$ [47, 48]. Dit betekent dat een sleutel die twee keer zo lang is ongeveer vier keer zo lang duurt om te vinden met een quantum computer.

4.10 Neven kanaal aanvallen op ecp256k1 (Side Channel Attacks)

Zoals eerder vermeld, gebruikt Bitcoin de 256 bit *secp256k1* elliptische curve domein parameters zoals gedefinieerd in de "Standards for Efficient Cryptography". Onder speciale omstandigheden kan een Bitcoin private key worden achterhaald door een ander proces op dezelfde klassieke computer met slechts 200 handtekeningen [51].[22] Met quantum computing achter de hoek, en het feit dat ECC reeds private keys lekt met neven kanaal aanvallen, moeten serieuze overwegingen worden gemaakt over de logica van elk

[20] Er zijn een aantal manieren om het risico op een dergelijke aanval op uw Bitcoins te beperken. Bewaar eerst niet te veel munten in één adres. Ten tweede, gebruik multi-factor authenticatie.

[21] Betalen aan public key hash[62]

[22] Dit is wat men een neven kanaal (side channel) aanval noemt.

Tabel 2: Qubits en tijd die nodig is om elke sleutel voor $\mathbb{F}_p$ te verbreken [27]

Quantum IFP			Quantum ECDLP			Klassiek
λ	Qubits λ	Tijd $4 \cdot \lambda^3$	λ	Qubits $7 \cdot \lambda$	Tijd $360 \cdot \lambda^3$	Tijd
512	1024	$0.54 \cdot 10^9$	110	700	$0.50 \cdot 10^9$	c
1024	2048	$4.30 \cdot 10^9$	163	1141	$1.60 \cdot 10^9$	$c \cdot 10^8$
2048	4096	$34 \cdot 10^9$	224	1568	$4.0 \cdot 10^9$	$c \cdot 10^{17}$
3072	6144	$120 \cdot 10^9$	256	1792	$6.0 \cdot 10^9$	$c \cdot 10^{22}$
15360	30720	$1.5 \cdot 10^{13}$	512	3584	$50 \cdot 10^9$	$c \cdot 10^{60}$

Waar λ de input lengte in bits is.

gebruik van algoritmen voor digitale handtekeningen om eigendom van tokens te bewijzen. Dit is de focus van voortdurend onderzoek en ontwikkeling van Nexus.

4.11 Sleutel Accommodaties in Nexus

Nexus ondersteunt momenteel sleutelgroottes tot 571 bits, met name sect571r1. Om meer keuze te bieden en te profiteren van het grotere aantal qubits dat nodig is om de curves van de priem velden te kraken, zullen we ook sleutels met verschillende curven implementeren.

De keuze van elliptische curve parameters is subtiel; we moeten zorgen dat beveiligingsrisico's worden voorkomen. We zijn van plan om ondersteuning voor meerdere curven toe te voegen, inclusief post-quantum oplossingen die op dit moment worden ontwikkeld. Om kwantum aanvallen tegen te gaan, zullen handtekening kettingen worden opgenomen als onderdeel van het Tritium protocol, waarbij gebruik wordt gemaakt van *PKH* en *OTS* of eenmalige handtekeningen, die neven kanaal aanvallen voorkomen en quantum aanvallen exclusief maken voor het algoritme van Grover. De geprojecteerde tijd voordat quantum computers gevaarlijke niveaus bereiken, is ongeveer vijf tot tien jaar. Door de sleutel formaten van de Nexus te verdubbelen, wordt de vereiste doorlooptijd vervierdubbeld, dit biedt meer tijd om zorgvuldig een post kwantum cryptografische methode te kiezen. Naar verwachting zal dit in de komende jaren plaatsvinden, aangezien de ontwikkeling van post-quantumcryptografie wordt bekeken en grondig bestudeerd.

4.12 Post-quantum cryptografie

Er zijn verschillende veelbelovende oplossingen voor het post-quantum raadsel waar we de komende jaren voor staan. Eén daarvan is veelbelovend: op rasters gebaseerde cryptografie die ervoor zorgt dat kwantum aanvallen, althans voorlopig, onhaalbaar zijn. Een andere haalbare oplossing voor dergelijke aanvallen is het gebruik van een op hash gebaseerde handtekeningen zoals *XMSS*, die wel bepaalde kenmerken van post-quantum oplossingen bezit, maar het heeft een groot nadeel dat er zeer grote hoeveelheden gegevens moeten worden overgedragen om de private key te beschermen. Dit is niet wenselijk bij het selecteren van een DSA *Digital Signature Algorithm* voor een blockchain, omdat er al zeer hoge data overhead is waarop de schaalbaarheid niet voorzien is. NIST heeft zojuist een nieuwe competitie geopend voor Post-Quantum standaardisatie, deze is vergelijkbaar met de SHA3-competitie. We verwachten dat deze de komende jaren zal afgerond worden en ons van een ruimer aanbod van post-quantumalgoritmen geeft. [15]

5 Besluit

Met moderne hashing, geüpgradede private keys, meerdere blok validatiemethoden, gedecentraliseerde controlepunten, tijdsynchronisatie, gedecentraliseerd vertrouwen, variabele blok beloning, tijdslot uitgave, gedecentraliseerde intrest, databank op laag niveau, kwantum overwegingen, op de grond gebaseerde mesh-netwerken en satelliet constellatie in lage baan om de aarde. Nexus is een van de technologisch meest geavanceerde frameworks op aarde. We hebben nu de mogelijkheid om afstand te nemen van bestaande systemen door simpelweg onze focus te veranderen. We kunnen ervoor kiezen weg te kijken van de systemen van het verleden en onze gedachten te richten op de systemen van de toekomst. Nexus bestaat als een publiek beschikbaar, gratis te gebruiken, peer-to-peer netwerk waarmee mensen verbinding kunnen maken en de kwaliteit van hun leven kunnen verbeteren. Peer-to-Peer technologieën kunnen ons helpen onze wereld opnieuw vorm te geven en Nexus betekent een belangrijke stap voorwaarts in dit proces. Het zelfstandig naamwoord “nexus” wordt gedefinieerd als: een verbinding of reeks verbindingen die twee of meer dingen met elkaar verbindt. Nexus is een idee van verbinding en de technologie om dit mogelijk te maken. Het is door deze verbinding dat we een toekomst kunnen creëren vol met leven, vrijheid en het nastreven van geluk. Welkom bij Nexus.

A Appendix: Referentie Samenvattingen om inhoud te versterken

Deze bijlage is ontworpen om gezien te worden als 'een uitbreiding op de kerninhoud' als verwijzingen naar de beschreven ideeën. Met het begrip en de studie van de volgende paragrafen, kan men een hoger niveau van perspectief krijgen van wat moet worden begrepen om ons als een soort te ontwikkelen. Zoals we kunnen zien, worden hieronder de maatschappelijke organisatiemodellen, oude filosofieën die de tand des tijds hebben doorstaan en voorlopige principes ontworpen om verwijzingen naar een groter begrip van de waarheid te zijn.

> Actie zonder visie is een dagdroom, visie zonder actie is een nachtmerrie.

B Visie

Visie is iemands vermogen om met wijsheid over de toekomst na te denken of de toekomst te plannen. Wijsheid is de eigenschap van ervaring, kennis en gezond verstand. In dit geval gaat visie gepaard met wijsheid, die een direct gevolg is van ervaring en dus van kennis. Dit betekent dat visie haalbaar is als men bereid is te leren van de ervaring van de wereld. Visie kan op een grotere diepte worden begrepen door het volgende toe te passen:

1. **Capabel** zijn om te verifiëren en / of te begrijpen zonder voorbarige conclusies te trekken
2. **Discipline** om te zien wat niet wordt gewijzigd door definities en geloof
3. **Kennis** die is opgedaan door de studie van de werkelijkheid, de maatschappij en het werk van anderen
4. **Overeenstemming** met de wetten van de natuur, deugd vinden in de wetten van jezelf
5. **Principe** gevormd door het begrip van deze overeenstemming

C Filosofie

Filosofie is de studie van de fundamentele aard van kennis, werkelijkheid en bestaan - *zoals het is* - met de bedoeling om te begrijpen *wat het is*. Hierna volgt een korte lijst van filosofieën die een fundament vormen voor visie en principe om te integreren in grotere deugd, reden en succes in de vorm van geluk zijnde de ultieme waarde waarnaar elk individu op zoek is.

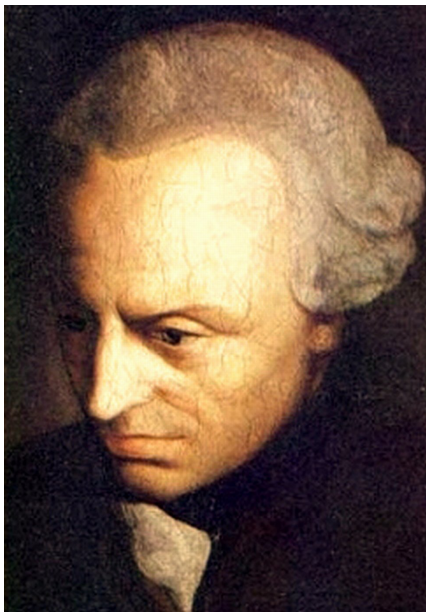
Ik moet niet bang zijn.
Angst is de moordenaar.
Angst is de kleine dood die totale vernietiging brengt.
Ik zal mijn angst onder ogen zien.
Ik zal toestaan dat het over en door mij heen passeert.
En als hij voorbij is, zal ik me omdraaien om zijn pad te zien.
Waar de angst is geweest zal er niets zijn.
Alleen zal ik blijven.
[23]

C.1 Ethica Nicomachea

Aristoteles was een oude Griekse filosoof en wetenschapper [33]. Aristoteles geloofde dat deugd essentieel was om het uiteindelijke doel te bereiken: geluk.
Als een deel van de filosofieën beschreven in zijn werken over Ethica Nicomachea, werd een idee gevormd onder de naam *"golden mean"*, die een wereld van overmaat en tekort beschreef. Deze filosofie beschreef de kwaden van de wereld - of opposities tegen de groei van het leven - als een overmaat of een tekort. De gulden middenweg wordt omschreven als de eigenschap om geen overmaat of tekort te hebben, maar eerder een 'gulden middenweg' tussen de twee uitersten.

[23] Bene Gesserit Litany Against Fear - Van Frank Herberts Dune Boeken serie

C.2 Kingdom of Ends



Immanuel Kant werd geboren voor zijn tijd op 22 april 1724 in Berlijn, Duitsland [34]. Hij had vele filosofieën die nog steeds worden bestudeerd tot op de dag van vandaag. Een van zijn meer opmerkelijke werken werd het *Kingdom of Ends*. genoemd. Hij beschrijft een hypothetisch bestaan waarin individuen volledig rationeel handelen, en met reden. Hij definieert deze mensen als degenen die in staat zijn tot correct gedrag. Hij stelde voor dat als degenen die in staat waren om te leven onder een gemeenschappelijke wet van wetten die van het grootste belang en de noodzaak waren, dat een meer harmonieuze en *morele* samenleving zich zou kunnen vormen als een *Kingdom of Ends*.

Deze gemeenschappelijke wetten kunnen worden beschouwd als referentiepunten voor de waarde van acties in een Kingdom of Ends, waar de correlatie met universele wetgeving de grootste waarde heeft voor die van Kingdom of Ends. Zijn tweede formulering toonde aan dat individuen die in overeenstemming met het principe leven om medemensen als een doel op zichzelf te behandelen, in staat waren tot grotere deugd, en daarom, vreugde. Dit beschrijft een idee en een filosofie van handelen in overeenstemming en harmonie mensen als een koninkrijk van doelen, in plaats van dat elk individu op zoek is naar elkaar als middel voor hun eigen doeleinden.

"People can only belong to the Kingdom of Ends when they become subject to these universal laws. Such rational beings must regard themselves simultaneously as sovereign when making laws, and as subject when obeying them. Morality, therefore, is acting out of reverence for all universal laws which make the Kingdom of Ends possible. In a true Kingdom of Ends, acting virtuously will be rewarded with happiness." [24]

[24] Overgenomen van `https://en.wikipedia.org/wiki/Kingdom_of_Ends`

C.3 The Tao

In het oude China was de bewaarder van de Imperiale Bibliotheek, Lao Tzu, beroemd om zijn wijsheid. Toen hij de toenemende corruptie van de regering zag, vertrok hij naar het platteland. Onderweg vroeg de bewaker bij de stadspoorten Lao Tzuto om de essentie van zijn begrip uit te schrijven om toekomstige generaties ten goede te komen. Lao Tzu schreef de Tao Te Ching, vertrok, en er werd nooit meer iets van hem gehoord [35].

[36] Hoofdstuk 1 van de Tao Te Ching: 章

De "Taoïs te groot om te worden beschreven door de naam "Tao". Als het zo eenvoudig genoemd zou kunnen worden, zou het niet de eeuwige Tao zijn.

Hemel en Aarde begonnen met de naamloze (Tao), maar de massa's dingen om ons heen werden met namen gemaakt.

We willen de wereld begrijpen door namen te geven aan de dingen die we zien, maar deze dingen zijn slechts de effecten van iets subtiels.

Wanneer we verder kijken dan de wens om namen te gebruiken, kunnen we de naamloze oorzaak van deze effecten voelen.

De oorzaak en de effecten zijn aspecten van hetzelfde, één ding. Ze zijn zowel mysterieus als diepzinnig.

Op hun meest mysterieuze en diepzinnige punt ligt de *"Poort van de Grote Waarheid"*.

道可道
非常道
名可名
非常名。
無, 名天地之始
有, 名萬物之母。
故常無欲以觀其妙
常有欲以觀其徼。
此兩者
同出而異名
同謂之玄。
玄之又玄
衆妙之門。

Mensen moeten in de eerste rechtvaardige principes hebben en dan zullen ze niet nalaten om deugdzame daden te verrichten.

Martin Luther

D Principes

Principes zijn de verlengstukken van filosofieën die gedachten raamwerken opzetten en fungeren als richtlijnen voor goed gedrag tussen onszelf en anderen.

D.1 Individueel

1. **Evalueer** als een middel tot grotere **kennis**
2. **Geluk** als gevolg van **deugd**
3. **Respect** als resultaat van **diepgang**
4. **Vrijheid** als de meest ware **uitdrukking**

D.2 Collectief

1. **Doel** met ontvankelijkheid, **Eerlijk** in Communicatie
2. **Respectvol** in gedrag, **Begrip** in Conflict
3. **Eer** aan een gesproken Woord, **Harmonie** met Actie

E Hoe we verandering maken

De cellen van ons lichaam werken samen om de capaciteit voor het leven te bieden. Op dezelfde manier kunnen we de cellen van onze planeet met elk individu vergelijken. Als we de voordelen van samenwerking begrijpen, kunnen uitdagingen grondig en snel worden opgelost zonder onnodige problemen. Dit is hoe we verandering maken; samenwerken om haalbare oplossingen te bieden voor uitdagingen. Dit is de meest efficiënte en effectieve manier om verandering in de richting van onze voorkeuren te sturen.

De gemeenschap is de basis van een economie. Een economie is alleen zo sterk als de basis. Wanneer mensen het vertrouwen in een economie verliezen, zal de basis van de economie instorten en zal de waarde van het systeem dalen. De Nexus community is reeds erg veerkrachtig tegen de stress van de markten. De community is een positieve aaneenhang van een groep mensen over de hele wereld die allemaal streven naar dezelfde doelen als transparantie, welvaart en vrijheid.

Nexus wil een sterke community opbouwen op basis van een spaarcultuur en liefdadigheid. De spaarcultuur is al lang verloren gegaan, maar het is het beste verzekeringsbeleid voor onzekere tijden die mogelijk in het verschiet liggen. Dit helpt de gemeenschap zich af te dekken tegen risicovolle en volatiele markten. Het idee is dat je communitylid je buurman is. Als je buurman het goed doet, zal je lokale economie ook gedijen.

F Lijst met bijdragers

1. Colin Cantrell
   Architect - colin@nexus.io
2. Kierre Reeg
   Visionary - kierre@nexus.io
3. Bryan Gmyrek Ph.D.
   Developer - bryan@nexus.io
4. Preston Smith
   Community Manager - preston@nexus.io
5. Keith Smith
   Cryptocurrency Expert - keith@nexus.io
6. Jacynda Smith
   Cryptocurrency Expert - jacynda@nexus.io
7. Mara Michael
   Editor - maramichael@q.com
8. Glenn Bogaerts
   Vertaler - glenn@bossit.be
9. Geschreven door sommigen van ons, Gegeven door ons allemaal
   The Nexus Community - team@nexus.io

Referenties

[1] Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf

[2] Wat zijn enkele historische voorbeelden van hyperinflatie? Investopedia. http://www.investopedia.com/ask/answers/061515/what-are-some-historic-examples-hyperinflation.asp

[3] William F. Ehrsam, Carl H. W. Meyer, John L. Smith, Walter L. Tuchman, "Message verification and transmission error detection by block chaining", US Patent 4074066, 1976 https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

[4] Mesh networking. Wikipedia. https://en.wikipedia.org/wiki/Mesh_networking

[5] Uitleg over wat Cache of tijdelijk geheugen is https://nl.wikipedia.org/wiki/Cache_(tijdelijk_geheugen)

[6] Nexus releases on GitHub.com https://github.com/Nexusoft/Nexus/releases

[7] SKMiner https://github.com/BitSlapper/SKMiner

[8] Wolf Niro Miner https://github.com/OhGodAPet/Wolf-Niro-Miner

[9] Clock Drift. Wikipedia. https://en.wikipedia.org/wiki/Clock_drift

[10] NexusEarth.com http://nexusearth.com/

[11] Cryptographic hash function. (2016, December 1). Wikipedia, The Free Encyclopedia. Retrieved 01:37, May 18, 2017 from https://simple.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=5540578.

[12] King, S.; Nadal, S. (August 12, 2012). "PPCoin: Peer-to-peer crypto-currency with proof-of-stake"(PDF). peercoin.net. Retrieved 2013-12-23. https://peercoin.net/assets/paper/peercoin-paper.pdf

[13] SEC 2: Recommended Elliptic Curve Domain Parameters, Daniel R. L. Brown (dbrown@certicom.com), Version 2.0, Section 3.7.2. 2010. Retrieved Jan 27, 2017 http://www.secg.org/sec2-v2.pdf

[14] secp256k1. Bitcoin Wiki. https://en.bitcoin.it/wiki/Secp256k1

[15] Submission Requirements for Post Quantum Cryptography https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/call-for-proposals-final-dec-2016.pdf

[16] Block hashing algorithm, Bitcoin Wiki https://en.bitcoin.it/wiki/Block_hashing_algorithm

[17] SHA-2. Wikipedia. https://en.wikipedia.org/wiki/SHA-2

[18] The Skein Hash Function Family. Version 1.3 1 Oct 2010. http://www.skein-hash.info/sites/default/files/skein1.3.pdf

[19] NIST Releases SHA-3 Cryptographic Hash Standard https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard

[20] Hashcash - A Denial-of-Service Countermeasure. Adam Back. 2002. http://www.hashcash.org/hashcash.pdf

[21] Google Security Blog: Announcing the First SHA1 Collison. Feb 23, 2017. https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

[22] NIST: SHA-3 Winner, October 2nd, 2010 http://csrc.nist.gov/groups/ST/hash/sha-3/winner_sha-3.html

[23] The Nobel Prize in Physics 1965 was awarded jointly to Sin-Itiro Tomonaga, Julian Schwinger and Richard P. Feynman "for their fundamental work in quantum electrodynamics, with deep-ploughing consequences for the physics of elementary particles"http://www.nobelprize.org/nobel_prizes/physics/laureates/1965/

[24] Nature: FIGURE 4. Implementation of Grover's search algorithm, July 9th, 2009 http://www.nature.com/nature/journal/v460/n7252/fig_tab/nature08121_F4.html

[25] Estimating Cost of generic quantum pre-image attacks, October 13th, 2016 https://arxiv.org/pdf/1603.09383.pdf

[26] Will Bitcoin's Block Rewards Halving Bring Crisis or Consistency? CoinDesk. http://www.coindesk.com/crisis-halving-bitcoin-mining/ip

[27] Quantum Attacks on Public Key Cryptosystems, Song Y. Yan 2013 http://www.springer.com/us/book/9781441977212

[28] bitcore-lib docs. Script section. https://github.com/bitpay/bitcore-lib/blob/master/docs/script.md

[29] Golden Mean. http://www.anus.com/zine/articles/draugdur/golden_mean/

[30] Nicomachean Ethics. Wikipedia. https://en.wikipedia.org/wiki/Nicomachean_Ethics

[31] Objectivism (Ayn Rand). Wikipedia. https://en.wikipedia.org/wiki/Objectivism_(Ayn_Rand)

[32] Kingdom of Ends. Wikipedia. https://en.wikipedia.org/wiki/Kingdom_of_Ends

[33] Aristotole. Wikipedia. https://en.wikipedia.org/wiki/Aristotle

[34] Immanuel Kant. Wikipedia. https://en.wikipedia.org/wiki/Immanuel_Kant

[35] TheTao.info http://www.thetao.info/index.htm

[36] TheTao.info Chaper 1. http://www.thetao.info/english/page1.htm

[37] Tragedy of the Commons. Investopedia. http://www.investopedia.com/terms/t/tragedy-of-the-commons.asp

[38] Nexus Prime Solo Miner Source Code, Github.com https://github.com/Nexusoft/PrimeSoloMiner

[39] NXSPrime.com http://nxsprime.com

[40] Probable prime. Wikipedia. https://en.wikipedia.org/wiki/Probable_prime

[41] Fermat primality test. Wikipedia. https://en.wikipedia.org/wiki/Fermat_primality_test

[42] Finding Clusters of Primes, I, Jorg Waldvogel and Peter Leikauf, January 2003. http://www.sam.math.ethz.ch/~waldvoge/Projects/clprimes03.pdf

[43] Prime Constellation - Wolfram MathWorld http://mathworld.wolfram.com/PrimeConstellation.html

[44] Wikipedia. Prime k-tuple: Prime Constellations https://en.wikipedia.org/wiki/Prime_k-tuple#Prime_constellations

[45] Quantum Magazine: Physicists Attack Math's $1,000,000 Question. https://www.quantamagazine.org/quantum-physicists-attack-the-riemann-hypothesis-20170404/

[46] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. Peter W. Shor (AT&T Research). http://arxiv.org/abs/quant-ph/9508027

[47] J. Proos, C. Zalka, Shor's discrete logarithm quantum algorithm for elliptic curves. Quant. Inf. Comput. 3(4), 317-344 (2003). https://arxiv.org/abs/quant-ph/0301141

[48] Optimized quantum implementation of elliptic curve arithmetic over binary fields. Phillip Kaye, Christof Zalka. 2004. https://arxiv.org/abs/quant-ph/0407095

[49] SHA3-256 is quantum-proof, should last BEELLIONS of years, say boffins. The Register. http://www.theregister.co.uk/2016/10/18/sha3256_good_for_beelions_of_years_say_boffins/

[50] Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3 http://eprint.iacr.org/2016/992

[51] "Ooh Aah... Just a Little Bit": A small amount of side channel can go a long way. N. Benger, J. van der Pol, Nigel P. Smart and Y. Yarom. http://eprint.iacr.org/2014/161

[52] Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack. Yuval Yarom. Naomi Benger. February 24, 2014. https://eprint.iacr.org/2014/140.pdf

[53] The Amazing Math of Bitcoin Private Keys - James DeAngelo. WeUseCoins.com. https://www.weusecoins.com/amazing-math-bitcoin-private-keys/

[54] SHA-256. Bitcoin Wiki. https://en.bitcoin.it/wiki/SHA-256

[55] SHA-3. Wikipedia. https://en.wikipedia.org/wiki/SHA-3

[56] NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition. October 02, 2012. NIST.gov https://www.nist.gov/news-events/news/2012/10/nist-selects-winner-secure-hash-algorithm-sha-3-competition

[57] Skein (hash function). Wikipedia. https://en.wikipedia.org/wiki/Skein_(hash_function)

[58] The Large Bitcoin Collider Is Generating Trillions of Keys and Breaking Into Wallets. Jordan Pearson. Apr 13 2017. MOTHERBOARD. https://motherboard.vice.com/en_us/article/nzpv8m/the-large-bitcoin-collider-is-generating-trillions-of-keys-and-breaking-into-wall

[59] Key Size. Wikipedia. https://en.wikipedia.org/wiki/Key_size

[60] "Information Assurance". Nsa.gov. 2016-05-04. Archived on 2009-02-07. Retrieved July 2017. https://web.archive.org/web/20090207005135/http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[61] Cryptography/Brute force attack. Wikibooks.org. Retrived on July 2, 2017. https://en.wikibooks.org/wiki/Cryptography/Brute_force_attack

[62] Bitcoin Developer Guide. P2PKH Script Validation. Bitcoin.org https://bitcoin.org/en/developer-guide#p2pkh-script-validation

[63] A fast quantum mechanical algorithm for database search. Lov K. Grover (Bell Labs, Murray Hill NJ) https://arxiv.org/abs/quant-ph/9605043