Whitepaper (Dutch)

P2P Digital Asset Distribution
aphelion.org
support@aphelion.org
October 2017 v.08

Samenvatting: Aphelion is gebouwd om de inherende problemen van de crypto-beurzen en handelsplatformen op te lossen. Aphelion gebruikt de distributed ledger-technologie (DLT) als een open source, peer-to-peer (P2P), gedecentraliseerd activa distributie toepassingsprotocol dat is gebouwd op de NEO-blockchain. Aphelion is ontworpen om een token gestuurde transactie aan te sturen die een Distributed Exchange Asset Ledger of DEAL wordt genoemd. Aphelion DEAL-transacties worden gefaciliteerd door smart contracts en gemaakt door gebruikers. Hierdoor is men onafhankelijk van beurzen of Handelsplatformen en zijn de beperkingen die zij inherent creëren niet meer aanwezig. Een Aphelion-token is het liquiditeitscontroleapparaat (LVD) dat de DEAL rechtstreeks tussen gebruikers aanstuurt: direct, veilig en vrij.

Disclaimer: Deze whitepaper vormt geen aanbod of uitnodiging om effecten of aandelen te verkopen en dient uitsluitend ter informatie. Het APH-token wordt beschouwd als een gebruiksmiddel dat is gebouwd binnen de blockchain-technologie. Het Aphelion-token (APH) -aanbod vertegenwoordigt geen aandelen of verkoop van effecten; het Aphelion-token kent geen aandelen- of stemrechten toe; het Aphelion-token verleent geen eigendomsrechten direct of indirect aan het Aphelion-bedrijf, het zijn fysieke, virtuele of intellectuele eigenschappen; het Aphelion-token geeft geen schuldzekerheid en is geen schuldinstrument; het Aphelion-token betaalt geen distributie-, uitbetalings- of rentebetaling aan token-houders. Als er toekomstige aanbiedingen beschikbaar komen, worden deze via vertrouwelijke en geschikte kanalen gemaakt en worden alle noodzakelijke wettelijke vereisten nageleefd. In overeenstemming met recente sec-aankondigingen, zal Aphelion geen bijdragen van een Amerikaanse ingezetene of ingezetene op de markt brengen of accepteren. In overeenstemming met de China Securities and Regulatory Commission (CSRC) en de People's Bank of China (PBOC) -voorschriften, zal Aphelion geen bijdragen van burgers of inwoners van de Volksrepubliek China (PRC) op de markt brengen of accepteren. In overeenstemming met de monetaire autoriteit van Singapore, zal Aphelion geen bijdragen van burgers of inwoners van Singapore in de handel brengen of accepteren.

Kennisgeving aan burgers en inwoners van de Verenigde Staten van Amerika: deze website en het aanbiedingsmemorandum zijn niet bij de Securities and Exchange Commission (SEC) ingediend als onderdeel van een registratieverklaring. Dienovereenkomstig mag deze website en het aanbiedingsmemorandum en enig ander document of materiaal in verband met de aanbieding of verkoop, of uitnodiging voor inschrijving of aankoop van de APH-tokens niet worden verspreid of gedistribueerd, noch mogen de APH-tokens worden aangeboden of verkocht, of een hulpmiddel kan zijn van een uitnodiging tot inschrijving of aankoop, direct of indirect, voor personen in de Verenigde Staten van Amerika.

Voor inwoners en burgers van de Volksrepubliek China (die voor de doeleinden van dit document en aanbiedingsmemorandum Hong Kong, Macau en Taiwan niet omvatten): APH-tokens mogen niet direct of indirect op de markt worden gebracht, aangeboden of verkocht aan openbaar in China en noch dit document noch het aanbiedingsmemorandum, dat niet aan de Chinese effecten- en regelgevende commissie is voorgelegd, noch enig aanbiedingsmateriaal of informatie hierin opgenomen met betrekking tot APH-tokens, mag aan het publiek in China worden verstrekt of in verband worden gebruikt bij elke aanbieding voor de inschrijving of verkoop van APH-tokens aan het publiek in China. De informatie op deze website en het aanbiedingsmemorandum vormen geen

aanbod om te verkopen of een uitnodiging, advertentie of verzoek om een aanbod om APH-tokens in de VRC te kopen.

Kennisgeving aan potentiële inschrijvers in Singapore: deze website en het aanbiedingsmemorandum zijn niet geregistreerd als een prospectus bij de monetaire autoriteit van Singapore onder de Securities and Futures Act (SFA) (hoofdstuk 289). Dienovereenkomstig mag deze website en het aanbiedingsmemorandum en enig ander document of materiaal dat een verband met de aanbieding of verkoop, of uitnodiging voor inschrijving of aankoop van de APH-tokens niet worden verspreid of gedistribueerd, noch mogen de APH-tokens worden aangeboden of verkocht, of een hulpmiddel kunnen zijn van een uitnodiging tot inschrijving of aankoop, direct of indirect, voor personen in Singapore.

Inhoudsopgave

Wat is Blockchain-technologie?

1. Inleiding

Gedistribueerde grootboeken (ledgers), blockchain-technologie, cryptovaluta en hun smart contracts verstoren een groot aantal industrieën. Sterker nog, experts beweren dat het de verwachting heeft de wereld meer te verstoren dan enige andere industriële ontwikkeling in de geschiedenis. We zien nu al dat de applicaties vooral groeien in de financiële wereld. Als onderdeel van deze nieuwe

technologie bouwen ontwikkelaars ongelooflijk veel nieuwe tools die hun weg dan ook zullen vinden naar het grote publiek en instellingen die deze dan ook zullen omarmen.

1.1 Achtergrond

Als onderdeel van het blockchain ecosysteem zijn cryptovaluta zoals Bitcoin (BTC), NEO (voorheen AntShares) en Ethereum (ETH) naar voren gekomen als vroege leiders in de distributie van digitale bedrijfsmiddelen. Gebaseerd op blockchaintechnologie en gedistribueerde ledgers, ontwikkelde Satoshi Nakamoto in 2008 de eerste cryptovaluta genaamd Bitcoin (BTC) [1]. Sindsdien zijn er veel cryptovaluta gecreëerd en groeit de totale markt als nooit tevoren (tot 1000% + in 2017). Ondernemers, durfkapitalisten, bankiers en andere experts speculeren dat cryptovaluta uiteindelijk de nieuwe norm zullen worden. Met als resultaat dat er een hele reeks nieuwe bedrijven zullen verrijzen. Maar de blockchain- en gedistribueerde ledger technologie die achter de opkomende cryptovaluta liggen zullen een veel belangrijkere rol kunnen gaan spelen.

1.2 Blockchain-technologie

Cryptovaluta worden mogelijk gemaakt door blockchain-technologie. "De blockchain is een onveranderlijk digitale grootboek (ledger) van economische transacties. Deze kunnen worden geprogrammeerd om niet alleen financiële transacties registreren maar vrijwel alles van waarde te registreren." [2] Wat is Blockchain-technologie? "Blockchain is vergelijkbaar met een historisch weefsel (kleed) waarin alles kan worden vastleggen. Wat er precies gebeurt zoals en hoe het zich voordoet. Men kan het zien als een draad of keten met gegevens in gecodeerde blokken die nooit kunnen worden gewijzigd. Deze stukken worden verspreidt over een wereldwijd netwerk van gedistribueerde computers of "knooppunten" (Nodes). Blockchain heeft altijd een onveranderlijk "grootboek" (Ledger) dat u kunt inzien en controleren. Tegelijkertijd heeft het geen enkel zwakpunt waaruit records of digitale assets kunnen worden gehackt of beschadigd. Vanwege de gedistribueerde ledger technologie heeft blockchain toepassingen in alle soorten digitaal archief en transacties. We beginnen nu al een grote verschuiving te zien naar verschillende industrieën. "[3]

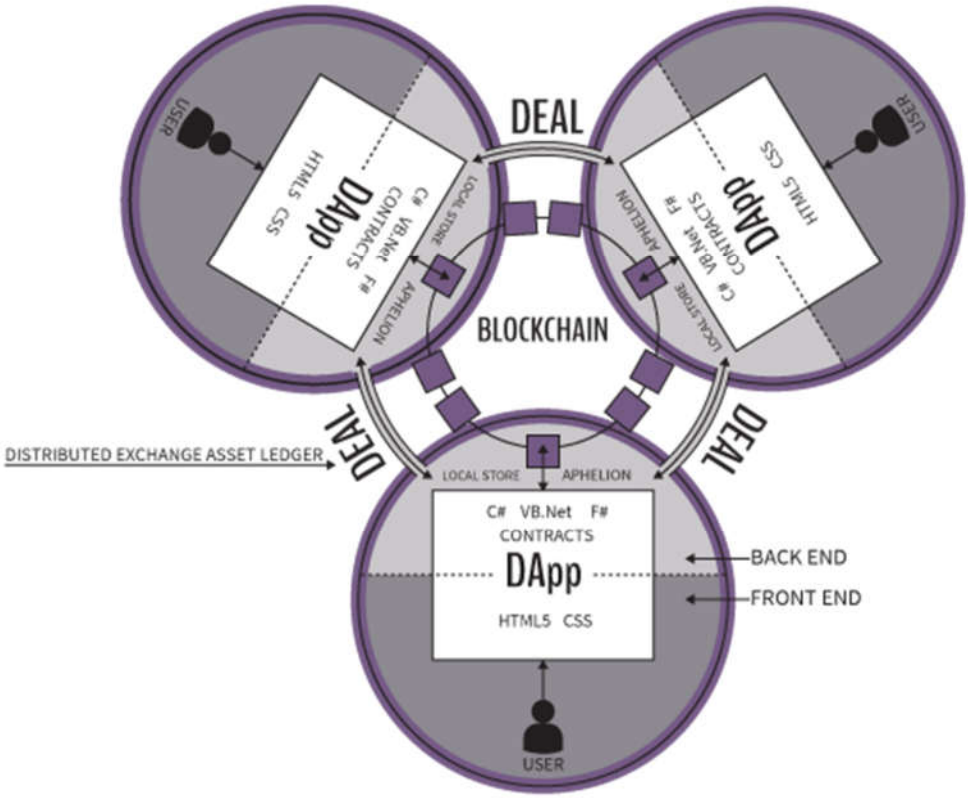
1.3 Gedistribueerde Ledger-technologie

"Een gedistribueerd ledger is een type database verspreid over meerdere sites, regio's of deelnemers. Zoals je zou verwachten moet een gedistribueerd ledger worden gedecentraliseerd. Anders zou het lijken op een gecentraliseerde database zoals de meeste bedrijven tegenwoordig gebruiken. Het verwijderen van de tussenpartij maakt het concept van gedistribueerde ledger technologie zo aantrekkelijk. Bovendien gebruiken ondernemingen gedistribueerde ledger technologie voor het verwerken, valideren of authentiseren van transacties of andere soorten gegevensuitwisseling. Records worden opgeslagen in een ledger zodra consensus (overeenstemming) is bereikt door de meerderheid van de partijen. Elk record dat is opgeslagen in het gedistribueerde grootboek heeft een tijdstempel en heeft een eigen cryptografische handtekening. Alle deelnemers aan het gedistribueerde ledger kunnen alle records in kwestie bekijken. De technologie biedt een verifieerbaar en controleerbare geschiedenis van alle informatie die is opgeslagen in die specifieke dataset. Gedistribueerde ledger technologie zal vaak worden aangeduid als DLT in financiële en regeringskringen. "[4] Door gebruik te maken van DLT zal Aphelion de gedecentraliseerde P2P-transacties op een veilige en beveiligde echt decentraliseren m.b.v. het APH token uitvoeren. Het omzeilen van de traditionele gecentraliseerde beurzen op deze manier en de DEAL laten plaatsvinden op een gedistribueerd ledger op de NEO blockchain. Dit is een enorme stap voorwaarts in de toekomst van crypto-transacties.

1.4 Gedecentraliseerde toepassing (DApp)

Een gedecentraliseerde toepassing of DApp, zoals deze is afgekort, heeft zijn back-endcode die werkt op een gedecentraliseerd peer-to-peer-netwerk. Een DApp kan een frontendcode en gebruikersinterfaces hebben die in elke taal zijn geschreven (net als een app) die naar de backend kan “bellen”. Bovendien kan de front-end worden gehost op gedecentraliseerde opslag zoals Swarm

of IPFS. Zoals geïllustreerd in de onderstaande afbeelding, als een app = frontend + server, dan DApp = frontend + community + contracten. Aphelion-contracten zijn codes die wordt uitgevoerd op het wereldwijde gedecentraliseerde peer-to-peer-protocol van Aphelion.



Aphelion is van nature een DApp en een gedecentraliseerde toepassing: peer-to-peer, open source, autonoom geëxploiteerd.Deze kan niet worden beheerd door een enkele operator of entiteit. Het cryptografische Aphelion token (APH) wordt opgeslagen in een openbare gedecentraliseerde blockchain.

1.5 PoW, PoS en dBFT van de volgende generatie

Van PoW tot PoS "Proof-of-Work (PoW), is het consensusalgoritme van Bitcoin dat verantwoordelijk is voor de hoge energievraag van het netwerk. Dit maakt het boekhoudmechanisme van het systeem kunstmatig intensief deze slurpt hierdoor energie. De Bitcoin-knooppunten moeten door prestaties van cryptografische taken zoals blokken en verificatie van transacties bewijzen om zo in aanmerking te komen voor de gewilde blokbeloning. Volgens de energieramingen hierboven vermeld, betekent dit dat dankzij PoW een aanvaller het geaggregeerde energieverbruik van een kleine Noord-Amerikaanse stad zou moeten investeren om een groot aandeel op de Bitcoin-blockchain te krijgen en zo de meerderheid te creëren. Het populairste alternatief voor PoW, gebruikt door de meeste alternatieve cryptovaluta-systemen, wordt Proof-of-Stake of PoS genoemd. PoS is veelbelovend in de zin dat het geen blockchain-knooppunten vereist. Om zware en anderszins nutteloze cryptografische taken uit te voeren om potentiële aanvallen kostbaar en onhaalbaar te maken. Vandaar dat dit algoritme de stroomvereisten van PoS-blockchains reduceert tot normale en beheersbare hoeveelheden. Waardoor ze meer schaalbaar zijn zonder de energiereserves van de planeet op te slurpen. PoS is een levensvatbaar alternatief voor PoW hoewel het zeer energie-inefficiënt is, zichzelf de afgelopen acht jaar als betrouwbaar heeft bewezen. Beide systemen hebben echter een cruciale fout die zelden wordt aangepakt in de nog enigszins conservatieve crypto-gemeenschap. PoS, net als

PoW laat de blockchain simpelweg toe om twee alternatieve versies te berekenen als er om de een of andere reden consensusonderbrekingen zijn. In feite zijn de meeste blockchains continue aan het splitsen “Fork” (verschillend pad/uitkomst). Om daarna terug te converteren naar een enkele bron van waarheid zoals in de bovenstaande afbeelding wordt weergegeven. Bij veel crypto-enthousiasten wordt deze voor de hand liggende bug vaak als een functie beschouwd. Waardoor verschillende versies van de waarheid kunnen overleven en strijden om publieke acceptatie totdat een oplossing wordt gegenereerd. Dit klinkt in theorie leuk, maar als we blockchain-technologie serieus de financiële sector willen laten verstoren en/of vergroten kan de mogelijkheid van de blockchain die zich splitst in twee alternatieve versies niet worden getolereerd. Byzantijnse fouttolerantie en dBFT. De term Byzantijnse foutentolerantie (BFT) ontleent zijn naam aan het Byzantijnse generaalsprobleem in speltheorie en computerwetenschap. Deze beschrijft het problematische karakter van het bereiken van consensus in een gedistribueerd systeem met suboptimale communicatie tussen middelen die elkaar noodzakelijkerwijs niet vertrouwen. Het BFT-algoritme rangschikt de relatie tussen blockchain-knooppunten (nodes) op een zodanige manier dat het netwerk resistent is voor het probleem dat Byzantijnse generaals hadden. Dit maakt het mogelijk dat het systeem een consensus bereikt, zelfs als sommige knooppunten (nodes) kwade kwaadaardige bedoelingen hebben of eenvoudigweg niet werken. Om dit te bereiken erkent de versie van de gedelegeerde BFT (of dBFT)-algoritme van NEO twee soorten spelers in de blockchain-ruimte: professionele knooppunt(node)operators, boekhoudknopen (ledgernodes) genoemd. Deze spelers hebben knooppunten (nodes) als bron van inkomsten die ze beheren en gebruikers die geïnteresseerd zijn in de voordelen en zo tevens toegang tot blockchain willen hebben. Theoretisch is deze differentiatie niet aanwezig in PoW en de meeste PoS-omgevingen. Praktisch gezien hebben de meeste Bitcoin-gebruikers geen miners. Deze bevinden zich meestal op gespecialiseerde locaties van professionals. Blokverificatie wordt daarom bereikt door middel van een consensusspel dat wordt gehouden tussen gespecialiseerde boekhoudknooppunten die worden aangewezen door gewone knooppunten via een vorm van gedelegeerd stemproces. In elke verificatieronde is een van de boekhoudknooppunten pseudo-willekeurig benoemd om zijn versie van de blockchain uit te zenden naar de rest van het netwerk. Als ⅔ van de overige knooppunten het eens is met deze versie wordt consensus bereikt en gaat de blockchain verder. Als minder dan ⅔ van het netwerk hiermee instemt wordt een ander knooppunt aangewezen om zijn versie van de waarheid uit te zenden naar de rest van het systeem totdat een consensus is bereikt. Op deze manier zijn succesvolle systeemaanvallen bijna onmogelijk uit te voeren tenzij de overweldigende meerderheid van het netwerk geïnteresseerd is in het plegen van financiële zelfmoord. Bovendien is het systeem “Fork” (splitsing) bestendig en bestaat er op elk gegeven moment slechts één versie van de waarheid. Zonder ingewikkelde cryptografische puzzels om op te lossen werken knooppunten veel sneller en kunnen ze concurreren met gecentraliseerde transactiemethoden. "[5]

1.6 Aphelion gebouwd op NEO dBFT

Omdat dBFT een oplossing biedt voor de bovengenoemde “problemen” die in Bitcoin PoW en de daaropvolgende alternatieve PoS-technologieën, die hierboven zijn uiteengezet, zal Aphelion worden gebouwd op NEO als een milieuvriendelijke, open source, volledig gedecentraliseerde digitale activatoepassing die de meest veilige en gedecentraliseerde toepassing voor digitale activadistributie creëert. Hierdoor kunnen gebruikers van Aphelion de DEAL P2P afhandelen en zo onafhankelijk van de traditionele beurzen/handelsplatformen zijn en zo de beperkingen/uitdagingen die ze met zich meebrengen achter zich laten. Aphelion is een tokenized DApp-protocol.

Waarom Neo? NEO ondersteunt de snelle ontwikkeling en implementatie van smart contracts en projecten, omdat ontwikkelaars kunnen programmeren met programmeertalen die ze al kennen. We bieden verschillende geavanceerde talen in de vorm van een compiler ", zegt Da Hongfei (oprichter van NEO). "Naast .Net en Java ondersteunen we Python en Go, die meer dan 90 procent van de ontwikkelaars beheersen. In vergelijking met Ethereum heeft de ontwikkeling een soepele leercurve en kortere leerkring, waardoor projecten snel kunnen worden gelanceerd. "

	Bitcoin	Ethereum	Neo
Rendement	POW op ASIC-machines gebruikt enorme hoeveelheden energie	GPU-mijnwerkers die gezamenlijk meer energie gebruiken dan een heel land*	dBFT garandeert finaliteit door uiterst efficiënte methode
Veilige contracten	Pseudo-anonimiteit creëert een gebrek aan integriteit in transacties	Kwetsbare contractcode die vatbaar is voor aanvallen door hackers **	Geïntegreerde digitale identiteit maakt toepassingen in de echte wereld mogelijk
Programmeer talen	C ++	Solidity	Solidity C #, .Net, Java, Python en Go komen voor 90% van de ontwikkelaars
Schaalbaarheid	Piektransactie per seconde is beperkt tot 3-4	Huidige piektransactie per seconde is 20	Tot 10.000 transacties per seconde

1.7 De Cryptovaluta-markt

"Vanaf april 2017 is de gecombineerde marktwaarde van alle cryptovaluta $27 miljard. Wat een niveau van waarde creatie vertegenwoordigt zoals in de succesverhalen in Silicon Valley liggende startups o.a. AirBnB. etc" [9] Eind augustus 2017 overtrof de marktkapitalisatie $180 miljard wat betekent dat de totale marktkapitalisatie van cryptovaluta dit jaar met bijna 1000% is gestegen volgens bitcoin.com. [12]. Het Probleem met Blockchain-technologie en de daaropvolgende cryptovaluta zijn zo nieuw dat er veel uitdagingen bestaan voor handelsplatformen en beurzen. Momenteel sluiten digitale valuta's niet op dezelfde manier op elkaar aan als informatienetwerken. Het huidige valutamodel voor valuta's heeft een kritische barrière voor het koppelen van kleinschalige valuta's aan andere populaire valuta's aan de hand van een door de markt bepaalde wisselkoers. Bovendien fungeren de beurzen en Handelsplatformen in wezen als een gecentraliseerd systeem. Die inherent bijbehorende fouten met zich meebrengt en het doel van decentralisatie verslaat. Uitdagingen voor crypto beurzen en Handelsplatformen van vandaag: centralisatie: regels, vergoedingen, niet-liquide activa, uitwisselingen controleren privésleutels voor wallets van gebruikers waardoor de beurs/handelsplatform volledige de bewaarrechten van de cryptovaluta kan hebben. Complexiteiten: Handelsplatformen en beurzen missen in vrijwel elk aspect het doel waarvoor de technologie is bedoeld. Belemmeringen voor toegang: er zijn verschillende regels om lid te worden van elk platvorm, vertragingen bij de goedkeuring, traditionele valutadossiers versus digitale stortingen en gebrek aan onmiddellijke stortingen. Problemen tijdens het gebruik: transacties geblokkeerd zonder uitleg, dagelijkse limieten, slechte gebruikersinterface, software met fouten en niet gebruiksvriendelijk. Latency: onophoudelijk gebrek aan snelheid en prestatieproblemen. Gebrek aan ondersteuning: er is een compleet gebrek aan klantenondersteuning en de mogelijkheid om op de meeste grote platvormen te reageren/ klacht in te dienen; Het is niet ongewoon om weken of maanden te wachten op een antwoord. Gebrek aan beveiliging: meerdere hacks, verloren geld, inbreuken op de privacy en afgesloten sites. Gebrek aan privacy: vereiste verificatie, creditcard, rijbewijs scans, paspoorten etc.

2. Het probleem

2.1 Cryptovaluta-uitdagingen

Omdat Bitcoin een relatief simpel blockchain-systeem is zijn er extra ontwikkelingsprotocollen nodig om het functioneel te maken voor transactionele uitwisselingen. NEO is ook compatibel met verschillende codeertalen, terwijl ETH alleen compatibel is met Solidity. "Bijvoorbeeld, terwijl je misschien denkt dat het huidige proof-of-work (POW) consensusmechanisme gebruikt door Bitcoin en Ethereum een voordeel is, maar in tegen deel dit komt eigenlijk met een prijs. Er is een probleem met het gebrek aan finaliteit. Bitcoin-transacties zijn definitief, zegt u? Niet echt. Het protocol geeft de voorkeur aan beschikbaarheid boven finaliteit - dit betekent dat een “Fork” (splisting) en alleenstaande blokken een mogelijkheid zijn. We hebben eerder gezien hoe Bitcoin-projecten de neiging hebben om te 'forken/splitsen' wanneer er ernstige beveiligingsproblemen zijn of wanneer ontwikkelaars meningsverschillen hebben met betrekking tot de standaard. POW is ook erg energie-intensief, wat betekent dat knooppunten (nodes) een hoge energie rekening hebben. "[6]

2.2 Gecentraliseerde beurzen

Er is een wijdverbreid gebruik van verschillende cryptovaluta-Handelsplatformen en beurzen. Ze zijn het duidelijke voorbeeld mechanisme voor P2P-handel, maar ze zijn niet gedecentraliseerd. Ze fungeren als tussenpersoon tussen handelaren die transacties initiëren en dit brengt een aantal inherente uitdagingen met zich mee. Ten eerste bepalen beurzen de regels voor wie kan handelen, wat kan worden verhandeld en wanneer. Er zijn talloze verhalen over gebruikersaccounts en zelfs geïnitieerde transacties worden zonder uitleg verwijderd of bevroren. We hebben ook talloze beveiligingsinbreuken gehad waardoor honderden miljoenen (USD) zijn gestolen. Bovenop deze inherente uitdagingen die de beurzen met zich meebrengen is er momenteel een volledig gebrek aan ondersteuning waarmee veel gebruikers worden geconfronteerd. Deze zogenaamde gedecentraliseerde beurzen zijn helemaal niet gedecentraliseerd. In feite helemaal niet het is eigenlijk net het tegenovergestelde. "P2P-beurzen zijn niet beter dan de reguliere beurzen in elk opzicht; langere handelstijden, minder intuïtieve use-cases en lagere liquiditeit zijn enkele van hun relatieve nadelen. De meeste tekortkomingen van gedecentraliseerde beurzen worden veroorzaakt door het feit dat ze een relatief nieuw soort dienst zijn. Bijvoorbeeld, Bitsquare, misschien wel een van de oudste van dergelijke beurzen, bestaat al drie jaar en het grootste deel daarvan was de ontwikkelingsperiode. Als zodanig hebben deze beurzen te maken met een aantal problemen. De meeste van hen zijn bijvoorbeeld momenteel gericht op kleine, specifieke doelgroepen van crypto-enthousiasten en hebben niet de behoefte gehad om op nieuwkomers in te spelen - daarom zijn ze minder intrek. Om dezelfde redenen - klein publiek en vroege fase van het bestaan, hebben gedecentraliseerde beurzen meestal veel lagere handelsvolumes dan de reguliere beurzen. Langere handelstijden aan de andere kant zijn waarschijnlijk ook een nadeel. Het zal een tijdje duren om dat te veranderen of dit gebeurd helemaal nooit. Dit wordt veroorzaakt door de manier waarop de transacties worden uitgevoerd. Handelaren die moeten wachten op daadwerkelijke Bitcoin- en fiat-transacties voordat een transactie is voltooid. Dit laatste probleem in combinatie met de lagere liquiditeit, betekent dat P2P-beurzen helemaal niet in trek zijn. Bijvoorbeeld bij professionele handelaren die snelle transacties nodig hebben om tijdig deals te sluiten. In hun huidige vorm kunnen deze beurzen/hanelsplatformen alleen maar nuttig zijn voor mensen die geïnteresseerd zijn in de specifieke voordelen die ze bieden - de toegenomen veerkracht, privacy, veiligheid en betalingsvrijheid. "[11]

	Gedecentraliseerde beurzen	Gecentraliseerde beurzen
Gelijkmoedigheid tussen koper en verkoper	X	
Verlies van geld van na stoppen beurs		X
Potentieel van geblokkeerde rekeningen		X
Inkomsten voor uitwisseling van transactie		X
Risico's voor het verhandelen		X
Stortingen vereist		X

2.3 Gedecentraliseerde beurzen

Verschillende projecten claimen dat ze een P2P Gedecentraliseerde Exchange (DEX) zijn. Echter zijn er maar weinig gebouwd als dApps, volledig gebouwd op een blockchain. Sommige zijn gecentraliseerde client-naar-server-operations die afhankelijk zijn van de hardware en bedrijfseigen software van een organisatie. Andere zijn gewoon een protocol dat integratie in bestaande gecentraliseerde beurzen vereist om goed te kunnen functioneren. Aphelion wil een van de pioniers van een DEX zijn die volledig in de blockchain zit als een dApp en heeft alleen een open source gebruikersinterface nodig om toegang te krijgen tot gegevens en smart contracts te beheren om zo digitale activa te verhandelen.

Aandachtspunten:

Ripple

Ripple [12] is een protocol dat een realtime, afwikkelingssysteem, wisselkantoor en overboekingsnetwerk biedt. Het vereist een bestaand netwerk om in te pluggen en is ontworpen om te werken binnen het centrale banksysteem. Het protocol van Ripple kan een revolutie teweegbrengen in de banksector. Dit door blockchain-technologie naar de grootste financiële instellingen ter wereld te brengen. Het biedt echter geen gedecentraliseerd P2P-uitwisselingssysteem.

Shapeshift

Shapeshift [13] is een server gebaseerde operatie die sterk afhankelijk is van zakelijke hardware en software om functioneel te blijven. Shapeshift maakt een opmerkelijke belofte om peer-to-peer te handelen, onmiddellijk zonder geld te storten op een uitwisselingsplatform. Een snelle zoekopdracht zal onthullen dat de gecentraliseerde serverinfrastructuur van shapeshift voor gebruikers kan leiden tot verloren munten en transacties. Dit zonder ondersteuning in moeilijke situaties en deze dan te kunnen verhelpen.

Loopring

Loopring [14] is een uitwisselingsprotocol dat momenteel in ontwikkeling is (vanaf september 2017). Het loopring-protocol vereist bestaande cryptovaluta-beurzen om in te pluggen, inclusief gebruikersautorisatie en bedrijfsintegratie tussen de exchange en loopring. Als loopring de uitdagingen van integratie met bestaande beurzen kan overwinnen, kan het een veelbelovende tussenpersoon blijken te zijn.

Bitshares

Bitshares [15], [16] is een intelligent contractplatform voor financiële blockchain van industriële kwaliteit. Het is een uitstekend voorbeeld van een echt gedecentraliseerde technologie. Sommige nuances die men zou kunnen opmerken over Bitshares DEX is het feit dat als stortingen worden gedaan, uw activa worden opgeslagen. Dit als onderpand voor Bitshares terwijl u de eigen versie van Bitshares van de valuta's die u misschien kent in de echte wereld, de zogenaamde slimme tokens, heeft uitgegeven. Gebruikers moeten afgeleide tokens verhandelen die valuta's en activa uit de echte wereld repliceren. Enkele voorbeelden zijn bitUSD, Bitshares-versie van de Amerikaanse dollar of bitGold, Bitshares-versie van goud.

OpenLedger
OpenLedger [17] Dex is ook een beurs/handelsplatvorm van cryptovaluta. Net zoals Bitshares, kunnen gebruikers ook echte activa uitwisselen in afgeleide tokens, ook wel bekend als slimme tokens die zich in het OpenLedger-netwerk bevinden. Met Openledger handelen bijvoorbeeld Open.BTC en Open.ETH, die OpenLedgers eigen versie van respectievelijk Bitcoin en Ethereum zijn.

Bancor
Het Bancor [18] -protocol maakt ingebouwde prijs en een liquiditeitsmechanisme voor tokens op smart contractblockchains mogelijk. Net als Bitshares en Openledger gebruikt Bancor 'slimme tokens' om een of meer echte tokens in reserve te houden, zodat elke partij het slimme token onmiddellijk kan kopen of liquideren in ruil voor een van zijn reservetokens. Dit gebeurt rechtstreeks via het contract van de slimme token, tegen een continu berekende prijs volgens een formule die koop- en verkoopvolumes in evenwicht brengt.

0x
0x [19] (Zero X) is een protocol dat peer-to-peer uitwisseling van ERC20-tokens op de Ethereum-blockchain vergemakkelijkt. Het protocol is bedoeld om te worden gebruikt in een bestaande dApp om Ethereum-gebaseerde tokenhandel mogelijk te maken.

3. De oplossing
Aphelion's baanbrekende tokengestuurde DApp maakt peer-to-peer activadistributies en smart contracts mogelijk via de DEAL. Aphelion lost de problemen op die de huidige traditionele beurzen en platvormen teisteren. De oplossing is om de centralisatie van die mechanismen te elimineren door gebruikers in staat te stellen vrij hun eigen smart contracts in te stellen en digitale middelen op hun voorwaarden in een open source, beveiligd, snel en echt gedecentraliseerd proces direct op de blockchain uit te wisselen. De Aphelion DApp en het protocoltoken lossen latentie, bevroren of gestolen activa en uiteindelijk gratis crypto-handel op voor altijd.

3.1 P2P Digital Asset Distribution en Protocol
Aphelion is een volgende generatie DApp- en tokenprotocol dat wordt geïntegreerd met elke andere DApp. Aphelion is echt open source, geen eigendom van of wordt beheerd door geen enkele entiteit, organisatie of agent. Door gebruik te maken van de smart contracttechnologie als een protocol met zijn eigen gelicentieërde systemen van escrow of bouwstenen kunnen Aphelion-gebruikers eindelijk de drempels en controles van de cryptovaluta beurzen en Handelsplatformen elimineren. Aphelion stelt gebruikers in staat om rechtstreeks met elkaar te handelen op basis van de contractvoorwaarden die zij kiezen. Het biedt een innovatieve, tokenized escrow-oplossing waarmee gebruikers direct Aphelion-goedgekeurde valuta kunnen verhandelen, verzenden, ontvangen voor iedereen die ze maar willen en waar ze maar willen.

3.2 Missie en visie
Missie: om collaboratieve, open source blockchain-technologie te ontwikkelen die de distributie van activa/bedrijfsmiddelen echt decentraliseert. Visie: een wereld die wordt aangedreven door gedecentraliseerde applicaties.

3.3 Aphelion-technologie
NEO-technologie: via technologieën zoals P2P-netwerken, dBFT-consensus, digitale certificaten, supergeleidende transacties en interoperabiliteit tussen verschillende chains, maakt de blockchain het mogelijk om slimme activa op een efficiënte, veilige en juridisch bindende manier te beheren. Digitale activa: digitale activa zijn programmeerbare activa die bestaan in de vorm van elektronische gegevens. Met blockchain-technologie kan de digitalisering van assets gedecentraliseerd, betrouwbaar, traceerbaar, zeer transparant en vrij van tussenpersonen zijn. Op de blockchain kunnen gebruikers meerdere soorten activa registreren, verhandelen en circuleren, zoals BTC, ETH, XRP, LTC en NEO om er maar een paar te noemen.

3.4 Belangrijkste verschillen
Echte decentralisatie: Aphelion-transacties worden op P2P- en knooppuntbasis (node-based) uitgevoerd zonder controle of invloed van derden. Gebruikers kunnen hun eigen regels instellen in de meest ware definitie van decentralisatie. Het is onmogelijk om de site te verwijderen want er is geen site. De transacties worden pas voltooid wanneer beide partijen de DEAL (Distributed Exchange Asset Ledger) aangaan en het grootboek (ledger) deze op potentieel miljoenen machines logt. Programmeerbaar in meerdere talen: volledig anders dan andere tokens zal Aphelion open en op te bouwen zijn in talen zoals Python, .Net, C #, F #, Go & Java. Waardoor het zeer aantrekkelijk en bevorderlijk is om het aan boord te hebben van diverse codeertalenten. Volgende generatie DApp: het NEO-systeem met een token die gebruik maakt van het DEAL-protocol voor de voorziening van een echte P2P-beurs die volledig gedecentraliseerd is dan de gecentraliseerde traditionele beurzen. Eenvoudig in te voeren: Aphelion vereist alleen toegang tot een open source Aphelion-portal die is ingebouwd in bv. de browser, in-app en op het bureaublad. Beveiliging: omdat de gegevens echt gedecentraliseerd zijn in het gedistribueerde blockchain-grootboek (ledgers), kan deze niet worden gestolen of beschadigd. Controle: Aphelion-gebruikers initiëren de DEAL-transacties en hebben volledige controle over de voorwaarden van hun individuele smart contracts, waardoor de transacties worden bevrijd van vergoedingen en regels.

3.5 Roadmap
Q1 2017 - Concept en onderzoek& O-blockchainopties

- Geïdentificeerde marktleiders
- Cryptovaluta marktonderzoek
- Cryptvaluta beurs/handelsplatform vergelijking/analyse

Q2 2017 - Strategie en ontwerp

- Juridische advies
- Concept gemaakt
- Naam project Aphelion gecreëerd
- Ontwerp mockups
- SWOT-analyse
- Onze missie gemaakt
- Rekrutering van ontwikkelaars mbv concept

Q3 2017 - Initiële bedrijfsuitrol en pre-marketing

- Opgenomen bedrijfseenheid
- Markten Geïdentificeerde

- Oprichter overeenkomst gemaakt
- Website gelanceerd
- Framework gemaakt
- NEO is the One
- Formed Founders alliance agreement
- Gerekruteerde en doorgelichte adviseurs

Q4 2017 - Marketing & ICO

- Start ontwikkeling
- Roll-out marketing
- Ontwikkel influencer-netwerk
- Bouw relaties met liquiditeits verstrekkers
- Implementeer Testnet
- GitHub-repo beheren
- Verbetering van de website en back-end
- KYC verificatie entiteit integratie
- Whitepaper finaliseren en vrijgeven
- Open presale
- Decstack-kanaal
- Slim contracttesten en audits
- ICO-transactietests
- Inital dApp-ontwikkeling
- KYC-audits voltooid
- ICO begint
- ICO wordt gesloten
- Tokens verdeeld
- PR begint
- Updates van wettelijke compliance

Q1 2018 - Een NEO-jaar begint

- Volledige dApp-ontwikkeling begint
- Cross-blockchain-transacties
- Oplossen voor liquiditeitsverificatie
- Marketing gaat door
- Exchange-registraties beginnen
- audits
- APH naar andere beurzen
- Start de eerste versie Aphelion DApp
- Aphelion dApp community ontwikkeling & groei
- Voortdurende marktanalyse
- Vooruitgang van de NEO smart economy

2018 en de toekomst [tbd]

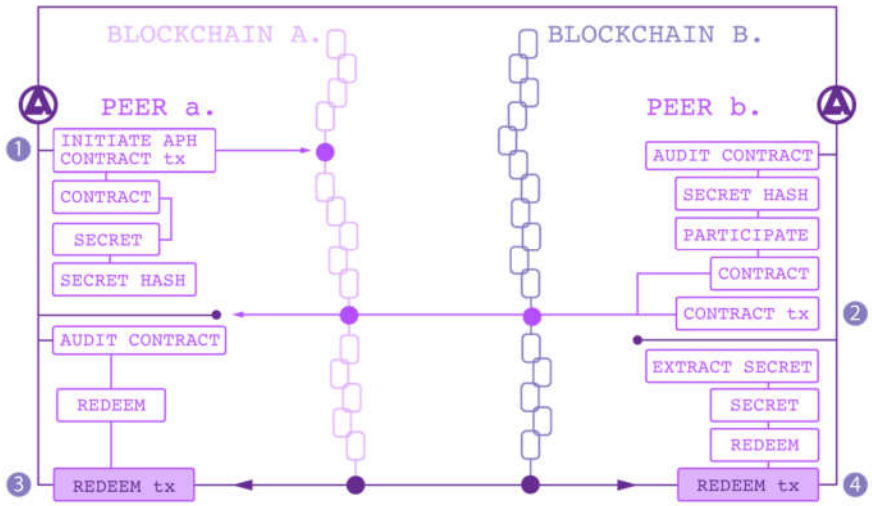
- Gaan door met het verder uitbouwen van het dev-team
- Bouw merk loyaliteit en creëren enthousiaste fans
- Vergroot marktbereik naar alle continenten
- Maak gebruik van partnerschappen om innovatie en integratie te bevorderen
- Vooruitgang boeken innoveren

3.6 Aphelion Tokens - Hoe het werkt ...

APH-tokens vertegenwoordigen een nieuw soort digitale activadistributie. Het Aphelion-token fungeert als een digitale escrow of liquiditeitscontroleapparaat (LVD) en legt tegelijkertijd voorwaarde vast van koper en verkoper, regelt het voorgestelde smart contract, controleert onmiddellijk de liquiditeit en vereffent de DEAL. Aphelion's gedistribueerde Exchange Asset Ledger (of DEAL) voert dit direct P2P uit en zonder toepassing van gecentraliseerde traditionele beurzen mbv een knooppunt (node) gebaseerd gedecentraliseerde ledger. De APH-tokenized DEAL is een protocol - DApp dat direct op de blockchain is gesitueerd. Waardoor de gecentraliseerde beurzen worden omzeild en APH het Liquiditeitverificatie-"apparaat" kan zijn en uiteindelijk de beloften van onmiddellijke, veilige en totale decentralisatie waar maken.

Laten we twee peers beschouwen die digitale assets willen uitwisselen die bestaan op afzonderlijke blockchains. Peer A, we zullen hem Alex noemen, is bereid om sommige van zijn activa op Blockchain A (B.A) te verhandelen voor een minimumbedrag aan activa op Blockchain B (B.B). Peer B, we zullen hem Bob noemen, is bereid om sommige van zijn activa op B.B te verhandelen voor een minimumbedrag van B.A. Beide peers hebben al adressen op beide blockchains en beide partijen kunnen het exchange-contract initiëren. Deze gedistribueerde cross-chain-transactie wordt uitgevoerd in meerdere fasen maar wordt behandeld als een enkele werkeenheid. Uiteindelijk slaagt de uitwisseling aan beide kanten of alles keert terug naar zijn oorspronkelijke staat naar peer A en naar peer B.

1. Hier is het Alex die de cross-chain digital asset exchange initieert met behulp van een Aphelion-token. Dit creëert een contracttransactie die het contract, de secret code (vaak alleen secret genoemd) en een hash van die secret code bevat. Dit vergrendelt dan ook Alex's benodigde bezittingen op B.A en verstrekt het adres op B.B waar hij de activa wil ontvangen.
2. Vervolgens bekijkt Bob het contract (genaamd auditing) en vindt het goed en besluit om deel te nemen volgende de gestelde voorwaarden. Hij gaat akkoord door een nieuwe contracttransactie te maken, waarbij de secret hash van de contracttransactie van Alex wordt gebruikt. Hierdoor worden ook de vereiste activa van Bob op B.B. vergrendeld en wordt het adres op B.A gegeven aan de plaats waar Alex activa naar Bob stuurt.
3. Alex kijkt wat Bob heeft verzonden (de audit) en besluit de DEAL te sluiten. Alex verzamelt de betaling van Bob door een aflossende transactie te maken. Hierdoor wordt Alex's secret voor Bob automatisch vrijgegeven en wordt een tweede verzilverde transactie (4.) gestart waarmee Bob de betaling van Alex kan ontvangen. De twee verzilverde transacties zijn vergelijkbaar met een traditionele relationele database in twee fasen waarbij als een deel van de metatransactie mislukt de individuele transacties worden teruggedraaid.



Een belangrijk element dat niet in dit vereenvoudigde diagram wordt getoond, is dat activa op bepaalde momenten tijdens de uitwisseling ook kunnen worden terugbetaald of worden teruggegeven aan de oorspronkelijke wallet. De contracttransactie van Alex bevat een vergrendeltijd die verloopt nadat de transactie is gedolven maar nog niet is ingewisseld. De contracttransactie van Bob bevat ook een sluis, wat de helft is van Alex's locktime. Als deze locktimes verlopen kan de betreffende partij een teruggave initiëren en worden alle relevante activa geretourneerd.
Wat is het volgende? Aphelion begint nog maar net op de NEO-blockchain. De ultieme visie is een gedecentraliseerde knooppuntgebaseerde (nodegebaseerde) brug die gemeenschappen verbindt over diverse blockchains. Aphelion begint op NEO voor de intrinsieke waarde van die blockchain en probeert zijn protocol te verbreden naar ETH, BTC en andere toekomstige blockchains. Wat het uiteindelijke doel en nut is van het token: complete blockchain agnostische, directe, P2P, cross-dimensionale, gedecentraliseerde handelsplatvorm, en het ultieme van de mogelijkheden van blockchain volledig benutten. Door een brug te slaan en zo een volwaardig en echt gedecentraliseerde DApp te worden wat de kracht is en het nut van de DApp- en Aphelion-tokenprotocol; *"The whole will exceed the sum of its parts."*

3.7 Aphelion Initial Coin Offering
Aphelion ICO. Vroege investeerders, adviseurs en oprichters zijn tokens toegewezen. De ICO is gepland op 15 november 2017. Stortingen kunnen direct bij Aphelion.org worden gedaan met NEO, BTC en ETH.

Token verdeling

- 45% Verkocht ICO
- 5% incentive-programma
- 5% Pre-ICO-bijdragers
- 15% adviseurs
- 30% organisatie

3.8 Prijsstructuur en tijdlijn
Aphelion ICO Token-prijs is $ 0,20. De wisselkoers van de NEO wordt op 13 november 2017 bepaald op basis van een voortschrijdend gemiddelde van 3 dagen. Het voortschrijdend gemiddelde wordt bepaald met behulp van de SMA-methode afgeleid van coinmarketcap.com historische gegevens.
Fase één begint in het eerste blok van 15 november 2017
De ICO Eindigt op het laatste blok van 7 december 2017
De volledige 50M ICO-tokenallocatie is beschikbaar voor elke ronde. Het is mogelijk dat alle ICO-tokens worden verkocht in ronde 1.
Alle tokens die aan het einde van ronde 3 niet zijn verkocht, worden vernietigd.
Voorbeeldwisselkoers bij $ 30 NEO:
Ronde 1: 1 NEO = 150 APH + 75 APH [225 APH totaal]
Ronde 2: 1 NEO = 150 APH + 38 APH [188 APH totaal]
Geen bonus: 1 NEO = 150 APH

Gebruik van de opgehaalde inkomsten van de ICO:

65% Blockchain & DApp-ontwikkeling
10% Marketing
15% Operatie (kosten onderhoud)
10% R&D

3.9 Aphelion Smart Contract Moratorium
Om het project te beheren en de ICO-deelnemers te beschermen, is er een verplicht moratorium van 6 maanden op de verkoop van Aphelion-tokens voor alle oprichters en adviseurs. Dit beleid zal worden ingebouwd in het blockchain smart-contract voor totale transparantie.

4. Aphelion Team
Het Aphelion-team bestaat uit een wereldwijd netwerk van succesvolle ondernemers, experts en visionairs met een succesvol track record in blockchain-technologie, financiën, economie, marketing, beveiliging, software-ontwikkeling.

5. Conclusie
Aphelion bouwt een nieuwe generatie, gebaseerd op cryptotoken en blockchain gebouwd mechanisme om de uitdagingen op te lossen die te maken hebben met gecentraliseerde cryptovaluta-uitwisselingen en handelsplatformen. Dit protocol maakt een echt peer-to-peer smartcontract mogelijk, een Distributed Exchange Asset Ledger (DEAL). Een Aphelion DEAL is een niewe generatie van DApp's, gebouwd op de NEO-blockchain die open source is, beschikbaar is in diverse programmeertalen, direct doorschakelt en DEAL-makers vrijwaart van: regels, latency en beveiligingsinbreuken. Doe mee met onze missie om een op samenwerking gebaseerde, open source P2P-blockchaintechnologie te ontwikkelen die ten slotte de asset-distributie decentraliseert en blockchain naar de toekomst brengt.

6. Referenties
[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system (2008) https://bitcoin.org/bitcoin.pdf
[2] Don & Alex Tapscott, authors Blockchain Revolution (2016)
[3] Rob Marvin, Blockchain: The Invisible Technology That's Changing the World (2017)
[4] JP Buntinx, Distributed Ledger Technology Vs Blockchain Technology (March 25, 2017) https://themerkle.com/distributed-ledger-technology-vs-blockchain-technology/
[5] Blockchain project Antshares explains reasons for choosing dBFT over PoW and PoS (July 17, 2017) https://www.econotimes.com/Blockchain-project-Antshares-explains-reasons-for-choosing-dBFT-over-PoW-and-PoS-659275
[6] Daan Pepijn, Here's how NEO plans to top Ethereum and Bitcoin (August 11, 2017) https://thenextweb.com/contributors/2017/08/17/heres-neo-plans-top-ethereum-bitcoin/
[7] Christopher Malmo, Ethereum Is Already Using a Small Country's Worth of Electricity (June 26, 2017)https://motherboard.vice.com/en_us/article/d3zn9a/ethereum-mining-transaction-electricity-consumption-bitcoin
[8] Haseeb Qureshi, A hacker stole $31M of Ether (July 20, 2017) https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce
[9] Dr Garrick Hileman & Michel Rauchs, Global Cryptocurrency Benchmarking Study, The Cambridge Centre for Alternative Finance (2017) https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf
[10] Jamie Redman, Another All Time High – Bitcoin Breaks Through 5,000 USD on Asian Exchanges (September 2, 2017) https://news.bitcoin.com/bitcoin-hits-5000-usd-new-all-time-high/
[11] Andrew Marshall, P2P Cryptocurrency Exchanges, Explained (APR 07, 2017) https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained
[12] Peter Todd, The ripple protocol consensus algorithm Review. Ripple Labs Inc White Paper (May, 2015) https://raw.githubusercontent.com/petertodd/ripple-consensus-analysis-paper/master/paper.pdf

[13] Shapeshift Reviews http://bittrust.org/shapeshift
[14] Loopring Project Ltd., LOOPRING Decentralized Token Exchange Protocol (Sept 26, 2017) https://github.com/Loopring/whitepaper/raw/master/en_whitepaper.pdf
[15] Fabian Schuh and Daniel Larimer. Bitshares 2.0: Financial smart contract platform (Nov 12, 2015) http://docs.bitshares.org/_downloads/bitshares-financial-platform.pdf
[16] Fabian Schuh and Daniel Larimer. Bitshares 2.0: General overview (2015) http://docs.bitshares.org/_downloads/bitshares-general.pdf
[17] Open ledger (2017) https://openledger.io/
[18] Eyal Hertzog, Guy Benartzi & Galia Benartzi, Bancor Protocol Continuous Liquidity and Asynchronous Price Discovery for Tokens through their Smart Contracts; aka “Smart Tokens” (March 30, 2017) https://www.bancor.network/static/bancor_protocol_whitepaper_en.pdf
[19] Amir Bandeali. Introducing 0x -An Open Protocol For Decentralized Exchange On The Ethereum Blockchain (February 22, 2017) https://blog.0xproject.com/introducing-0x-d51d5231ba53
[20] Binance GAS(was Antcoin), (July 2017) https://binance.zendesk.com/hc/en-us/articles/115000967291-GAS-was-Antcoin-

7. Bijlage - Aphelion DApp Pseudo-Code Algoritme

Parties
• {COIN_A} holder
• {COIN_B} holder
Process
• The 'superconducting transaction' (also 'on-chain atomic swap') proceeds through two transactions, one on the {COIN_A} blockchain, the other on the {COIN_B} blockchain.
◦ [1]:{COIN_A} holder has an unspent amount, A, of {COIN_A} in an address recorded in a transaction on the {COIN_A} blockchain.
{COIN_A} holder will pay this unspent amount into a {COIN_A} address controlled by {COIN_B} holder through a transaction on the {COIN_A} blockchain.
◦ [2]:{COIN_B} holder has an unspent amount, B, of {COIN_B} in an address recorded in a transaction on the {COIN_B} blockchain.
{COIN_B} holder will pay this unspent amount into a {COIN_B} address controlled by {COIN_A} holder through a transaction on the {COIN_B} blockchain.
Steps
◦ {COIN_A} holder 'initiates'.
▪ Obtains following information from {COIN_B} holder:
• {COIN_B} holder's address on {COIN_A} blockchain, into which {COIN_A} payment will be made.
▪ Creates and publishes contract transaction on {COIN_A} blockchain, with a locktime set by the seller sometime in the future (user set expiry date/time).
▪ This step returns the secret, the secret hash, the contract script, the contract transaction, and a refund transaction that can be sent after (user set expiry date/time) if necessary.

◦ {COIN_B} holder 'audits contract'.
▪ Obtains following information from {COIN_A} holder:
• Swap-script, the output script that may be redeemed on the {COIN_A} blockchain by one of two signature scripts.
• Trans, superconducting transaction for {COIN_A} blockchain.
▪ Inspects {COIN_A} blockchain superconducting transaction contract script to review addresses that may claim the output, the locktime, and the secret hash. Also validates that contract transaction pays to the contract and reports the contract output amount.

◦ {COIN_B} holder 'participates'.
▪ Obtains following information from {COIN_A} holder:

• {COIN_A} holder's address on {COIN_B} blockchain, into which {COIN_B} payment will be made.
• Secret-hash, the hash of the secret key for the {COIN_A} blockchain contract transaction.
▪ Creates and publishes contract transaction on {COIN_B} blockchain, incorporating also the secret hash from the {COIN_A} blockchain contract transaction 'initiated', above, and with a locktime of (user set expiry date/time).
▪ This step returns the the contract script, the contract transaction, and a refund transaction that can be sent after (user set expiry date/time) if necessary.

◦ {COIN_A} holder 'audits contract'.
▪ Obtains following information from {COIN_B} holder:
• Swap-script, the output script that may be redeemed on the {COIN_B} blockchain by one of two signature scripts.
• Trans, superconducting transaction for {COIN_B} blockchain.
▪ Inspects {COIN_B} blockchain superconducting transaction contract script to review addresses that may claim the output, the locktime, and the secret hash. Also validates that contract transaction pays to the contract and reports the contract output amount.

◦ {COIN_A} holder 'redeems'.
▪ Will already have obtained (see prior step) the following information from {COIN_B} holder:
• Swap-script, the output script that may be redeemed on the {COIN_B} blockchain by either of two signature scripts.
• Trans, the superconducting transaction for the {COIN_B} blockchain.
▪ Redeems {COIN_B} coins paid into the contract in {COIN_B} blockchain by {COIN_B} holder. Redeeming requires the secret, known only to the {COIN_A} holder up to this point.

◦ {COIN_B} holder 'extracts secret'.
▪ Extracts secret from {COIN_A} holder's redemption transaction. With the secret known, the {COIN_B} holder may claim the {COIN_A} coins paid into the contract in the {COIN_A} blockchain by {COIN_A} holder.

◦ {COIN_B} holder 'redeems'.
▪ Will already have obtained (see 'audit contract' step) the following information from {COIN_A} holder:
• Swap-script, the output script that may be redeemed on the {COIN_A} blockchain by either of two signature scripts.
• Trans, the superconducting transaction for the {COIN_A} blockchain.
▪ Redeems {COIN_A} coins paid into the contract in {COIN_A} blockchain by {COIN_A} holder.

Refunds
◦ If a period of time equal to the time-lock (i.e. (user set expiry date/time), in the case of the {COIN_A} blockchain superconducting transaction, and (user set expiry date/time), in the {COIN_B} case) expires after the transaction has been mined but has not been redeemed, the contract output can be redeemed back to the holder's wallet.

Pseudo-code
'initiate', by {COIN_A} holder
{COIN_A} holder runs:
$ 'initiate', with parameters
– [{COIN_A} blockchain, i.e. the blockchain on which {COIN_A} holder's payment will be made]
– [string representing {COIN_B} holder's address on {COIN_A} blockchain, into which {COIN_A} payment will be made]

– [string representing A, amount of {COIN_A} to be paid to this address]
{
Decode parameter [string representing {COIN_B} holder's address on {COIN_A} blockchain, into which {COIN_A} payment will be made]. If it conforms with a valid address for the {COIN_A} blockchain, return this address, their-address.
Decode [string representing A, amount of {COIN_A} to be paid to this address]. If it conforms to a valid double-precision floating-point number (i.e. binary64), and is not NaN or +/- infinity, return this number, amount.
Open JSON-RPC connection with the {COIN_A} blockchain.
Generate [secret], a new secret key for the {COIN_A} blockchain.
Calculate [secret-hash], the hash of [secret].
Calculate [lock-time], a locktime (user set expiry date/time) from current time.
Calculate [refund-address], a {COIN_A} address for the refund transaction.

Build the superconducting contract on the {COIN_A} blockchain, with parameters:
– [their-address]
– [lock-time]
– [secret-hash]
– [refund-address]
Return [swap-script], the output script that may be redeemed on the {COIN_A} blockchain by one of two signature scripts:
– [{COIN_B} holder's sig] [{COIN_B} holder's pub key] [{COIN_A} holder's secret], or
– [{COIN_A} holder's sig] [{COIN_A} holder's pub key]
Calculate [swap-address-script-hash], a new address script hash of [swap-script].
Calculate [tx-script], a new script to pay the transaction output to [swap-address-script-hash].
Calculate [fee], the fees associated with the transaction.
Calculate [trans], superconducting transaction for {COIN_A} blockchain, with parameters:
– [A, amount]
– [tx-script]
– [refund-address]
– [fee]
– [lock-time]
Sign [trans].
Calculate:
– [refund trans], the refund transaction
– [refund fee], the fee associated with the refund transaction.

Return and Display:
– [secret]
– [secret-hash]
– [swap-script]
– [trans]
– [refund-trans]
– [lock-time]
Publish transaction.
}

'audit contract', by {COIN_B} holder
{COIN_B} holder runs:
$ 'auditcontract', with parameters
– [{COIN_B} blockchain, i.e. the blockchain on which {COIN_B} holder's payment will be made]

– [string representing swap-script, output script that may be redeemed on the {COIN_A} blockchain by one of two signature scripts]
– [string
representing trans, superconducting transaction for {COIN_A} blockchain]
{
Decode parameter [string representing swap-script, output script that may be redeemed on the {COIN_A} blockchain by one of two signature scripts]. If it conforms to a valid hexadecimal string of the right length, return the bytes, swap-script.
Decode parameter [string representing trans, superconducting transaction for {COIN_A} blockchain]. If it conforms to a valid hexadecimal string of the right length, return the bytes, swap-script.

Open JSON-RPC connection with the {COIN_A} blockchain.

Calculate superconducting transaction data pushes, with parameters:
– [swap-script], the output script that may be redeemed on the {COIN_B} blockchain by either of two signature scripts
Return
– [address], {COIN_B} holder's address on {COIN_A} blockchain, into which {COIN_A} payment will be made
– [secret-hash], the hash of the secret key for the {COIN_A} blockchain contract transaction
– [lock-time]
Calculate pay to address, with parameters:
- [trans], the superconducting transaction for the {COIN_A} blockchain

Return
– [PubKeyTx], address on {COIN_A} blockchain into which {COIN_A} holder will make payment

Display
– [swap-script-hash], address on {COIN_A} blockchain of superconducting contract
– [amount], value of {COIN_A} to be paid into {COIN_B} holder's address on {COIN_A} blockchain
– [address], {COIN_B} holder's address on {COIN_A} blockchain, into which {COIN_A} will be paid
– [refund-address], {COIN_A} holder's address on {COIN_A} blockchain for payment of refund of {COIN_A}
– [lock-time]
}

'participate', by {COIN_B} holder
{COIN_B} holder runs:
$ 'participate', with parameters
– [{COIN_B} blockchain, i.e. the blockchain on which {COIN_B} holder's payment will be made]
– [string representing {COIN_A} holder's address on {COIN_B} blockchain, into which {COIN_B} payment will be made]
– [string representing B, amount of {COIN_B} to be paid to this address]
– [string representing secret-hash, the hash of the secret key for the {COIN_A} blockchain contract transaction]
{
Decode parameter [string representing {COIN_A} holder's address on {COIN_B} blockchain, into which {COIN_B} payment will be made] . If it conforms with a valid address for the {COIN_B} blockchain, return this address, their-address.

Decode [string representing B, amount of {COIN_B} to be paid to this address]. If it conforms to a valid double-precision floating-point number (i.e. binary64), and is not NaN or +/- infinity, return this number, amount.
Decode [string representing secret-hash, the hash of the new secret key for the {COIN_A} blockchain contract transaction]. If it conforms to a valid hexadecimal string of the right length, return the bytes, their-secret-hash.
Open JSON-RPC connection with the {COIN_B} blockchain.
Calculate [lock-time], a locktime (user set expiry date/time) from current time.
Calculate [refund-address], a {COIN_B} address for the refund transaction.
Build the superconducting contract on the {COIN_B} blockchain, with parameters:
– [their-address]
– [lock-time]
– [their-secret-hash]
– [refund-address]
Return [swap-script], the output script that may be redeemed on the {COIN_B} blockchain by one of two signature scripts:
– [{COIN_A} holder's sig] [{COIN_A} holder's pub key] [{COIN_A} holder's secret], or
– [{COIN_B} holder's sig] [{COIN_B} holder's pub key]
Calculate [swap-address-script-hash], a new address script hash of [swap-script].
Calculate [tx-script], a new script to pay the transaction output to [swap-address-script-hash].
Calculate [fee], the fees associated with the transaction.
Calculate [trans], superconducting transaction for {COIN_B} blockchain, with parameters:
– [B, amount]
– [tx-script]
– [refund-address]
– [fee]
– [lock-time]
Sign [trans].

Calculate: – [refund trans], the refund transaction
– [refund fee], the fee associated with the refund transaction.

Return and Display:
– [secret]
– [secret-hash]
– [swap-script]
– [trans]
– [refund-trans]
– [lock-time]

Publish transaction.
}

'audit contract', by {COIN_A} holder
{COIN_A} holder runs:
$ 'auditcontract', with parameters
– [{COIN_B} blockchain, i.e. the blockchain on which {COIN_B} holder's payment will be made]
– [string representing swap-script, output script that may be redeemed on the {COIN_B} blockchain by one of two signature scripts]
– [string representing trans, superconducting transaction for {COIN_B} blockchain]
{

Decode parameter [string representing swap-script, output script that may be redeemed on the {COIN_B} blockchain by one of two signature scripts]. If it conforms to a valid hexadecimal string of the right length, return the bytes, swap-script.
Decode parameter [string representing trans, superconducting transaction for {COIN_B} blockchain]. If it conforms to a valid hexadecimal string of the right length, return the bytes, swap-script.
Open JSON-RPC connection with the {COIN_B} blockchain.
Calculate superconducting transaction data pushes, with parameters:
– [swap-script], the output script that may be redeemed on the {COIN_B} blockchain by either of two signature scripts

Return
– [address], {COIN_A} holder's address on {COIN_B} blockchain, into which {COIN_B} payment will be made
– [secret-hash], the hash of the secret key for the {COIN_B} blockchain contract transaction
– [lock-time]

Calculate pay to address, with parameters:
- [trans], the superconducting transaction for the {COIN_B} blockchain
Return
– [PubKeyTy], address on {COIN_B} blockchain into which {COIN_B} holder will make payment

Display
– [swap-script], address on {COIN_B} blockchain of superconducting contract
– [amount], value of {COIN_B} to be paid into {COIN_A} holder's address on {COIN_B} blockchain
– [address], {COIN_A} holder's address on {COIN_B} blockchain, into which {COIN_B} will be paid
– [refund-address], {COIN_B} holder's address on {COIN_B} blockchain for payment of refund of {COIN_B}
– [lock-time]
}

'redeem', by {COIN_A} holder
{COIN_A} holder runs:
$ 'redeem', with parameters
– [{COIN_B} blockchain, i.e. the blockchain on which {COIN_B} holder's payment will be made]
– [string representing swap-script, the output script that may be redeemed on the {COIN_B} blockchain by either of two signature scripts:
– [{COIN_A} holder's sig] [{COIN_A} holder's pub key] [{COIN_A} holder's secret], or
– [{COIN_B} holder's sig] [{COIN_B} holder's pub key]]
– [string representing trans, the superconducting transaction for the {COIN_B} blockchain]
– [string representing secret, the secret key for the {COIN_A} blockchain]
{
Decode parameter [string representing swap-script, the output script that may be redeemed on the {COIN_B} blockchain by either of two signature scripts]. If it conforms to a valid hexadecimal string of the right length, return the bytes, swap-script.
Decode [string representing trans, the superconducting transaction for the {COIN_B} blockchain]. If it conforms to a valid hexadecimal string of the right length, return the bytes, trans.
Decode [string representing secret, the secret key for the {COIN_A} blockchain]. If it conforms to a valid hexadecimal string of the right length, return the bytes, secret.
Open JSON-RPC connection with the {COIN_B} blockchain.
Calculate superconducting transaction data pushes, with parameters:
– [swap-script], the output script that may be redeemed on the {COIN_B} blockchain by either of two signature scripts

Return
– [address], {COIN_A} holder's address on {COIN_B} blockchain, into which {COIN_B} payment will be made
– [secret-hash], the hash of the secret key for the {COIN_A} blockchain contract transaction
Calculate pay to address, with parameters:
- [trans], the superconducting transaction for the {COIN_B} blockchain

Return
– [PubKeyTy], address on {COIN_B} blockchain into which {COIN_B} holder will make payment
Verify [address] and [PubKeyTy] are equal.
Calculate [pay-script], script to pay a transaction output to [PubKeyTy].
Create [redeemTx], redeem transaction.
Sign [redeemTx].
Publish [redeemTx]
}

'extract secret', by {COIN_B} holder
{COIN_B} holder runs:
$ 'extractsecret', with parameters:
– [string representing redeemTx, the redeem transaction published by {COIN_A} holder on the {COIN_B} blockchain]
– [string representing secret-hash, the hash of the secret key for the {COIN_A} blockchain contract transaction]
{
Decode [string representing redeemTx, the redeem transaction published by {COIN_A} holder on the {COIN_B} blockchain]. If it conforms to a valid hexadecimal string of the right length, return the bytes, redeemTx.
Decode [string representing secret-hash, the hash of the new secret key for the {COIN_A} blockchain contract transaction]. If it conforms to a valid hexadecimal string of the right length, return the bytes, their-secret-hash.
Open JSON-RPC connection with the {COIN_B} blockchain.
Loop over all pushed data, searching for one that hashes to the expected hash. Return [secret].
Display [secret].
}

'redeem', by {COIN_B} holder
{COIN_B} holder runs:
$ 'redeem', with parameters
– [{COIN_A} blockchain, i.e. the blockchain on which {COIN_A} holder's payment will be made]
– [string representing swap-script, the output script that may be redeemed on the {COIN_A} blockchain by either of two signature scripts:
– [{COIN_B} holder's sig] [{COIN_B} holder's pub key] [{COIN_A} holder's secret], or
– [{COIN_A} holder's sig] [{COIN_A} holder's pub key]]
– [string representing trans, the superconducting transaction for the {COIN_Aa} blockchain]
– [string representing secret, the secret key for the {COIN_A} blockchain]
{
Decode parameter [string representing swap-script, the output script that may be redeemed on the {COIN_A} blockchain by either of two signature scripts]. If it conforms to a valid hexadecimal string of the right length, return the bytes, swap-script.

Decode [string representing trans, the superconducting transaction for the {COIN_A} blockchain]. If it conforms to a valid hexadecimal string of the right length, return the bytes, trans.
Decode [string representing secret, the secret key for the {COIN_A} blockchain]. If it conforms to a valid hexadecimal string of the right length, return the bytes, secret.
Open JSON-RPC connection with the {COIN_A} blockchain.
Calculate superconducting transaction data pushes, with parameters:
– [swap-script], the output script that may be redeemed on the {COIN_A} blockchain by either of two signature scripts

Return
– [address], {COIN_B} holder's address on {COIN_A} blockchain, into which {COIN_A} payment will be made
– [secret-hash], the hash of the secret key for the {COIN_A} blockchain contract transaction
Calculate pay to address, with parameters:
- [trans], the superconducting transaction for the {COIN_A} blockchain

Return
– [PubKeyTy], address on {COIN_A} blockchain into which {COIN_A} holder will make payment
Verify [address] and [PubKeyTy] are equal.
Calculate [pay-script], script to pay a transaction output to [PubKeyTy].
Create [redeemTx], redeem transaction.
Sign [redeemTx].
Publish [redeemTx]
}

'refund', by either holder
Either holder runs:
$ 'refund', with parameters
– [B, blockchain, i.e. the blockchain on which refund will be made]
– [string representing swap-script, for the superconducting transaction to be refunded]
– [string representing trans, the superconducting transaction to be refunded]
{
Decode [string representing swap-script, for the superconducting transaction to be refunded]. If it conforms to a valid hexadecimal string of the right length, return the bytes, redeemTx.
Decode [string representing swap-script, for the superconducting transaction to be refunded]. If it conforms to a valid hexadecimal string of the right length, return the bytes, their-secret-hash.
Open JSON-RPC connection with the blockchain, B.
Calculate superconducting transaction data pushes, with parameters:
– [swap-script], the output script that may be redeemed on the {COIN_A} blockchain by either of two signature scripts
Return
– [amount], value to be refunded on blockchain, B
– [fees], fees associated with the transaction
– [refund-address], the address on blockchain, B, into which refund will be made
Calculate [pay-script], script to pay a transaction output to [refund-address].
Create [refundTx], refund transaction.
Sign [refundx].
Publish [refundTx]
}