SafeHaven.io

… Maakt digitale bezittingen erfelijk…

Brussel, december 2017

www.safehaven.io

Geschreven door het Safe Haven Team

Index

Index van afbeeldingen

Voorwoord

Dit document is bedoeld om inzicht te scheppen in wat Safehaven.io inhoudt en wat Safe Haven kan betekenen voor u. Dit is een technisch document die de huidige en toekomstige ontwikkelingen van het Safe Havenproject omschrijven. Dit document is alleen voor informatiedoeleinden en is geen verklaring voor de toekomst. Tenzij uitdrukkelijk anders vermeld, de producten en innovaties zijn in dit document momenteel in ontwikkeling en worden momenteel niet geïmplementeerd. We geven geen garanties met betrekking tot de succesvolle ontwikkeling van dergelijke technologieën en innovaties en wijzen alle garanties af voor zover wettelijk toegestaan. Niemand heeft het recht om te vertrouwen op de inhoud van dit document of enige gevolgtrekking hieruit. Safe Haven wijst alle aansprakelijkheid af voor verlies of welke schade dan ook die hieruit kan voortvloeien.
Vele termen zijn in het Engels beschreven alsook de schetsen en dit om de verwoording niet te bemoeilijken.

1 Inleiding

Weinig mensen weten het, maar crypto-valuta's kwamen naar voren als bijproduct van een andere uitvinding. Satoshi Nakamoto, de onbekende uitvinder van Bitcoin, de eerste en nog steeds belangrijkste crypto-valuta, was nooit van plan een valuta uit te vinden.
In zijn aankondiging van Bitcoin eind 2008, zei Satoshi dat hij een "peer-to-peer elektronisch cash-systeem" heeft ontwikkeld. “
Zijn doel was om iets te verzinnen; veel mensen konden geen digitaal geld creëren. Het belangrijkste aspect van Satoshi ‘s uitvinding was dat hij een manier vond om een gedecentraliseerd digitaal geldsysteem te creëren. In de jaren negentig zijn er veel pogingen geweest om digitaal geld te creëren, maar ze faalden allemaal. Nadat alle gecentraliseerde pogingen faalden, probeerde Satoshi een digitaal geldsysteem te bouwen zonder een centrale entiteit. Als een peer-to-peer-netwerk voor het delen van bestanden.
Deze beslissing werd de geboorte van crypto-valuta. Ze zijn het ontbrekende deel dat Satoshi digitaal contant geld heeft laten realiseren. De reden waarom is een beetje technisch en complex, maar als je het begrijpt, weet je meer over crypto-valuta's dan de meeste mensen. Laten we het zo gemakkelijk mogelijk houden: ·Voor het realiseren van digitaal contant geld heeft u een betalingsnetwerk nodig met rekeningen, saldo en transacties. Dat is gemakkelijk te begrijpen. Een groot probleem dat elk betaalnetwerk moet oplossen, is het voorkomen van de zogenaamde dubbele uitgaven: voorkomen dat diezelfde entiteit hetzelfde bedrag tweemaal uitgeeft. Meestal gebeurt dit door een centrale server die de balans bewaart.
In een gedecentraliseerd netwerk hebt u deze server niet. U hebt dus elke afzonderlijke entiteit van het netwerk nodig om deze taak uit te voeren. Elke peer in het netwerk moet een lijst met alle transacties hebben om te controleren of toekomstige transacties geldig zijn of een poging om de uitgaven te verdubbelen.
Maar hoe kunnen deze entiteiten een consensus over deze archieven behouden?
Als de peers van het netwerk het niet eens zijn over slechts één enkele, kleine balans, is alles verbroken. Ze hebben een absolute consensus nodig. Meestal neem je opnieuw een centrale autoriteit om de juiste balans te verklaren. Maar hoe kun je consensus bereiken zonder een centrale autoriteit?
Niemand wist het totdat Satoshi uit het niets opdook. Niemand geloofde zelfs dat het mogelijk was.
Satoshi bewees dat het zo was. Zijn belangrijkste innovatie was om consensus te bereiken zonder een centrale autoriteit. Crypto-valuta's maken deel uit van deze oplossing - het deel dat de oplossing opwindend, fascinerend en hielp om over de wereld te rollen.

1 bedenkingen

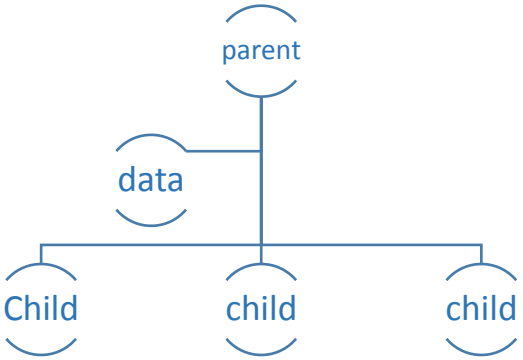
Heb je ooit gedacht aan de dag dat er iets met je zou kunnen gebeuren of heb je al nagedacht over de dag dat je sterft? Heb je ooit gedacht aan de dag dat je familie het leven zonder jou tegemoet moet treden? Hoe zit het met uw crypto-valuta investeringen? Hoe zit het met die moeilijke markten met honderden privésleutels, uitwisselingen en portefeuilles? Zullen ze die investering ooit zonder jou kunnen terugkrijgen? Konden ze iemand vertrouwen die hen zou helpen zonder de angst, dat er iets misgaat? Ja, dat kunnen ze! Safe Haven biedt de oplossing! We bouwen een platform / Ecosysteem voor de populairste en veiligste blokkeerketens, zodat je je geen zorgen meer hoeft te maken over je nalatenschap

2 Oplossingen

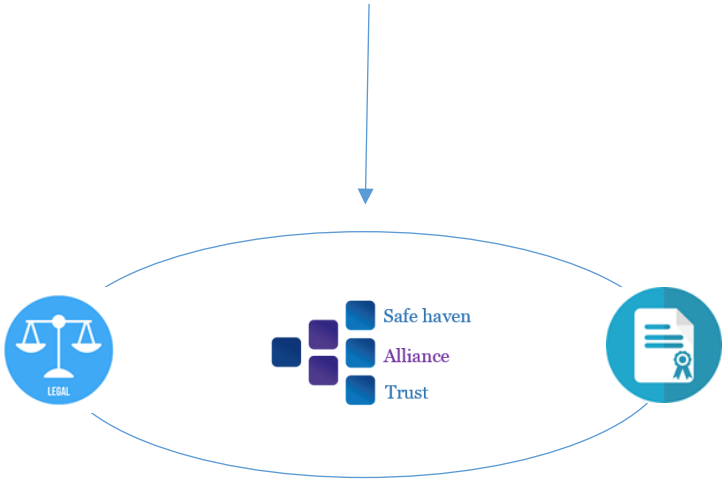
Om uw digitale bezittingen te beschermen, bieden wij u bij Safe Haven de mogelijkheid om dit te doen zonder uzelf te blokkeren, dankzij ons TFC Share Distribution Key Escrow Protocol en het Trust Alliance-programma, kunnen privésleutels / wachtzinnen worden gedeeld onder belanghebbenden of kinderen op een transparante en veilige manier.
Ons protocol verdeelt de aandelen op een dergelijke manier dat de initiatiefnemer ten koste van alles de macht over zijn vermogen behoudt. De ongelukkige dag dat hij / zij zou moeten overlijden, kan een geregistreerd lid van het Trust Alliance Platform (notaris) zijn resterende aandeel in het blockchain ophalen om zijn erfenis over te dragen aan zijn kinderen / belanghebbenden.
Hoe bereiken we dat? Bekijk de stapsgewijze handleiding, die slechts 3 stappen omvat, en de gebruikte technieken die verderop in dit document worden beschreven.

2.1 Stap voor stap

Stap 1: De gebruiker besluit zijn nalatenschap te beschermen (crypto-assets) en is van plan zijn zaden / privésleutels of wachtzinnen te verspreiden met behulp van beveiligde veilige en transparante blockchain-oplossing onder zijn drie kinderen. De initiatiefnemer van het proces gaat naar een geregistreerd lid van ons Trust Alliance-programma, dit is een groep van rechtspersonen die een betrouwbare relatie hebben met Safe Haven om de noodzakelijke valideringsstappen te verwerken.

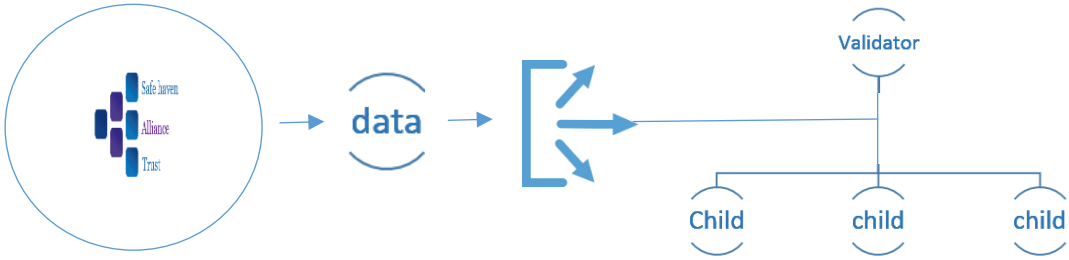


Afbeelding 1 : The Family Circle (TFC)



Afbeelding 2 : The trust Alliance Representation

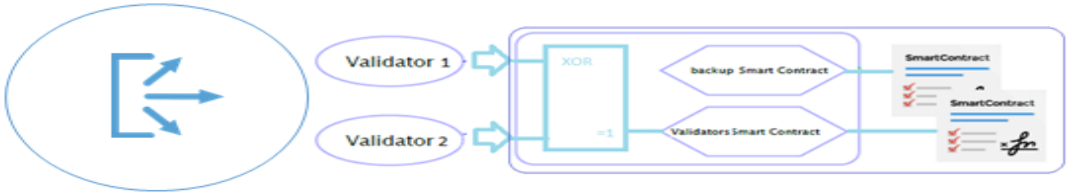
Stap 2: De juridische entiteit, die zich in veilige havens bevindt, protocolleert de validator, verdeelt de gegevens om de verkregen aandelen te beschermen en te distribueren (zie TFC shares distributie Protocol) door gebruik te maken van de safe havens-applicatie die speciaal voor dat gebruik is ontwikkeld. De software die hiervoor wordt gebruikt, bewaard geen gegevens in het geheugen, noch in lokale noch in gecentraliseerde databases. Alleen de validators delen (zie het proces voor het delen van validators.) Worden naar de blockchain gestuurd. Het beveiligingsalgoritme voor het coderen en decoderen van de share voordat deze wordt geïmplementeerd via een slim contract, wordt om evidente beveiligingsredenen niet bekendgemaakt. Safe Haven zal alleen een soort van mapping hebben om de validators ID en het Smart contract te identificeren, de mapping zal worden geïmplementeerd op een gedecentraliseerde blockchain-database. Dit zal ook het geval zijn voor de back-up validators (zie Multiple Validators Possibility & TFC Fail-Safe Share (s)).



Afbeelding 3 : split in shares step

Stap 3: De aandelen die aan de kinderen worden uitgedeeld, worden door de notaris getemperd in de vorm van een wettelijk certificaat. Het te beveiligen deel, afkomstig van de ouder / initiator, zal worden gecodeerd door de Safe Haven-applicatie (alleen toegankelijk voor leden van de Trust Alliance) en worden verzonden naar de blockchain in de vorm van een Smart-contract.

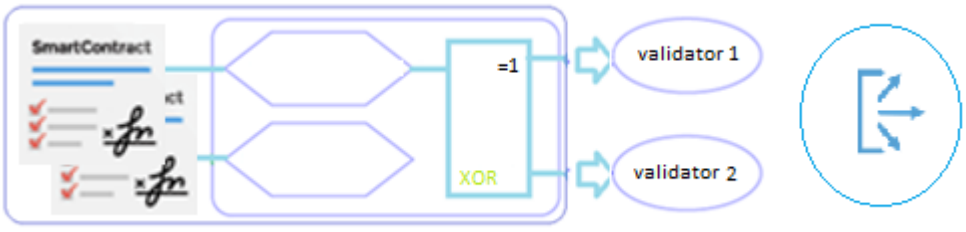
Afbeelding 4 : Child certificates



Afbeelding 5 : Validators process

De onderliggende aandelen kunnen worden gedeeld via het maken van een certificaat en / of via de integratie van een hardware-grootboek in ons protocol. We werken momenteel aan het uitwerken van de details om dit te bereiken, op basis van onze eigen hardware-grootboeken. Details worden nog niet openbaar gemaakt, omdat we nog steeds in de ICO-fase van ons project zitten.

Stap 4: In het geval van een plotseling overlijden of in het geval dat de initiatiefnemer niet in staat is om zijn bezittingen alleen te verwerken, kunnen de kinderen of belanghebbenden het ontbrekende aandeel verkrijgen door de nodige wettelijke documenten aan zijn notaris voor te leggen. Hij zal dan, eenmaal geverifieerd door Safe Haven, in staat zijn om het ontbrekende deel uit de blockchain te halen.
Ons protocol handelt een fail-safe share af en de mogelijkheid om een back-up validator te hebben, voor meer informatie bekijk je onze TFC Fail-Safe Share (s) & Multiple Validators-secties die verderop in dit document worden beschreven.



Afbeelding 6 : share Retrieval process

3 Basis Principes

3.1 Blockchain

De Blockchain is een software-innovatie om digitale vertrouwensrelaties tussen gebruikers tot stand te brengen
Vergemakkelijken van transacties van waarde, via een netwerk. De blockchain maakt het mogelijk dat vertrouwen wordt verspreid over een netwerk, zonder dat een centrale tussenpersoon nodig is om de digitale uitwisseling van waarde te volgen, te verifiëren en goed te keuren. Het idee om vertrouwen van een centrale tussenpersoon toe te staan, ondersteunt momenteel zowel institutionele als institutionele structuren, maar dit blijkt kostbaar, traag en ook kwetsbaar voor aanvallen te zijn. De blockchain overwint deze problemen door te werken als een gedecentraliseerde gedistribueerde database, met behoud van een voortdurend groeiende lijst met records die blokken worden

3.2 Smart contract

Computercode op de ketting of slimme contracten zijn computerprotocollen die de uitvoering van een contract vergemakkelijken, controleren of afdwingen waardoor een contractuele clausule overbodig wordt. Slimme contracten emuleren vaak de logica van contractuele clausules. Slimme contracten kunnen op transparante, conflictvrije wijze geld, bezittingen, aandelen of iets van waarde uitwisselen, terwijl de diensten van een tussenpersoon worden vermeden. Gewoonlijk vereist een proces betaling aan een tussenpersoon, overheidsinstantie, bank, advocaat of een notaris en vervolgens een verwerkingstijd vóór de ontvangst van goederen of diensten. Met slimme contracttechnologie kan dit echter allemaal worden geautomatiseerd. Slimme contracttechnologie kan worden vergeleken met die van een geautomatiseerde automaat. Met een automaat wordt geld in de automaat gestort en valt het gewenste bedrag af, op voorwaarde dat het juiste bedrag wordt gestort. Vergelijkbaar met dat, met een slim contract, wordt het geld gestort in escrow op de blokketting voor ontvangst van een overdracht van een token (bijv. Een digitaal certificaat van eigendom voor een huis), dat onmiddellijk wordt overgebracht naar de controle van een tegenpartij zodra de voorwaarden zijn leerde kennen. Slimme contracten definiëren niet alleen de voorwaarden en condities rond een overeenkomst op dezelfde manier als een traditioneel contract, maar bieden ook handhaving van die verplichtingen

4 Technische en concepionele rekenkunde

4.1 Polynomial interpolation

Polynomen kunnen worden gebruikt om gecompliceerde curven te benaderen, bijvoorbeeld de vorm van letters in de typografie die een paar punten bevat. Een relevante toepassing is de evaluatie van de natuurlijke logaritme en trigonometrische functies: kies een paar bekende gegevenspunten, maak een opzoektabel en interpoleer tussen die gegevenspunten. Dit resulteert in aanzienlijk snellere berekeningen.

Definities:

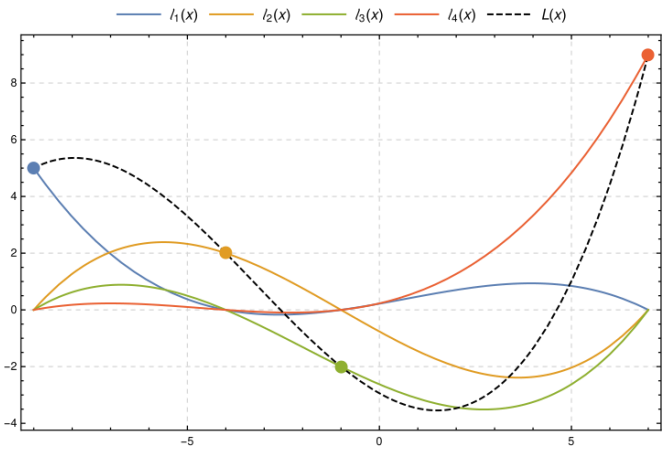
Gegeven een set van n + 1 datapunten (xi, yi) waar geen twee xi hetzelfde zijn, is men op zoek naar een polynoom p van mate hoogstens n met de eigenschap

$$p(x_i) = y_i, \qquad i = 0, \ldots, n.$$

De niet-isolatielase vermeldt dat een dergelijke polynoom p bestaat en uniek is en kan worden bewezen door de Vandermonde-matrix, zoals hieronder wordt beschreven De stelling stelt dat voor n + 1 interpolatie knooppunten (xi), polynoominterpolatie een lineaire bisection definieert

$$L_n : \mathbb{K}^{n+1} \to \Pi_n$$

Waarbij Πn vector de vectorruimte is van polynomen (gedefinieerd op elk interval dat de knopen bevat) van graad maximaal n.



Afbeelding 7 : Polynomials

Polynomiaal interpolatie vormt ook de basis voor algoritmen in numerieke kwadratuur en numerieke gewone differentiaalvergelijkingen en Secure Multi Party Computation, Secret Sharing-schema's. Geheime deelschema's zijn wat we gebruiken om ons doel te bereiken.

4.2 Key escrow

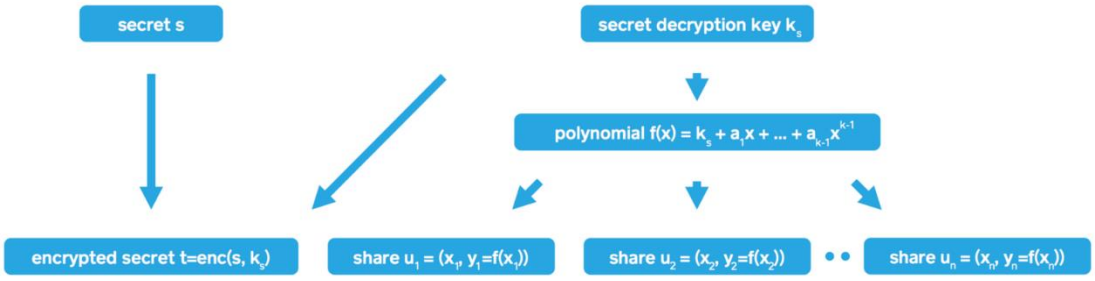
We bestaan niet eeuwig en het zou jammer zijn als we met ons de toegang tot een digitaal erfgoed zouden verliezen.

Het plotselinge verlies van een aandeelhouder kan een probleem zijn om de volledige wachtwoordzin te herstellen. In dit document zullen we het voorbeeld van een familiekring of vrienden blijven gebruiken om de verschillende scenario's te benadrukken.
Een antwoord op dit probleem is de zogenaamde 'key escrow', waarmee een derde 'onder bepaalde voorwaarden' toegang heeft tot deze aandelen. Maar welke derde, onder welke voorwaarden, en hoe moet het onze morele maar ook technische betrouwbaarheid krijgen? De escrow-autoriteit moet de vertrouwelijkheid van de escrow-sleutels veilig kunnen garanderen.
Allereerst moeten we de te beveiligen gegevens coderen, dit kan een privésleutel zijn of een zaad met een beveiligd versleutelalgoritme zoals SHA265-512 en door een wachtwoordzin te gebruiken. Deze wachtzin kan dan in aandelen worden verdeeld en worden gedistribueerd via ons TFC SD-protocol.

4.3 Secret Sharing

In cryptografie is een geheim deelschema een methode voor het verspreiden van een geheim onder een groep deelnemers, aan elk waarvan een deel van het geheim wordt toegewezen. Het geheim kan alleen worden gereconstrueerd wanneer de aandelen samen worden gecombineerd; individuele aandelen hebben op zich geen zin.
Meer formeel is er in een geheim delende schema één dealer en meer spelers. De dealer geeft een geheim aan de spelers, maar alleen als aan specifieke voorwaarden is voldaan. De dealer doet dit door elke speler een aandeel te geven op een manier dat elke groep van t (voor drempelwaarde) of meer spelers samen het geheim kunnen reconstrueren, maar geen groep van minder dan t-spelers kan. Zo'n systeem wordt een (t, n) -drempelschema genoemd.

in een (t, n) schema kan men bewijzen dat het geen verschil maakt of een aanvaller t-1 geldige aandelen tot zijn beschikking heeft of helemaal niet; zolang hij minder dan t-aandelen heeft, is er geen betere optie dan te raden om het geheim te achterhalen.
Sommigen gebruiken gevallen van geheim delen: (Zie SHA-beschermingsplannen)
• Goede wachtwoorden zijn moeilijk te onthouden. Een slimme gebruiker zou een geheim delen-schema kunnen gebruiken om een reeks aandelen voor een bepaald wachtwoord te genereren en één aandeel in zijn adresboek op te slaan, één in zijn bankstortkluis, één aandeel achter te laten bij een vriend, enz. Als hij op een dag zijn zijn boek vergeet wachtwoord, hij kan het gemakkelijk reconstrueren. Natuurlijk zou het schrijven van wachtwoorden rechtstreeks in het adresboek een veiligheidsrisico vormen, omdat het door een "vijand" zou kunnen worden gestolen. Als een geheim gedeeld schema wordt gebruikt, moet de aanvaller veel aandelen stelen van verschillende plaatsen.
Een typische toepassing van dit scenario is de veilige implementatie van een gecodeerd back-upsysteem. Ervan uitgaande dat gegevensherstel zelden nodig is, kunnen back-upgegevens openbaar gecodeerd worden gecodeerd - dit kan automatisch en zonder gebruikersinteractie gebeuren - terwijl de privé-herstelsleutel beveiligd is via geheim delen.
• "Een dealer kan t-shares, die allemaal nodig zijn om het oorspronkelijke geheim te herstellen, naar een enkele ontvanger sturen, met gebruik van verschillende kanalen. Een aanvaller zou alle t-shares moeten onderscheppen om het geheim te herstellen, een taak die wellicht meer moeilijker dan het onderscheppen van één bericht ".
• De directeur van een bank kan aandelen genereren voor de kluis ontgrendelingscode van de bank en deze uitdelen aan zijn werknemers. Zelfs als de regisseur niet beschikbaar is, kan de kluis worden geopend, maar alleen als een bepaald aantal werknemers het samen doet. Hier kunnen geheime deelschema's de tewerkstelling van niet volledig vertrouwde mensen mogelijk maken.

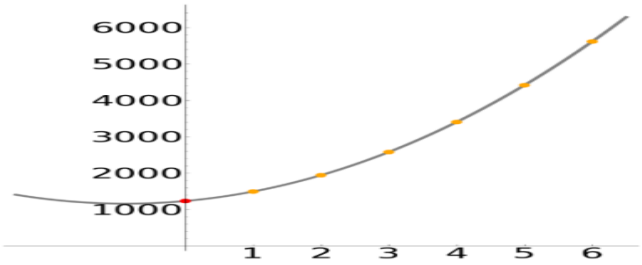


Afbeelding 8 : secret share principles

4.4 Two men's rule

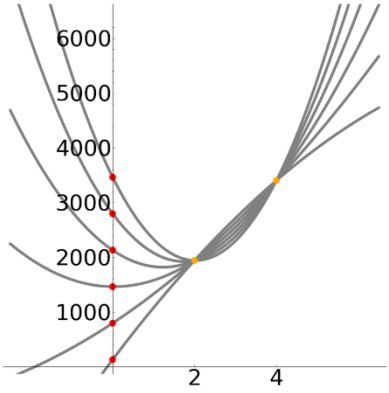
Deze regel wordt gebruikt in gevoelige gebieden, zoals het bevel om kernraketten te sturen om onopzettelijk of opzettelijk slippen te voorkomen. In cryptografie gebruiken Amerikanen de uitdrukking "two-person integrity" (TPI) als het erom gaat te voorkomen dat een persoon toegang heeft tot crypto grafische sleutels voor beveiligde communicatie (COMSEC).

Dus hier is een interessant concept dat ons zou helpen om deze problemen van vertrouwen en veiligheid op te lossen met de escrow-autoriteit. Door te eisen dat twee personen samenwerken om de gegevens in escrow te onthullen, beschermen we ons tegen een geïsoleerde kwaadwillige daad.
Laten we de wachtwoordzin van de escrow-sleutel verdelen en de stukken aan een groep vertrouwde mensen geven die we de familiekring (TFC) noemen
Hoe deze wachtwoordz op te splitsen? Het eenvoudig verdelen van N-stukken tussen de N-leden van de TFC dwingt hen om elkaar te ontmoeten om de privé-sleutel te vervolledigen.
Twee punten zijn voldoende om een lijn te definiëren, drie om een parabool te definiëren, enzovoort. Als we nu een geheim willen delen, zeggen de waarde 1234, tussen zes individuen en drie van hen zijn nodig om het geheim te vinden, zullen we willekeurig een parabool kiezen tussen degenen die door het punt gaan (0, 1234) en we zullen de coördineert zes van zijn punten aan deze zes personen (zie figuur 9).



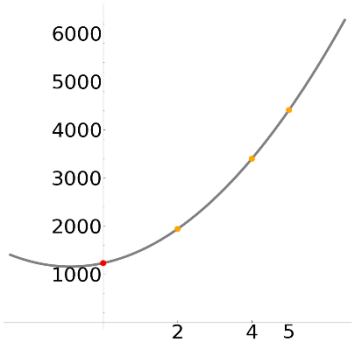
Afbeelding 9: Parabolic Passant Couples (0, 1234) one six seen points.

Als slechts twee van hen, nr. 2 en 4, kwamen om hun coördinaten te delen, ze konden de originele parabool en dus de waarde van het geheime punt in x = 0 niet vinden (zie figuur 10).



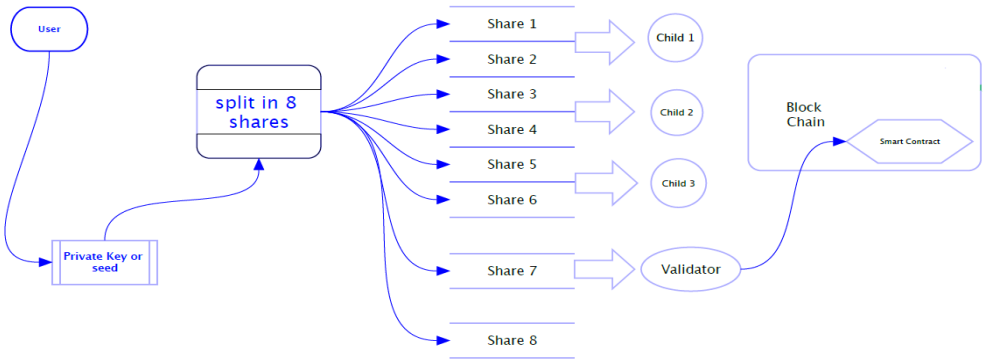
Afbeelding 10 : Parables passing through the points of the n ° 2 and 4.

Het is daarom noodzakelijk dat een derde persoon ermee instemt om zijn / haar coördinaten te delen om één en slechts één gelijkenis te definiëren en de geheime waarde 1234 te onthullen (zie figuur 11).



4.5 TFC shares distribution Protocol

De familiekring is voor een veilige haven een context van leden die tot een groep behoren, deze groep kan familieleden omvatten, een groep van belanghebbenden van het bedrijf of gewoon een vriendenkring. De TFC SDP is een protocol ontwikkeld door Safe Haven om een cirkel van vertrouwen in ons ecosysteem tot stand te brengen.
Als we onze hierboven beschreven technieken overwegen, hebben we een dealer (de persoon die zijn nalatenschap wil beschermen) en n spelers (zijn kinderen en de validator [notarissen]). De dealer geeft een geheim aan de spelers, maar alleen als aan specifieke voorwaarden is voldaan. De dealer doet dit door elke speler een aandeel te geven op een manier dat elke groep van t (voor drempelwaarde) of meer spelers samen het geheim kunnen reconstrueren, maar geen groep van minder dan t-spelers kan. Zo'n systeem wordt een (t, n) -drempelschema genoemd.



Afbeelding 11 : TFC Share Distribution Protocol

Basisregels voor TFC SD-protocol:

• Het veilige geheim om te splitsen in aandelen kan maximaal 1024 bit zijn.

• Als u een geheim groter dan 1024 bits wilt beschermen, moet een hybride techniek worden toegepast, het geheim moet worden gecodeerd met een blokcijfer en dan passen we alleen het geheim delen toe op de sleutel (openssl en gpg zijn geldige hulpmiddelen) .

• Het geheime beveiligingsniveau kan een bovengrens voor de lengte inhouden omdat korte geheimen / zaden / sleutels met wat zoutbeten worden opgevuld.

• We kunnen hexadecimale cijfers gebruiken in plaats van ASCII-tekens voor I / O, zodat binaire gegevens ook kunnen worden beveiligd / opgesplitst in shares.

• Tijdens het splitsen of combineren van het gedeelde geheim vergrendelt het protocol de virtuele adresruimte in RAM- of privacy redenen.

• Het aantal gedistribueerde aandeelentiteiten is technisch gesproken beperkt tot 99, we beperken dit zelfs verder tot 15, terwijl elke entiteit meer dan 15 maar <99 kan hebben.

• De validator y heeft altijd -1 minder gedeeld dan de n (spelers / kinderen).

• We hebben minstens 1 speler n en 1 validator nodig om een volledig netwerk van vertrouwen in het ecosysteem van veilige havens tot stand te brengen.

• Meerdere validators kunnen worden toegevoegd.

4.5.1 TFCSD Case 1: 1 kind en 1 validator

Gebaseerd op onze geheime schemaformule:

$$T = (\mathrm{y.n} - 1) + (\mathrm{X.n})$$

T = drempel van de minimale aandelen die nodig zijn om het geheim te reconstrueren.
Y = de validator van het proces, in ons geval is het een geregistreerd lid van het Alliance-programma van de Safe haven
X = de aandeelhouders

$T = (y.n - 1) + (X.n)$

$T = (y.1 - 1) + (X.1)$

$T = (2.1 - 1) + (2.1)$

$T = (2 - 1) + (2)$

$T = 1 + 2$

$T = 3$ (Minimaal aantal shares dat nodig is om de volledige gedeelde sleutel te verkrijgen.
Max aantal aandelen is 3 (2 voor het kind en 2 (-1) voor de validator.
Dus nemen we bijvoorbeeld het geheim: "Mijn gedeelde wachtwoordzin" krijgen we de volgende 3 gesplitste aandelen

```
1-4894b94c42b425aea3dc379edb9fbf47acac1eff
2-ec6f4decf4f21704a1db1263971f4b05d5966e5f
3-5fb79bc83b2cf7e7a04fd38e6dff8e06e538afec
```

Omdat we een aandelenrepresentatie van 100% hebben, is er maar één haalbaar scenario voor succes.

1 child = (1 x 2) & (2 – 1) validator = 3 = T so OK

4.5.2 TFCSD Case 2: 3 kinderen en 1 validator

Gebaseerd op onze geheime schemaformule:

$$T = (\mathrm{y.n} - 1) + (\mathrm{X.n})$$

T = drempel van de minimale aandelen die nodig zijn om het geheim te reconstrueren.
Y = de validator van het proces, in ons geval is het een geregistreerd lid van het Alliance-programma Safe haven
X = de aandeelhouders

$\boldsymbol{T = (y.n - 1) + (X.n)}$

$\boldsymbol{T = (y.1 - 1) + (X.3)}$

$\boldsymbol{T = (2.1 - 1) + (2.3)}$

$\boldsymbol{T = (2 - 1) + (6)}$

$\boldsymbol{T = 1 + 6}$

$\boldsymbol{T = 7}$ (Min. of shares that are needed in order to obtain the complete shared key.

Max aantal aandelen is 8 (6 voor de kinderen en 2 (-1) voor de validator
Dus nemen we bijvoorbeeld het geheim: "Mijn gedeelde wachtwoordzin" krijgen we de volgende 8 gesplitste aandelen.

```
1-4894b94c42b425aea3dc379edb9fbf47acac1eff
2-ec6f4decf4f21704a1db1263971f4b05d5966e5f
3-5fb79bc83b2cf7e7a04fd38e6dff8e06e538afec
4-71475064933c8d89f205f1ba5130482f4ad074ed
5-fe82d14bc9a2c2af21b9cb2b27f7baa4e819fc72
6-bf6c7907cde9d5aa66a366ef133b5c9260dde965
7-4f4e94991acbcead67cc871f04a4bfd1b8e98598
8-03d8b8a9d0e1d3b112c0ed60de3a9295639a7759
```

En we zullen 7 van de 8 nodig hebben om het geheim te reconstrueren. Dus als we de aandelen nemen van

3 kinderen = 3 x 2 = 6 <7 dus NOK
2 kinderen + 1 validator = 2 x 2 + 2-1 = 5 <T dus NOK
3 kinderen + 1 validator = 3 x2 + 2-1 = 7 = T dus OK

4.5.3 TFCSD Case 2: 3 kinderen + fail-safe en 1 validator

Op basis van onze geheime schemaformule en voeg toe (b = x-):

$T = (\mathrm{y.n} - 1) + (\mathrm{X.n})$ + (b= x)

T = drempel van de minimale aandelen die nodig zijn om het geheim te reconstrueren.
Y = de validator van het proces, in ons geval is het een geregistreerd lid van het Alliance-programma van de Safe haven

X = de aandeelhouders

$T = (y.n - 1) + (X.n)$ *+ (b=x)*

$T = (y.1 - 1) + (X.3)$ *+ (b=x)*

$T = (2.1 - 1) + (2.3)$ *+ (b = 2)*

$T = (2 - 1) + (6)$ *+ 2*

$T = 1 + 6$ *+ 2*

T = 7 (het aantal benodigde aandelen om de volledige gedeelde sleutel te verkrijgen.
Max aantal aandelen is 9 (6 voor de kinderen en 2 (-1) voor de validator + 2 (fail-save)
Dus nemen we bijvoorbeeld het geheim: "Mijn gedeelde wachtwoordzin" krijgen we de volgende 9 gesplitste aandelen

1-c6bde31ffc0b7474dcc576b0ab66cc3b09d7696a
2-aaae1588d6b7ddd80a14fac4fb68b7b7b19237f4
3-72061a3daf8af2585d139e37a095cddc35804e54
4-b158248b9dcf57d9c925287741532aa3ea5cc719
5-75516fa7eb1601e44863553254b0c99637392129
6-399bce6c6b29b04cfcf96e5292575f1670ff5b98
7-672c6a3398102ce986e62c46370861ffc6a0964c
8-1270dd67873bae0e21fba54a45e25622cbe7c7e1
9-084c327b0c9b727cd5d68210fe0000ce5da376af

En we zullen 7 van de 9 nodig hebben om het geheim te reconstrueren. Dus als we de aandelen nemen van
3 kinderen (of 2 + fail-safe) = 3 x 2 = 6 <7 dus NOK
2 kinderen + 1 validator = 2 x 2 + 2-1 = 5 <T dus NOK
3 kinderen (of 2 + fail-safe) + 1 validator = 3 x2 + 2-1 = 7 = T dus OK

4.5.4 TFCSD Case 3: 3 kinderen en 2 validators

Gebaseerd op onze geheime schemaformule:

$$T = (\mathrm{y.n} - 1) + (\mathrm{X.n})$$

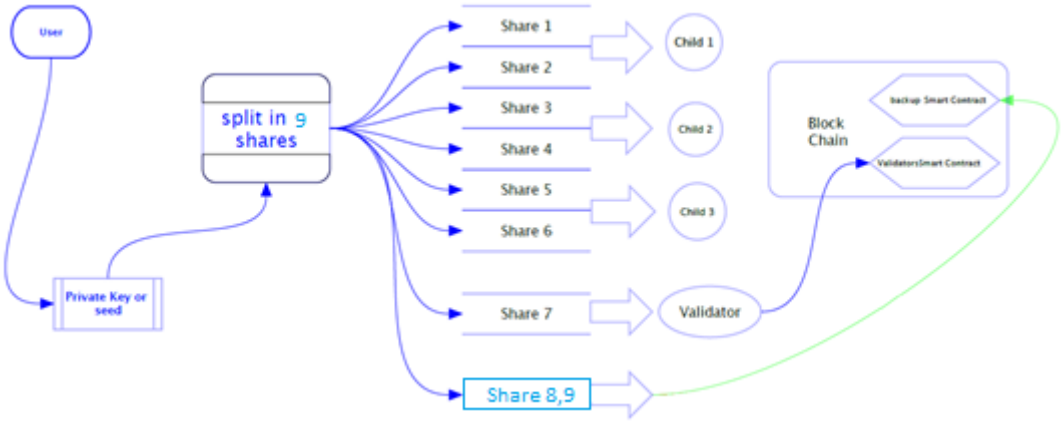
T = drempel van de minimale aandelen die nodig zijn om het geheim te reconstrueren.
Y = de validator van het proces, in ons geval is het een geregistreerd lid van het Alliance-programma van de Safe haven
-1 = Fail-save share
X = de aandeelhouders
T = (y.n-1) + (X.n)
T = ((Y2) -1) + (X.3)
T = ((2.2) - 1) + (3.3)
T = (4-1) + (9)
T = 12
T = 12 (Aantal shares dat nodig is om de volledige gedeelde sleutel te verkrijgen.
Max aantal aandelen is 13 (9 voor de kinderen en 4 (-1) voor de validator

Dus nemen we bijvoorbeeld het geheim: "Mijn gedeelde wachtwoordzin" krijgen we de volgende 13 gesplitste aandelen

01-b8d792946afa60b35d53609c03ae96320b78a0f6
02-92769c90836c393d06675d4e25201c3cc2ac0a85
03-9968d3d6e953590dc15363fc92acea7464eb2053
04-92a5e10da6dae5a4353ec755a5febaa76023c0fb
05-c0afccce07c511436f83db4c3a7aeaf5f69aa44f
06-a47453a4cd7b887f82df30ccdf864cc91467e738
07-3a95ee802152c02045cb1dc9aa2843291497a19c
08-82e043652371d0e9972520dade32660c6bc6d504
09-d0db492e80b8ebf2a5498867ebf91413864aa73f
10-a334c5ae2f2d00e6cb04dc97be9c1cf08c0e47e9
11-058f661fbe6bb9f94401c4b143888dbb9d58ed92
12-56f805b3d9a83ed57dcfed5014eb92a3c7ad287f
13-6803214791f5621cdb01a6291cc189e7a1b173b1

En we zullen 12 van de 13 nodig hebben om het geheim te reconstrueren. Dus als we de aandelen van nemen
3 kinderen = 3 x 3 = 9 <12 dus NOK
3 kinderen + 1 validator = 3 x 3 + 2 - 1 = 10 <T dus NOK
3 kinderen + 2 validators = 3 x 3 + 4 - 1 = 12 = T dus OK

5 TFC Fail-Safe aandelen



Afbeelding 12 : TFC Fail-safe share

TFC SD Fail-safe Protocol:

• De resterende aandelen worden gebruikt als een soort fail-safe share

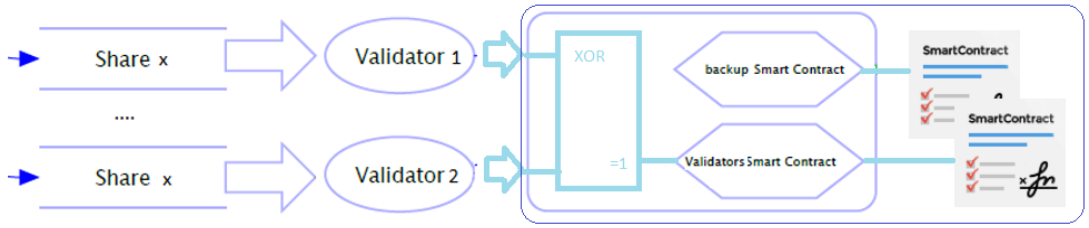
• Dit kan handig zijn in het geval dat een van de n (spelers / kinderen) zijn deel verliest, niet in staat is om rechtmatig te handelen of sterft.

• Ons protocol biedt een afzonderlijk "back-up" slim contract op de blockchain met verschillende voorwaarden die zijn geschreven.

• De fail-safe shares kunnen in geen geval aan een van de n (spelers / kinderen) worden gegeven, omdat dit de complete set-up van de dealer (ouder) in gevaar zou brengen, zoals in use case 2 (3 kinderen + 1 validator)) de kinderen kunnen de geheime share niet opnieuw compileren zonder dat de validators delen (via de Smart Contract-query voor blockchain-koppelingen), maar als u de back-upshares geeft, kunnen ze dit doen.

• Het enige geval waarin we geen fail-save share hebben, is wanneer we een consensus van 100% van de stakeholder nodig hebben, bijvoorbeeld use case 1 (1 child + 1 validator).

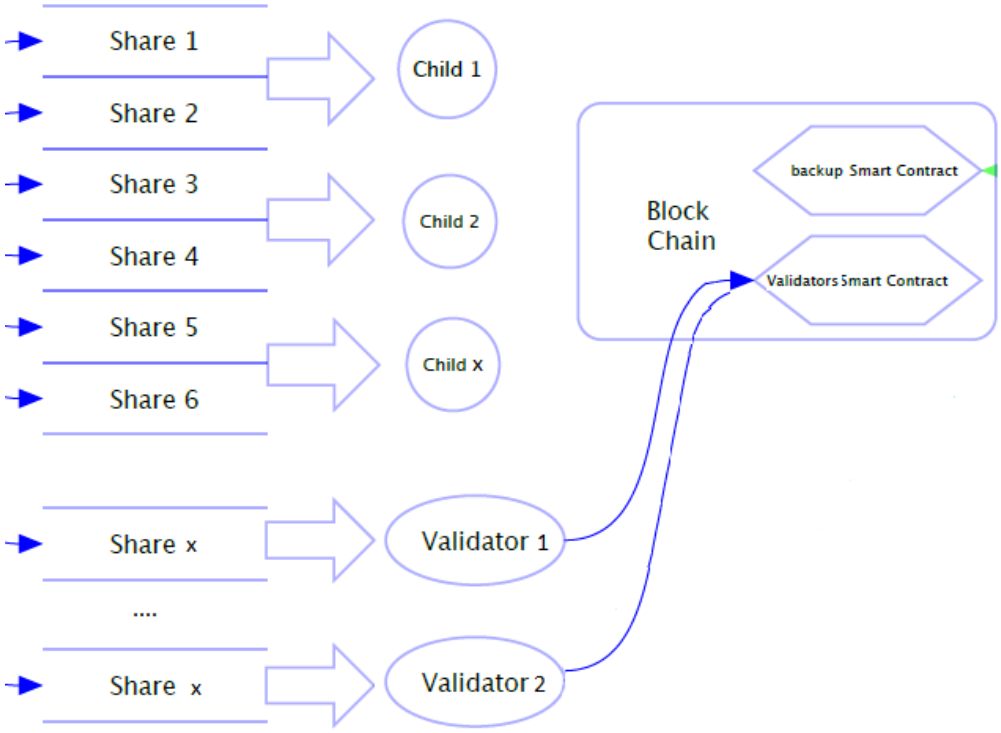
5.1 Het validatie – deel proces.



Afbeelding 13 : Validators share process

• Het deelproces van de validators bestaat uit een pool van validators van rechtspersonen, die lid zijn van ons Alliantieprogramma.
• De validator heeft niets van de shares die bestemd zijn om naar de blockchain te worden verzonden, bezit of ziet, daar is de rol transparant wat betreft de inzet van geheime shares.
• Ze verdelen de aandelen aan de n (spelers / kinderen / belanghebbenden) op een formele manier door een wettelijk certificaat af te geven aan n en de transactie naar de blockchain op een transparante manier te valideren.
• De validators delen is eigenlijk het deel van de persoon die het proces om te beginnen heeft gestart, hij beveiligt het in de blockchain via een validator om volledig recht te houden op het volledige geheime aandeel, en dus zijn vermogen zolang hij leeft.
• De validator (s) is / zijn de enige die de vorige verzending van de share naar de blockchain kunnen ophalen als aan de volgende voorwaarden is voldaan.
o Het totale aantal aandelen van de n (spelers / kinderen / stakeholders) moet aanwezig zijn, zo niet, en indien nodig, kan het fail-safe-aandeel ook worden opgehaald door de validator als aan de voorwaarden voor Smart-contractbevestiging is voldaan.
o In het geval dat de initiator (ouder / dealer) sterft, moet de validator de rechtmatige medische formulieren valideren om het ophaalproces van het gedeelde dat is opgeslagen in de blockchain te starten.
• Het aandeel van initiatiefnemer / ouders is ook overdraagbaar aan een andere legitieme persoon wanneer dat nodig is

5.2 Verschillende Validatie mogelijkheden



Afbeelding 14 : Multiple validator's scheme

TFC SD mogelijkheid voor meerdere validators:

• Niemand is eeuwig en de juridische entiteiten nemen ook niet deel aan ons alliantieprogramma. Daarom bieden we de mogelijkheid om een netwerk van vertrouwensrelaties op te zetten met meer dan 1 validator.

• Als u ervoor kiest om meerdere validators bij de hand te hebben, pushen we een slim back-upcontract in de blockchain die de benodigde shares bevat, n (spelers / kinderen) -1, die kunnen worden gebruikt door een tweede validator.

• Door dit te doen bieden we een ecosysteem van vertrouwen dat volledig overbodig is in termen van verdeling en validatie van het aandeel.

6 SH-Alliantie Programma

Het Safe Havens Alliantieprogramma is een groep van rechtspersonen die door een veilige haven zijn gescreend om alle noodzakelijke stappen te ondernemen om ons doel te bereiken, het starten van de toekomst van vertrouwen door uw vermogen veilig te stellen en door dat te doen uw familieleden, belanghebbenden en jouw nalatenschap.
Als u een rechtspersoon bent die lid wil worden van ons Bondgenootschap, stuur dan een aanvraag naar info@safehaven.io en we nemen contact met u op zodra we ons juridische platform hebben uitgewerkt. We zullen binnenkort een toegewijd vertrouwd Alliance-portaal lanceren om alle juridische vragen te beantwoorden.
Zodra onze portal wordt gelanceerd, kunnen juridische entiteiten zich inschrijven, uiteraard worden er juridische certificeringsdocumenten gevraagd die het screeningproces helpen. De leden zullen worden gevraagd om een jaarlijkse vergoeding te betalen om een abonnement op onze diensten te verkrijgen. De tokens worden gebruikt als gas om de slimme contracten op de blockchain in te zetten.
We zijn momenteel aan het analyseren welke juridische entiteiten precies lid van onze alliantie zouden kunnen zijn. We hebben vertrouwensrelaties nodig in onze cirkel van vertrouwen.

7 SHA beschermings plannen

1. Het Family Circle Plan (TFC)
Het gezinscirkelplan is voor diegenen die hun familieleden willen geruststellen, dat is waar, de dag dat ze overlijden, kunnen kinderen toegang krijgen tot de door de ouder verworven vermogens. De mogelijkheden zijn bijna eindeloos, aandelen kunnen op flexibele wijze worden verdeeld, terwijl het geheim op een veilige en transparante manier wordt bewaard. Het feit dat we validators toevoegen aan ons proces, houdt het proces bekend voor belangrijke zaken zoals die we willen helpen beveiligen. We voegen de wondere wereld van block chaining toe aan ons proces dat het aandeel gedecentraliseerd houdt. De gedecentraliseerde toewijzing van database-validator-slimme contracten voegt een extra beveiligingsfunctie toe, gecombineerd met een state-of-the-art, nog steeds simplistisch protocol voor geheim delen.

2. Het Business Continuity Plan (BCP)
Het Business Continuity-plan lijkt veel op de TFC, het belangrijkste verschil is dat we spreken over belanghebbenden in plaats van kinderen en dat het validatieproces verschillend is in termen van het ontgrendelen van aandelen. In een BCP heeft de notaris geen medische herroepingsdocumenten nodig om het ontbrekende aandeel via onze diensten te verkrijgen, maar eerder notariële handelingen die door hemzelf worden voorbereid. Dit procesplan wordt momenteel intern ontwikkeld en komt beschikbaar voor gebruik vanaf het moment dat de Trust Alliance-portal online is. BCP kan nuttig zijn voor de distributie van gedeeld geheim van multi-sig-portefeuilles, uitwisselingen of eenvoudig voor het bewaren van importwachtwoorden / wachtzinnen. Nogmaals, de mogelijkheden zijn eindeloos.

3. De investeringskring

De investeringskring is bedoeld voor iedereen die bereid is om een fonds te creëren bij vrienden, familieleden of zakelijke belanghebbenden. Laten we zeggen dat 5 vrienden willen investeren in crypto, en kopen voor elke crypto-valuta van 1000 dollar. Wat zijn hun opties? Het creëren van een multi-sig wallet (met alle onvolkomenheden die we de laatste tijd hebben ontdekt), zelfs als deze volledig veilig is, heb je altijd vertrouwen binnen de groep nodig ... ok, hoe gaan we dit beheren? Eenvoudig! Via het Safe Haven Share Distribution-protocol. U codeert de privésleutel en we splitsen de wachtwoordzin in aandelen, de belanghebbenden ontvangen evenveel aandelen. Als we de formule beschouwen zonder een faalveilig mechanisme, hebben we T = (yn-1) + (Xn), T = (2 -1) + (2,5) = 1 + 10 = 11 aandelen om te verdelen waar 1 zal zijn opgeslagen op de blockchain via de validator (juridische entiteit) De voorwaarden om dit aandeel te kunnen vrijmaken, kunnen variëren van prijsdrempels tot mijlpalen tot simpelweg 100% consensus om dit te doen. Nogmaals, de mogelijkheden zijn eindeloos.

4. Safe Haven Vault

Goede wachtwoorden zijn moeilijk te onthouden en kunnen niet worden overgedragen, niet op een legale manier, van u naar uw familieleden. Dit wachtwoord kan van alles zijn, van Facebook, Gmail of een ander belangrijk account. Als je dat wilt, zorg er dan voor dat je digitale nalatigheid niet met je sterft, dat je familieleden toegang hebben tot die accounts, zelfs als je er niet meer bent, sla ze op via Safe Haven op de blockchain met behulp van een van onze Share Distribution-protocollen.

8 Conclusie

Investeren in Crypto-valuta en Bitcoin kost tegenwoordig veel tijd en is zeer uitdagend, aan de andere kant zal het enorme winsten opleveren door de jaren heen. Het beveiligen van die assets en ze te kunnen beschermen tegen elke vorm van traktatie van buitenaf, is iets waar alle traders en langetermijn beleggers al heel lang naar vragen. We zijn allemaal om dezelfde reden in dit bedrijf, zijn financieel onafhankelijk en bouwen een veilige toekomst voor onze familieleden. Daarom zullen we ons gedecentraliseerde platform ontwikkelen en onze oplossing wereldwijd aanbieden. The Safe Haven Company zal een verschil maken in het beveiligen en opslaan van uw digitale sleutels of zaden. Het bouwen van een oplossing zoals Safe Haven zal het stuk in gedachten brengen voor de belegger en familieleden. We hopen dat u overtuigd bent van ons platform en verschillende oplossingen en we kunnen u verwelkomen als een van onze investeerders!

9 Markt

Crypto-valuta's zijn digitale activa die cryptografie gebruiken, een coderingstechniek, voor beveiliging. Crypto-valuta's worden voornamelijk gebruikt voor het kopen en verkopen van goederen en diensten, hoewel sommige nieuwere crypto-valuta's ook functioneren als een reeks regels of verplichtingen voor de houders ervan. Ze hebben geen intrinsieke waarde omdat ze niet inwisselbaar zijn voor een ander goed, zoals goud. In tegenstelling tot traditionele valuta, worden ze niet uitgegeven door een centrale autoriteit en worden ze niet als wettig betaalmiddel beschouwd.
Op dit moment is het gebruik van crypto-valuta's grotendeels beperkt tot 'early adopters'. Op schaal zijn er wereldwijd ongeveer 10 miljoen Bitcoin-houders, waarbij ongeveer de helft Bitcoin puur voor beleggingsdoeleinden houdt. Objectief gezien zijn crypto-valuta's niet nodig omdat door de overheid gesteunde valuta's adequaat functioneren. Voor de meeste gebruikers zijn de voordelen van crypto-valuta's theoretisch. Daarom zal mainstream-adoptie alleen plaatsvinden als er een significant tastbaar voordeel is van het gebruik van een crypto-valuta. Dus wat zijn de voordelen om ze te gebruiken?
Crypto-valuta Uitwisseling
Crypto-valutawissels zijn websites waar individuen crypto-valuta kunnen kopen, verkopen of inwisselen voor andere digitale valuta of traditionele valuta. De beurzen kunnen crypto-valuta's omzetten in door de overheid gesteunde valuta's en kunnen crypto-valuta's omzetten naar andere crypto-valuta's. Enkele van de grootste uitwisselingen zijn Poloniex, Bitfinex, Kraken en GDAX, die meer dan $ 100 miljoen (equivalent) per dag kunnen verhandelen. Vrijwel elke beurs is onderworpen aan anti-witwasreglementen van de overheid en klanten moeten een identiteitsbewijs tonen bij het openen van een account.

In plaats van uitwisselingen gebruiken mensen soms peer-to-peer-transacties via sites zoals LocalBitcoins, waardoor handelaren geen persoonlijke informatie hoeven te onthullen. In een peer-to-peer-transactie verhandelen deelnemers crypto-valuta's in transacties via software zonder tussenkomst van een andere tussenpersoon.

Crypto-valuta wallets:

Crypto-valuta portefeuilles zijn nodig voor gebruikers om digitale valuta te verzenden en ontvangen en hun saldo te controleren. Portefeuilles kunnen hardware of software zijn, hoewel hardware portefeuilles als veiliger worden beschouwd. De Ledger-portemonnee ziet er bijvoorbeeld als een USB-stick eruit en maakt verbinding met de USB-poort van een computer. Terwijl de transacties en saldi voor een bitcoin-account op de blockchain zelf worden geregistreerd, wordt de privésleutel die wordt gebruikt om nieuwe transacties te ondertekenen, opgeslagen in de Ledger-portefeuille. Wanneer u een nieuwe transactie probeert te maken, vraagt uw computer de portefeuille om deze te ondertekenen en verzendt deze naar de blockchain. Omdat de persoonlijke sleutel nooit de hardware portefeuille verlaat, zijn uw bitcoins veilig, zelfs als uw computer is gehackt. Toch zou het verlies van de activa van de houder resulteren in verlies van de portefeuille, tenzij een back-up wordt gemaakt. Een portemonnee voor een software zoals de Coin-basisportemonnee is daarentegen virtueel. Dit type softwareapparaat kan het geld van de houder online plaatsen in het bezit van de portefeuilleprovider, wat extra risico's met zich mee brengt.
Nu meer mensen en meer geld de crypto-valutamarkt binnenstromen, moeten meer mensen uitwisselingen of portefeuilles openen en privésleutels krijgen. Safe Haven is de perfecte oplossing aan het bouwen. In principe kan elke persoon die een portemonnee opent, een crypto-valuta kopen, een Safe Haven-klant zijn. Ons potentieel om te groeien in deze markt is enorm! We zijn ervan overtuigd dat Safe Haven een verschil zal maken.

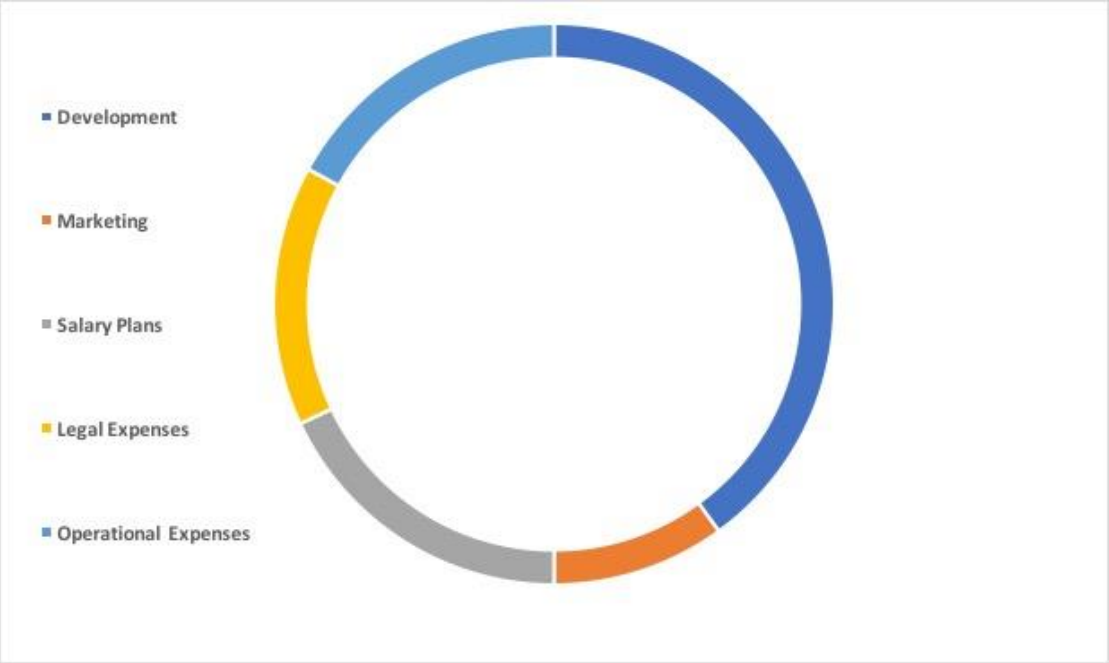
10 Token

Het SHA-token is een ERC20-token dat bovenop Ethereum is gebouwd. ERC20-standaard is geïntroduceerd op de Ethereum-blockchain om ontwikkelaars in staat te stellen decentrale apps (Dapps) te ontwerpen om direct met tokens te werken zonder het wiel telkens opnieuw uit te vinden wanneer een nieuw tokensysteem wordt geïntroduceerd. Daarom kan iedereen met een idee met ERC20 een product op de blockchain implementeren zonder het hele proces van het ontwerpen van het platform te hoeven ondergaan. Met ERC20 kunnen we een gemeenschappelijke reeks regels definiëren waaraan de op Ethereum gebaseerde SHA zich moet houden. We kunnen van tevoren weten hoe het token zich zal gedragen op basis van de standaard. Het SHA-

token is ontwikkeld om de gebroken markt te helen die we in dit document hebben beschreven. De eerste fase van ontwikkeling betreft het aantal tokens dat we maken. Het SHA-token zal tijdens het proces als een gas worden gebruikt.

11 toewijzing van fondsen

- Ontwikkeling 40%
- Marketing 10%
- Salarisplannen 18%
- Juridische kosten 15%
- Operationele kosten 17%



We streven ernaar een groot deel van de ingezamelde gelden toe te wijzen om de ontwikkeling in termen van het platform te vergemakkelijken. Daarom gaat 40% van de middelen naar dit initiatief. 10% van de middelen zal worden toegewezen om verschillende marketingactiviteiten, waaronder bounty-campagnes en handtekeningcampagnes, te vergemakkelijken. 15% zal worden toegewezen aan legale markten zoals beurzen. 17% van de middelen zijn voor operationele kosten en 18% zal worden toegerekend aan salarisplannen.

12 ICO Parameters + Token toewijzing

Ticker: SHA

Totale voorraad: 120.000.000

Ethereum Based Tokens (ERC20)

Startdatum ICO: ZIE https://ico.safehaven.io

VOORVERKOOP Startdatum: ZIE https://safehaven.io/#pre-sale

Wisselkoers vroege beleggers: 2500 SHA = 1ETH

Wisselkoersvoorverkoop: 2000 SHA = 1 ETH

Wisselkoers ICO: 1500 SHA = 1 ETH

Minimale dop: 1000 ETH

Maximum Cap: 54.500ETH

Token toewijzing

ICO VROEGE INVESTEERDERS: 2500 SHA / ETH TOTAAL (5.000.000 SHA)

ICO PRE-SALE: 2000 SHA / ETH TOTAL (25.000.000 SHA)

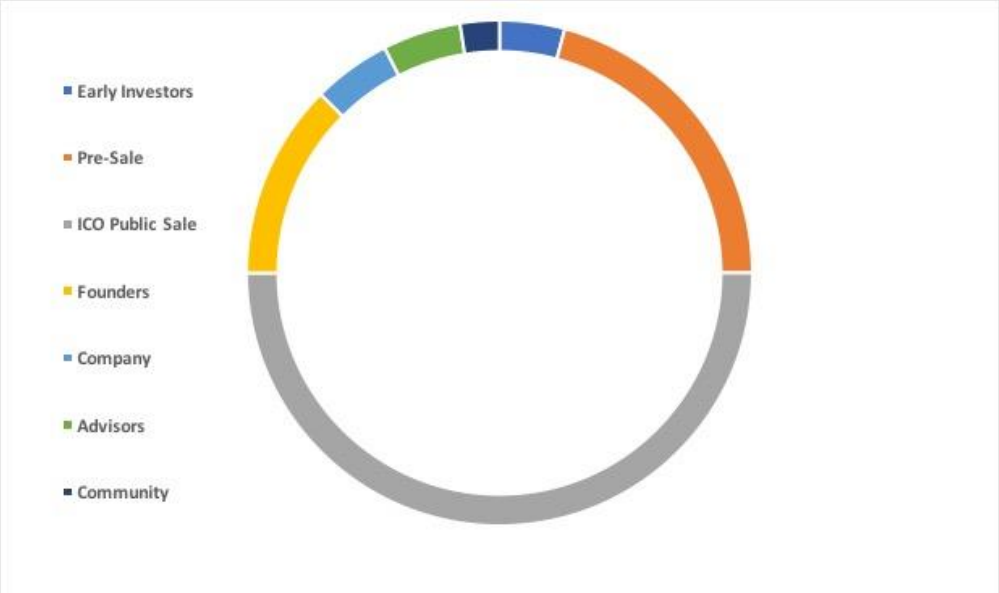
ICO PUBIC VERKOOP: 1500 SHA / ETH TOTAAL (60.000.000 SHA)

FOUNDERS: 15.000.000 SHA

BEDRIJF: 6.000.000 SHA

ADVISEURS: 6.000.000 SHA

GEMEENSCHAP & PROVINCIE: 3.000.000 SHA



13 Roadmap


Q3 2017
• Idea Reflection
• Creating SD Protocols
Q4 2017
• Writing White paper
• Development front-end
• Setting up social media
• Consulting Advisors & legal entities
• Pre sale Launch
Q1 2018
• Ico Launch
• Safehaven platform development
• Alliance program expansion
• Off-line client dev (Linux,...)
Q2 2018
• Safehaven platform development + beta launch
• Alliance program expansion
Q3 2018
• Platform Production Launch
• Alliance program expansion
• Hardware ledger integration program launch
Q4 2018
• (will be published once available on safehaven.io site)