SAFE HAVEN

The Solution To Digital Inheritance

Executive Summary

Cryptocurrencies and digital assets are a new and evolving concept that promote a future with decentralized stores of value and peer-to-peer transactions. However, with any new and revolutionary idea comes skepticism and distrust. Digital currencies are volatile, unpredictable, and easily lost. Once our valuable stakes in digital assets are gone, they cannot ever be retrieved regardless of reasons (simple forgetfulness, loss of keys or saved passphrases, or in some instances, death). Losing cryptocurrencies contributes to the many problems hindering the advancement and widespread utilization of digital assets in the modern world.

Safe Haven offers a solution to this problem by providing a safe, secure, and transparent means for one's digital assets to be inherited by anyone they choose, at any time they choose, while remaining in full control of their investment. Safe Haven's complex, yet effective platform uses the advanced technology of Smart Contracts combined with legal entities from across the globe. This combination empowers Safe Haven Digital Asset (SHA DA) holders to ensure secure inheritance of widespread digital assets. Any group or organization can utilize Safe Haven's platform.

The Safe Haven solution requires minimal involvement, which results in the initiator remaining in control. The initiator may retrieve his or her token at any time throughout the process. Through secure encryption, the initiator's keys are split and encoded in the blockchain. The number of times the key is split varies, and depends on The number of times the key is split varies between each case. By enlisting legal entities worldwide via our TAN (Trust Alliance Network) each individual case is legally noted, and conditions for inheritance are given on an individual level, dependent on the wishes of the initiator. By involving both legal entities and secure, encrypted transactions all while leaving the initiator completely in control, our solution is transparent, easy to use, and unprecedented.

Table of Contents

1. INTRODUCTION

Nearly every day, someone or some news outlet releases a story about lost Bitcoin, Litecoin, or various other digital assets. Typically, the loss can be pinned to carelessness, misplacement of private keys, death, and even blockchain mistakes[1]. The crypto-space is young, both in age and investor demographic. With it comes a lack of concern regarding the loss of digital assets due to unforeseeable circumstances.

Consider Bitcoin's loss statistic: 4 million Bitcoin are assumed to be lost forever due to general human and transactional error[2]. As mentioned earlier, the youth and pace of this space does not allow time individuals to necessarily plan for future life circumstances. Failure to recall the private key or passphrase results in a permanent loss of digital currency. This also means that the access point to your assets is shut off indefinitely should your heirs be unaware of you holding digital assets, or if they lack access to your keys. Even in cases where heirs have access to the investor's keys, the heirs may not have the skills to retrieve the digital assets themselves. These facts may justify some of the hesitation traditional investors have in choosing cryptocurrency as an investment or store of value.

There's also the issue of an investor's lack of confidence with sharing his or her private key with heirs. Storing this information insecurely could lead to physical loss of it, theft, or even manipulation of assets.[3] There are many investors in the cryptocurrency market and the vast majority invest with the long-term goal of securing their future and family's financial stability.

Digital assets are prone to loss; either by error or death, but that does not mean one has to bear all of the risks if he or she wishes to share in the profits. The Safe Haven Digital Asset (SHA DA), was built to protect one's digital legacy and ensure one's family has access to his or her assets, when necessary. The SHA DA is the only truly secure and 100% inheritable digital asset to date. Safe Haven's platform incorporates cutting edge features and

[1] Southurt, J. (2013, October 25). How "dumb mistakes" can lead to costly bitcoin losses. *Coin Desk.* Retrieved March 25, 2018, from https://www.coindesk.com/dumb-mistakes-costly-bitcoin-losses/

[2] Roberts, J. J., & Rapp, N. (2017, November 25). Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says. *Fortune.* Retrieved February, 2018, from http://fortune.com/2017/11/25/lost-bitcoins/

[3] Roberts, J. J. (2017, September 26). What Happens to Cryptocurrency When You Die? *Fortune.* Retrieved February/March, 2018, from http://fortune.com/2017/09/26/crytocurrency-bitcoin-death/

revolutionary technologies such as the Ethereum Blockchain, smart contracts, and our own patented Trust Alliance Network, which allows SHA tokens to be extremely secure and inheritable, while still granting the investor liquidity and complete control over his or her funds as they grow in value.

2. Four-Step Solution

Safe Haven gives contributors the opportunity to secure their digital assets without locking themselves out. Thanks to our TFC Share Distribution Key, Escrow Protocol, and the Trust Alliance Network (TAN), seeds/private keys/passphrases can be shared amongst stakeholders or family members in a transparent and secure manner. Our protocol distributes the shares in a way where the investor keeps (at all costs) the power over his assets. On the unfortunate day that he/she should pass away, a registered member of the Trust Alliance Platform (notary) can retrieve the remaining share on the blockchain to pass the contributor's legacy down to his/her children or stakeholders.

Step 1:

The example user protects his legacy (crypto assets) and plans to distribute his seeds/private keys or passphrases using Safe Haven's secure and transparent blockchain solution amongst his three children. The initiator of the process goes to a registered member of our Trust Alliance Network; this is a group of legal entities that have a secure relationship with Safe Haven. Together, they process the necessary validation steps.

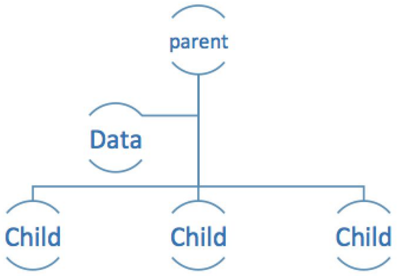


Figure 1: The Family Circle (TFC)

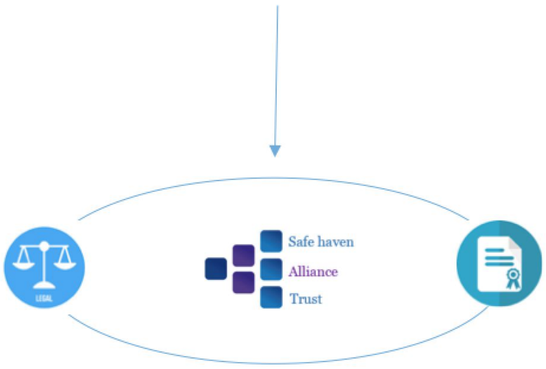


Figure 2: The Trust Alliance Representation

Step 2: The legal entity, referred to as the validator, divides the data to protect and distribute (see TFC shares distribution Protocol) the obtained shares to the children by using the Safe Haven application specifically developed for this use. The software used for this will not keep any data in memory or in centralized databases. Only the validator's share (see section 4.6 Validator's Share Process) will be sent to the blockchain. The security algorithm to encrypt and decrypt the share, before getting deployed through a smart contract, will not be revealed for obvious security reasons. Safe Haven will only have mapping in place to identify the validator's ID and the Smart contract; the mapping will be deployed on a decentralized blockchain database. This will also be the case for the backup validators (see Multiple Validators Possibility & TFC Fail-Safe Share(s)).

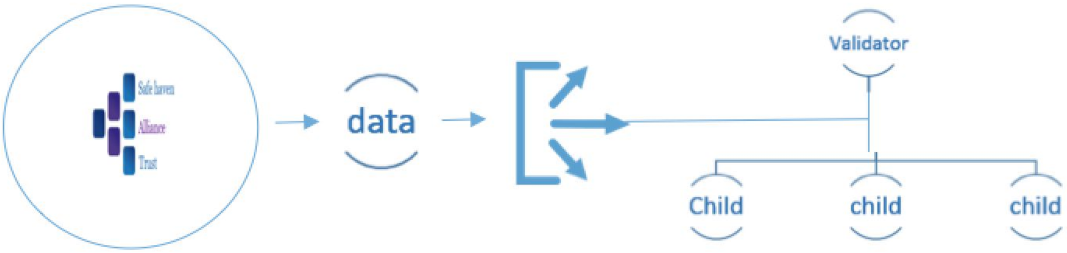


Figure 3: Split In Shares Step

Step 3: The shares distributed to the children are managed by the notary in the form of a legal certificate. The share (which is being protected), coming from the parent/initiator, will be encrypted by the Safe Haven Application (only accessible by members of the Trust Alliance) and sent to the blockchain in the form of a Smart Contract.

The child's shares can be shared through the creation of a certificate and/or through the integration of a hardware ledger in our protocol. We are currently working out the details in order to achieve this, based on our own hardware ledgers. Details are not made public yet as we are still in the ICO phase of our project.

Figure 4 : Child Certificates

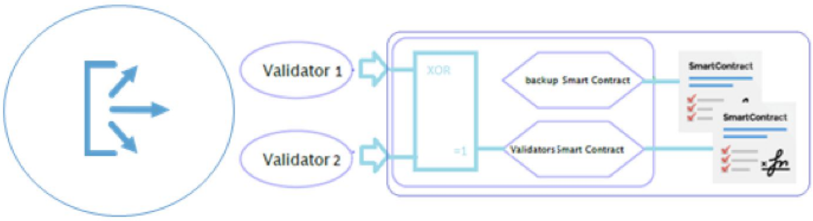


Figure 5 : Validators Process

Step 4: In the case of a sudden death or in case the contributor is not able to handle his/her assets on his/her own, the children or stakeholders can obtain the missing share by introducing the necessary legal documents to the notary. Stakeholders will then, once verified by Safe Haven, be able to retrieve the missing share from the blockchain.

Our Protocol handles fail-safe share and the possibility to have a backup validator. For further details check out our TFC Fail-Safe Share(s) & Multiple Validators Possibility in section 4.5.

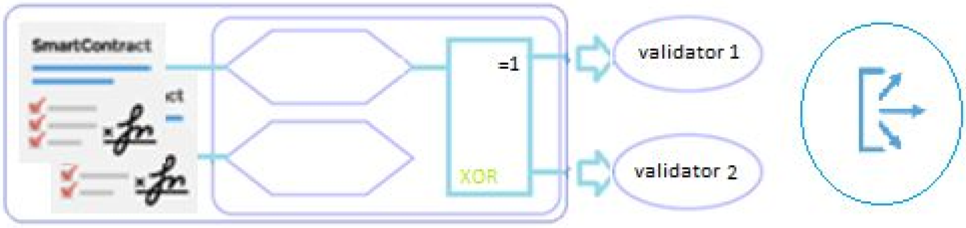


Figure 6: Share Retrieval Process

3. Basic Principles

3.1 Blockchain

The blockchain is a software innovation for establishing digital trust between users who facilitate transactions of value over a network. The blockchain enables trust to be distributed throughout a network, without the need for a central intermediary to track, verify, and approve the digital exchange of value. The notion of authorizing trust from a central intermediary currently underpins both private and government institutional structures; however, this is proving to be costly, slow, and also vulnerable to attack. The blockchain overcomes these issues by operating as a decentralized distributed database, maintaining a continuously growing list of records called blocks.

3.2 Smart Contract

On-chain computer code or "Smart Contracts" are computer protocols that facilitate, verify, and enforce the performance of a contract, making a contractual clause unnecessary. Smart contracts often emulate the logic of contractual clauses. Smart contracts can exchange money, property, shares, or anything of value in a transparent, conflict-free way, while avoiding the services of a middleman. Ordinarily, a process would require payment to a middleman, government agency, bank, lawyer or a notary, and then a processing time before the receipt of goods or services. However, smart contract technology automates this process. Smart contract technology can be compared to an automated vending machine: money is deposited into the machine and the desired item drops for collection, as long as the correct amount is deposited. In comparison, with a smart contract, the money is deposited into escrow on the blockchain for a receipt of a transfer of a token (e.g. a digital certificate of title for a house), which is instantaneously transferred into a counterparty’s control once the conditions are met. Smart contracts not only define the terms and conditions around an agreement in the same way that a traditional contract does, but it also provides enforcement of those obligations.

4. Techniques & Conceptual Mathematics

4.1. Polynomial Interpolation

Polynomials can be used to approximate complicated curves, for example, the shapes of letters in typography. A relevant application is the evaluation of the natural logarithm and trigonometric functions: pick a few known data points, create a lookup table, and interpolate between said data points. This results in significantly faster computations.

Definition:

Given a set of $n + 1$ data points (x_i, y_i) where no two x_i are the same, one is looking for a polynomial p of degree at most n with the property.

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

The "unisolvence" theorem states that such a polynomial p exists and is unique, and can be proved by the Vandermonde matrix, as described below.

The theorem states that for n + 1 interpolation nodes (xi), polynomial interpolation defines a linear bisection.

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

Where Πn is the vector space of polynomials (defined on any interval containing the nodes) of degree at most *n*.

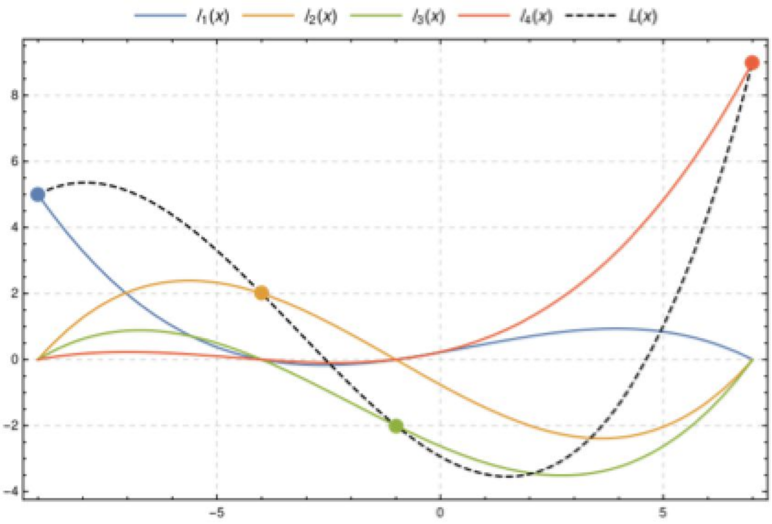


Figure 7: Polynomials

Polynomial interpolation also forms the basis for algorithms in numerical quadrature, numerical ordinary differential equations, and Secure Multi-Party Computation, and Secret Sharing schemes. Secret Sharing schemes are what we use to achieve our goal.

4.2 Key Escrow

We are not immortal, and it would be a shame if our assets disappeared with us.

The sudden loss of a shareholder could be a problem in order to retrieve the complete passphrase In this document we will continue to use the example of a family circle or friends in order to highlight the different case scenarios.

One answer to this problem is what is called the key escrow, which allows a third party "under certain conditions" to access these shares. But what third party? Under what conditions? And how do we give it our moral but also technical confidence? The escrow authority must be able to securely guarantee the confidentiality of the escrow keys.

First, we would encrypt the data, this can be a private key or a seed with a secure encryption algorithm (like SHA256-512) and by using a passphrase. This passphrase could then be divided into shares and distributed by our TFC SD Protocol.

4.3 Secret Sharing

In cryptography, a secret sharing scheme is a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined. Individual shares are of no use on their own.

More formally, in a secret sharing scheme there is one dealer and more players. The dealer gives a secret to the players, but only when specific conditions are fulfilled. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret, but no group of less than t players can. Such a system is called a (t, n)-threshold scheme.

In a *(*t, n*)* scheme one can prove that it makes no difference whether an attacker has *t-1* valid shares at his disposal or none at all; so long as he has less than *t* shares, there is no better option than guessing to find out the secret.

Some cases of secret sharing: (See SHA Protection Plans)

• Good passwords are hard to memorize. A clever user could use a secret sharing scheme to generate a set of shares for a given password and store one share in his address book, one in his bank deposit safe, leave one share with a friend, etc. If one day he forgets his password, he can reconstruct it easily. Of course, writing passwords directly into the address book would pose a security risk, as it could be stolen. If a secret sharing scheme is used instead, the thief must steal many shares from different places.

A typical application of this scenario is the secure implementation of an encrypted backup system. Assuming data recoveries are rarely needed, backup data can be public-key encrypted; this can be done automatically and without user interaction -- while the private recovery key is protected via secret sharing.

• A dealer could send t shares, all of which are necessary to recover the original secret, to a single recipient, using *t* different channels. An attacker would have to intercept all t shares to recover the secret, a task which may be more difficult than intercepting a single message.

- The director of a bank could generate shares for the bank's vault code and hand them out to his employees. Even if the director is unavailable, the vault can be opened, but requires a certain number of employees do it together.

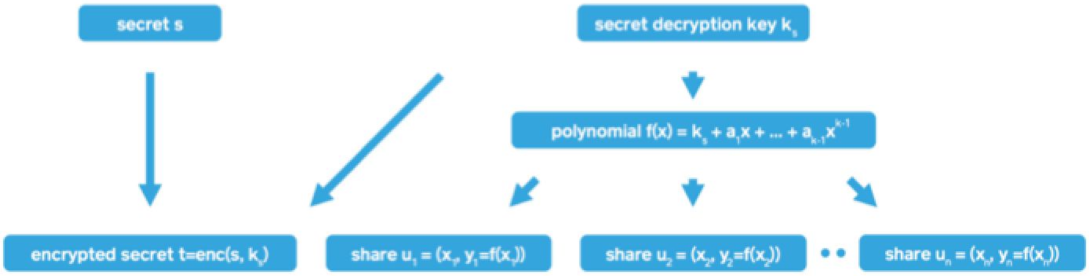

secret s
secret decryption key k_s
polynomial $f(x) = k_s + a_1x + ... + a_{k-1}x^{k-1}$
encrypted secret $t=enc(s, k_s)$
share $u_1 = (x_1, y_1=f(x_1))$
share $u_2 = (x_2, y_2=f(x_2))$
share $u_n = (x_n, y_n=f(x_n))$

Figure 8: Secret Share Principles

4.4 Two-Man Rule

The two-man rule is used in sensitive areas such as command to send nuclear missiles to prevent accidental or malicious skidding. In cryptography, Americans use the phrase "two-person integrity" (TPI) when it comes to preventing a single person from having access to cryptographic keys for secure communications (COMSEC).

This concept helps to resolve these issues of trust and security with the escrow authority. By requiring that two individuals collaborate to reveal the data in escrow, holders protect themselves from an isolated, malicious act.

For example: a holder would divide the passphrase of the escrow key and distribute the pieces to a group of trusted people called, The Family Circle (TFC). To break up the passphrase, simply distribute *N* pieces between *N* members of TFC, forcing them to meet together to use the private key escrow.

Two points are enough to define a line, three to define a parabola, four for a cubic, and so on. If now we want to share a secret, say the value 1234, between six individuals and three of them are needed to find the secret, we will randomly choose a parabola among those passing through the point (0, 1234) and we will give the coordinates of six of his/her points to these six individuals (see Figure 9).

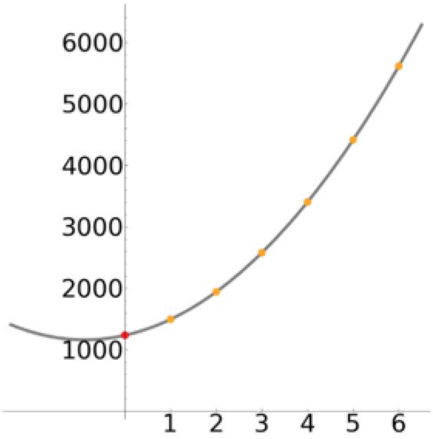


Figure 9: Parabolic Passant Couples (0, 1234) one six seen points.

If only two of them, numbers 2 and 4, came to share their coordinates, they could not find the original parabola and therefore the value of the secret point in x = 0 (see Figure 10).

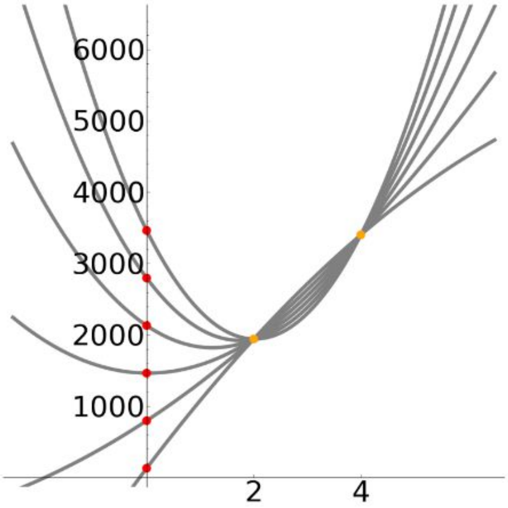


Figure 10: Parables passing through the points of the n ° 2 and 4.

Therefore, it is necessary that a third individual agrees to share his / her coordinates in order to define one, *and only one*, parable and to reveal the secret value 1234 (see Figure 11).

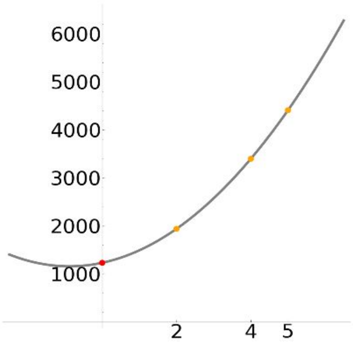


Figure 11: Only one parable can pass through the points of the 2, 4 and 5.

4.5 TFC Shares Distribution Protocol

The Family Circle is a conglomerate of members belonging to a group; this group can include family members, a company's group of stakeholders of trust, or simply a circle of friends. The TFC SDP is a protocol developed by Safe Haven in order to establish a circle of trust in our ecosystem.

If we consider our techniques described above, we have a dealer (the person that wants to protect his legacy) and n players (his children and the validator [notaries]). The dealer gives a secret to the players, but only when specific conditions are fulfilled. The dealer accomplishes this by giving each player a share in such a way that any group of *t* (for *threshold*) or more players can together reconstruct the secret but no group of less than *t* players can. Such a system is called a *(t, n)*-threshold scheme.

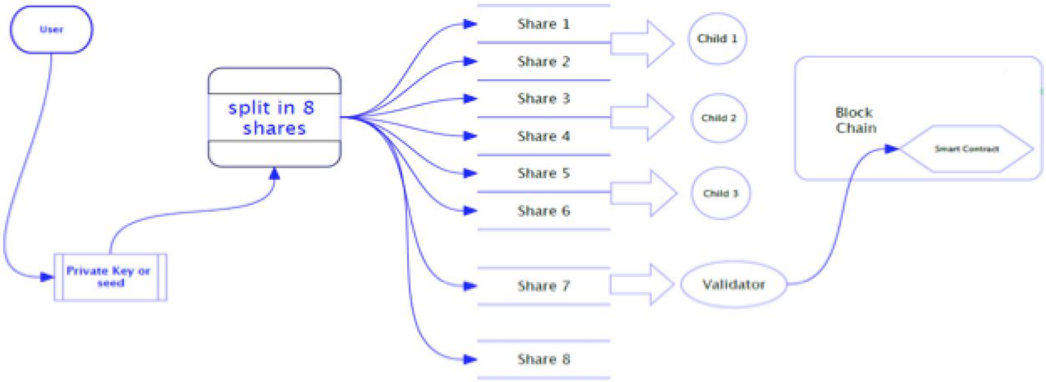


Figure 12: TFC Share Distribution Protocol

TFC SD Protocol base rules:

- The secret is split in shares (can be maximum 1024 bit).
- If you want to protect a secret larger than 1024 bits, a hybrid technique must be applied. The secret must be encrypted with a block cipher and then we apply only the secret sharing to the key (openssl and gpg are valid tools).
- The secret security level can imply an upper bound for the length, as short secrets/seeds/keys will be padded with some salt bits.
- We can use hexadecimal digits in place of ASCII characters for I/O, so binary data can be protected/split into shares as well.
- While splitting or combining the shared secret, the protocol locks its virtual address space into RAM or privacy reasons.
- The number of distributed share entities is, technically speaking, limited to 99, we limit this even further to 15, while each entity can have more than 15 but less than 99.
- The validator *y* has always -1 share less than the *n* (players/children).
- We need at the least 1 player *n* and 1 validator *y* to establish a complete network of trust in safe havens ecosystem.
- Multiple validators can be added.

4.5.1 TFCSD Case 1: 1 child and 1 validator

Based on our secret sharing scheme formula:

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

T = threshold of the minimum shares needed to reconstruct the Secret.

y = the validator of the process, in our case it's a registered member of the Safe haven's Alliance Program

X = the share holders

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

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

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

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

$$T = 1 + 2$$

$T = 3$ (Min. of shares that are needed to obtain the complete shared key).

Max of shares will be 3*:* 2 for the child and 2(-1) for the validator.

So we take for instance the secret: “My shared passphrase” we obtain the following 3 split shares.

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

As we have a share representation of 100% there is only one feasible scenario for success.

1 child = (1 x 2) and (2 – 1) validator = 3 = T

4.5.2 TFCSD CASE 2: 3 CHILDREN AND 1 VALIDATOR

Based on our secret sharing scheme formula:

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

T = threshold of the minimum shares needed to reconstruct the secret.

y = the validator of the process, in our case it’s a registered member of the Safe Haven’s Alliance Program

X = the share holders

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

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

$$T = (2.1 - 1) + (2.3)$$

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

$$T = 1 + 6$$

$T = 7$ (Min. of shares that are needed in order to obtain the shared key).

Max of shares will be 8: 6 for the children and 2(-1) for the validator

Suppose we take the secret: “My shared passphrase” and we obtain the following 8 split shares.

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

We will need 7 out of 8 to reconstruct the secret. So if we take the shares of

3 children = 3 x 2 = 6 < 7 (Valid)

2 children + 1 validator = 2 x 2 + 2-1 = 5 < T (Not Valid)
3 children + 1 validator = 3 x2 + 2-1 = 7 = T (Valid)

4.5.3 TFCSD Case 3: 3 children + fail-safe and 1 validator

Based on our secret sharing scheme formula and adding (b=x-):

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

T = threshold of the minimum shares needed to reconstruct the Secret.

Y = the validator of the process; in our case it's a registered member of the Safe Haven's Trust Alliance Network

X = the shareholders

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

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

Max of shares will be 9: 6 for the children and 2(-1) for the validator + 2 (fail-safe)

Suppose we take the secret: "My shared passphrase" and we obtain the following 9 split shares.

```
1-c6bde31ffc0b7474dcc576b0ab66cc3b09d7696a
2-aaae1588d6b7ddd80a14fac4fb68b7b7b19237f4
3-72061a3daf8af2585d139e37a095cddc35804e54
4-b158248b9dcf57d9c925287741532aa3ea5cc719
5-75516fa7eb1601e44863553254b0c99637392129
6-399bce6c6b29b04cfcf96e5292575f1670ff5b98
7-672c6a3398102ce986e62c46370861ffc6a0964c
```

```
8-1270dd67873bae0e21fba54a45e25622cbe7c7e1
9-084c327b0c9b727cd5d68210fe0000ce5da376af
```

We will need 7 out of 9 to reconstruct the secret. So, if we take the shares of

3 children (or 2 + fail-safe) = 3 x 2 = 6 < 7 (Not Valid)
2 children + 1 validator = 2 x 2 + 2-1 = 5 < T (Not Valid)
3 children (or 2 + fail-safe) + 1 validator = 3 x2 + 2-1 = 7 = T (Valid)

4.5.4 TFCSD CASE 4: 3 CHILDREN AND 2 VALIDATORS

Based on our secret sharing scheme formula:

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

T = threshold of the minimum shares needed to reconstruct the secret.

y = the validator of the process, in our case it's a registered member of the Safe Haven's Alliance Program

-1 = Fail-safe share

X = the shareholders

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

$$T = ((y.2) - 1) + (X.3)$$

$$T = ((2.2) - 1) + (3.3)$$

$$T = (4 - 1) + (9)$$

$$T = 12$$

$T = 12$ (Min. of shares that are needed in order to obtain the complete shared key)

Max of shares will be 13: 9 for the children and 4(-1) for the validator

Suppose we take the secret: "My shared passphrase" we obtain the following 13 split shares.

```
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
```

And we will need 12 out of 13 to reconstruct the secret. So, if we take the shares of

3 children = 3 x 3 = 9 < 12 (Not Valid)
3 children + 1 validator = 3 x 3 + 2 - 1 = 10 < T (Not Valid)
3 children + 2 validators= 3 x 3 + 4 - 1 = 12 = T (Valid)

4.5.5 TFC Fail-Safe Share(s)

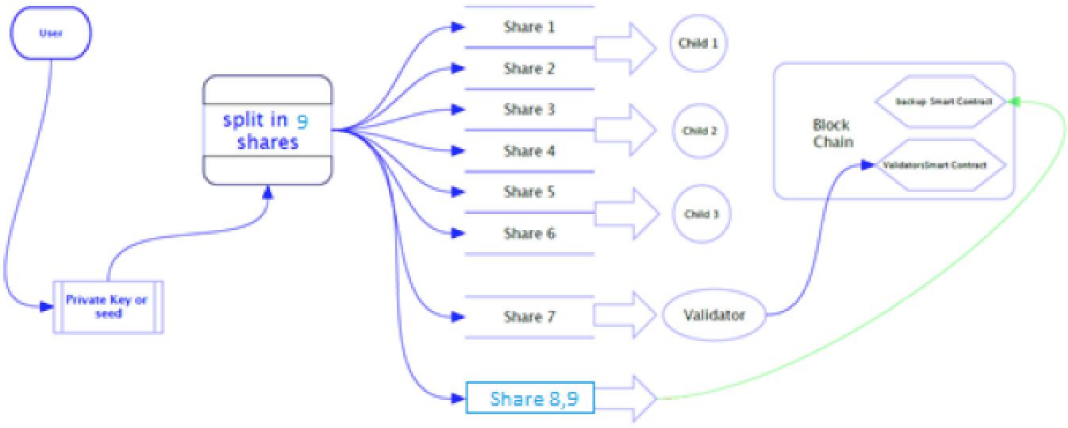


Figure 13 : TFC Fail-Safe Share

TFC SD Fail-safe Protocol:

- The remaining shares will be used as a fail-safe share.
- This can be useful in the case that of one of the *n* (players/children) lost his share, becomes unable to act, or dies.
- Our protocol provides a separate “backup” smart contract on the blockchain with different conditions written in.
- The fail-safe shares can’t be given under any circumstances, to one of the *n* (players/children) as this would jeopardize the complete operation setup by the dealer (parent), as in use case 2 (3 children + 1 validator) the children can’t construct the secret share without the validators share (through blockchain Smart Contract query) but when you give the backup shares, they will be able to do so.
- The only case where we don’t have a fail-safe share is when we need a consensus of 100% of the stakeholder, for instance the use case 1 (1 child + 1 validator)

4.6 The Validator's Share Process

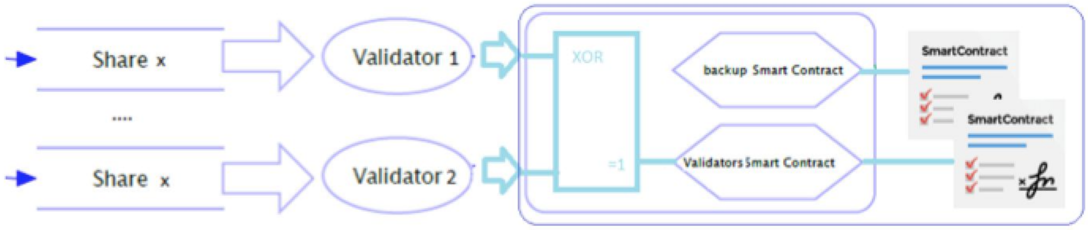


Figure 14: Validators Share Process

- The validator's share process consists of a pool of legal entity validators, which are members of our Trust Alliance Network.
- The validator does not store, own, or see the shares meant to be sent to the blockchain; their role is transparent.
- They distribute the shares to the *n* (players/children/stakeholders) in a formal way by delivering a legal certificate to *n* and validating the transaction towards the blockchain.
- The validator's share is the share of the person that initiated the process to begin with; he/she safeguards it in the blockchain via a validator in order to keep full rights of the complete secret share. His assets are his as long as he lives.
- The validator(s) is/are the only one(s) that can retrieve the share previously sent to the blockchain... If the following conditions are met:
  - The total number of shares of the *n* (players/children/stakeholders) have to be present, if not and if needed, the fail-safe share can be retrieved by the validator as well if the backup smart contract conditions are fulfilled.
  - In the case that the initiator (parent/dealer) dies, the validator must validate the rightful medical forms in order to initiate the retrieve process of the share stocked in the blockchain.
- The initiator/ parent's share is also transferable to another legitimate person when needed.

4.7 Multiple Validators Possibility

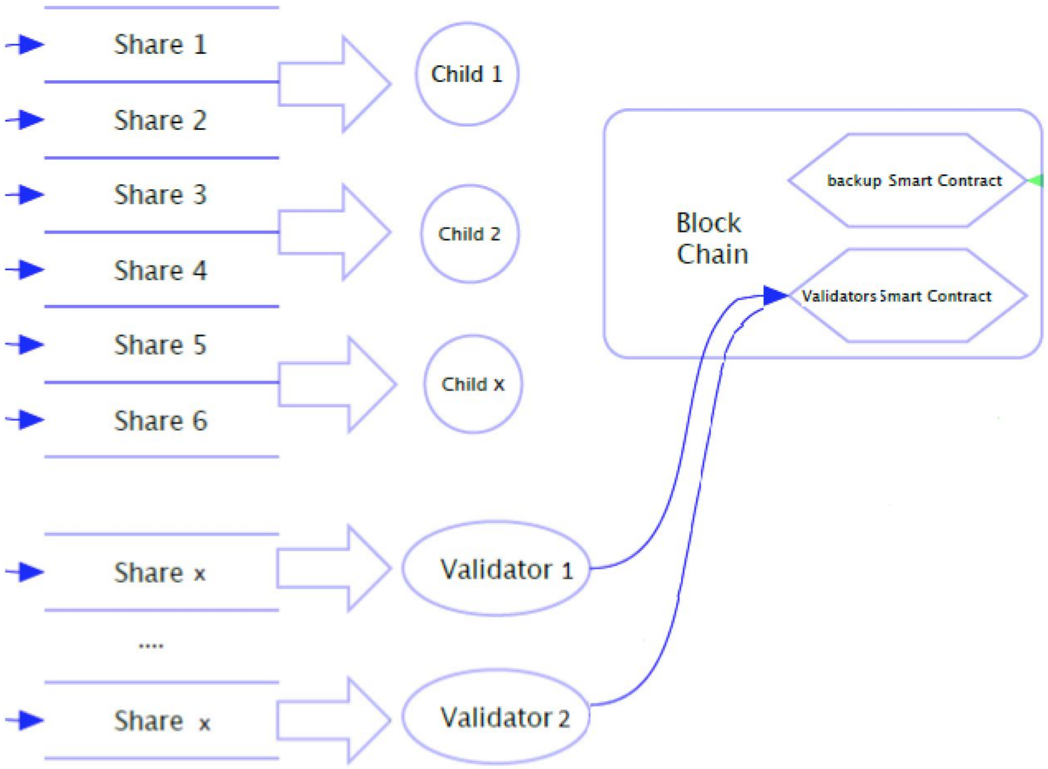


Figure 15 : Multiple Validator's Scheme

TFC SD Multiple Validators Possibility:

- No one is immortal, that's why we provide the opportunity to establish a network of trust containing more than 1 validator.
- When you chose several validators to be involved, we push a backup smart contract in the blockchain that holds the necessary shares, *n* (players/children) -1, that can be used by a second validator.
- This offers a system of security, which is completely derived from share distribution and validation.

5. SH- Trust Alliance Network

The TAN is an autonomous social networking hub for blockchain-related legal affairs. The goal is to connect lawyers and notaries that specialize in cryptocurrencies to crypto investors and enthusiasts. The TAN will become a hub for legal related blockchain information, articles, laws, etc. The TAN will be world's first legal reference for distributed ledger/blockchain applications, users, and companies.

Legal entities will be able to offer their services and highlight their fields of specialization to potential clients. A profile page will be available for each legal entity containing their contact information, remunerations details, and a short description of themselves and their services. Also, users will be able to chat between themselves and legal entities via our platform.

5.1 Articles

Blockchain law-related articles will be published on the platform, so the average contributor can stay informed. Legal entities and users will be able to share their thoughts as well by commenting on the articles.

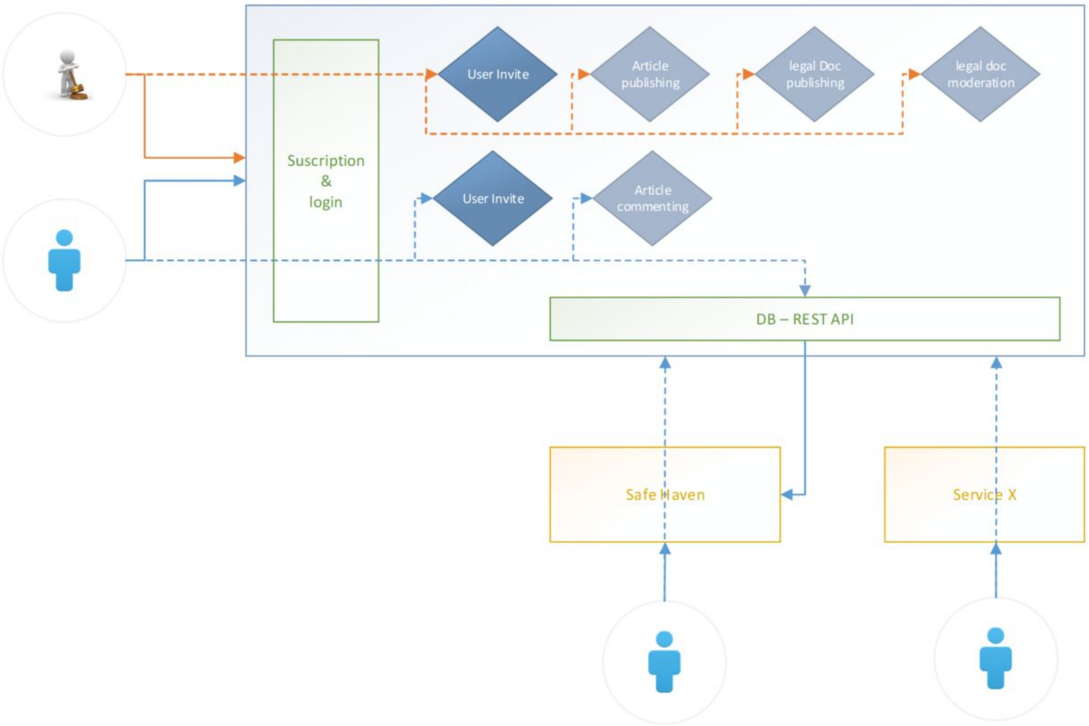
5.2 Legal documents

The TAN will be updated with legal, blockchain-related articles. The subject of these articles can range anywhere from taxes to simple regulations. Legal entities will be able to publish them and comment/upvote them. Users will also be able to comment on articles and up-vote them.

5.3 Legal Entity Profiles

The TAN will contain a profile page from each subscribed legal entity. This page will contain contact details such as the address of the Legal Entity, Remuneration details, Cost by hour, day, etc.

5.4 TAN Usage



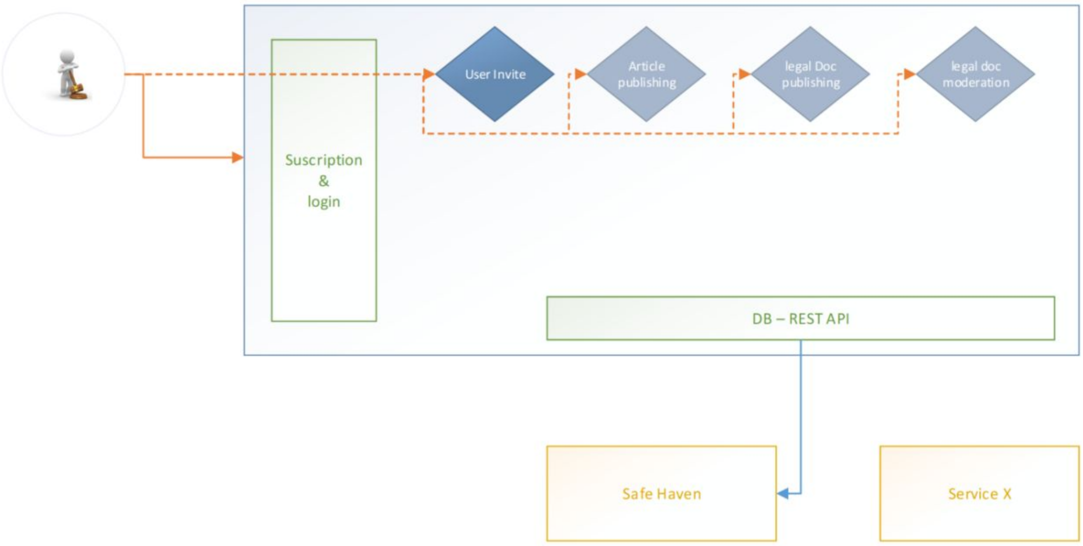
5.4.1 Legal Entity Perspective

In the TAN, Legal entities will be able to subscribe in order to sell their services to their customers. Every legal entity will have a page describing their expertise and services (prices/hours/location).

Those subscriptions will be for free, as we want to motivate them to come to our site, and it will also help the TAN's growth over time.

The goal is that those legal entities add, in their own language and for their own country, district, or state, all documentation related to crypto law, ranging from tax affairs to inheritance. The goal is that the TAN will become a sort of "wiki" for blockchain law, but only with credible documents and articles.

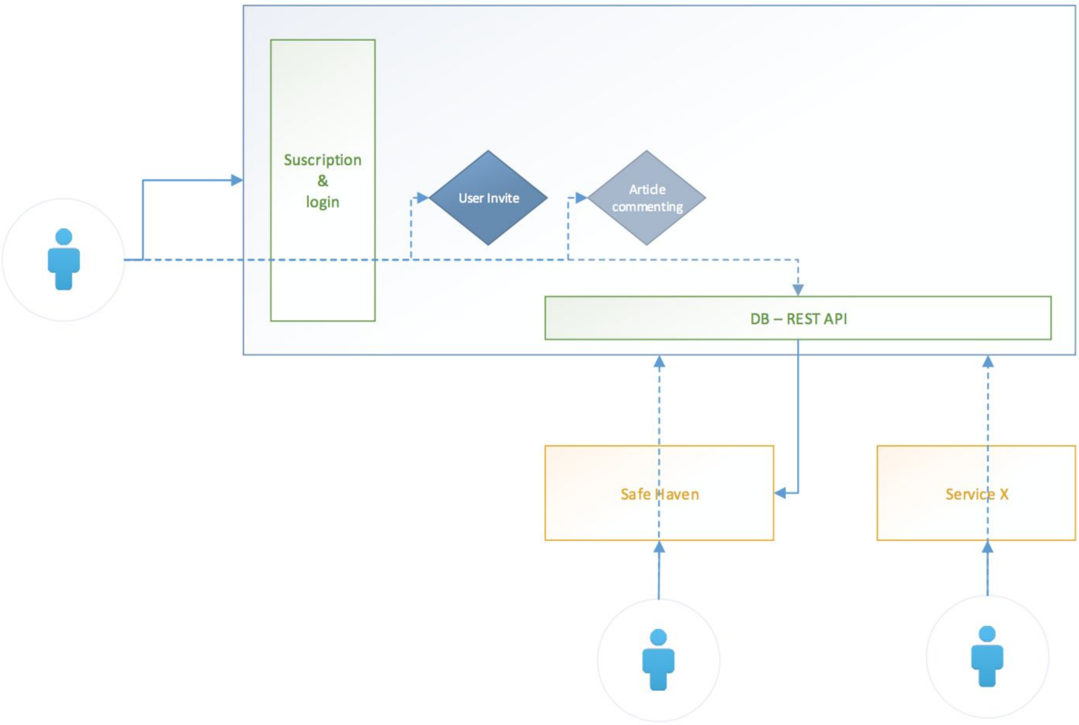
Once a service like Safe Haven becomes available on the TAN, legal entities will be able to add those services to their portfolio. The legal entity must pay an annual fee, and lock SHA tokens in order to offer Safe Haven's services to potential customers. More details will be released in the following months.



- Legal Entities can login/subscribe to the TAN free of charge
- Legal Entities can Invite other users to the TAN
- Legal Entities can comment on articles on the TAN
- Legal Entities can publish articles and legal documents (references and clarifications about crypto law)
- Legal Entities can moderate legal documents.
- Legal Entities need to pay an annual fee to offer Safe Haven's services to his/her clients.
- Legal Entities need to lock a minimum amount of SHA tokens to be able to use the Safe Haven platform

5.4.2 User Perspective

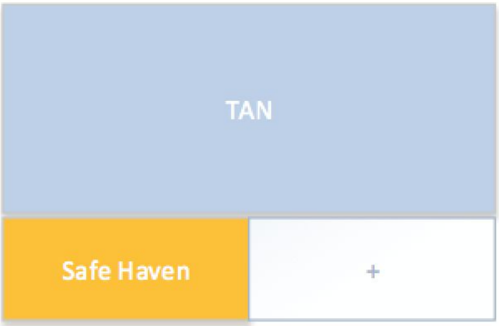
Users will be able to view legal entities' profiles and use their services to safeguard their legacy through one of Safe Haven's protection plans. Users will also be able to consult the TAN for free.



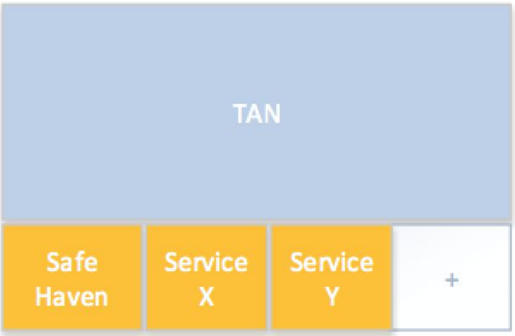
Users can sign up/subscribe on the TAN free of charge
Users can Invite other users to the TAN
Users can comment on articles on the TAN
Users can consult legal entities via Safe Haven's platform

5.5 TAN Services Integration

Safe Haven is service committed to making digital assets inheritable; they offer digital inheritance services that are completely decentralized on the blockchain with the TAN involvement. This means Safe Haven will integrate the TAN into its platform.



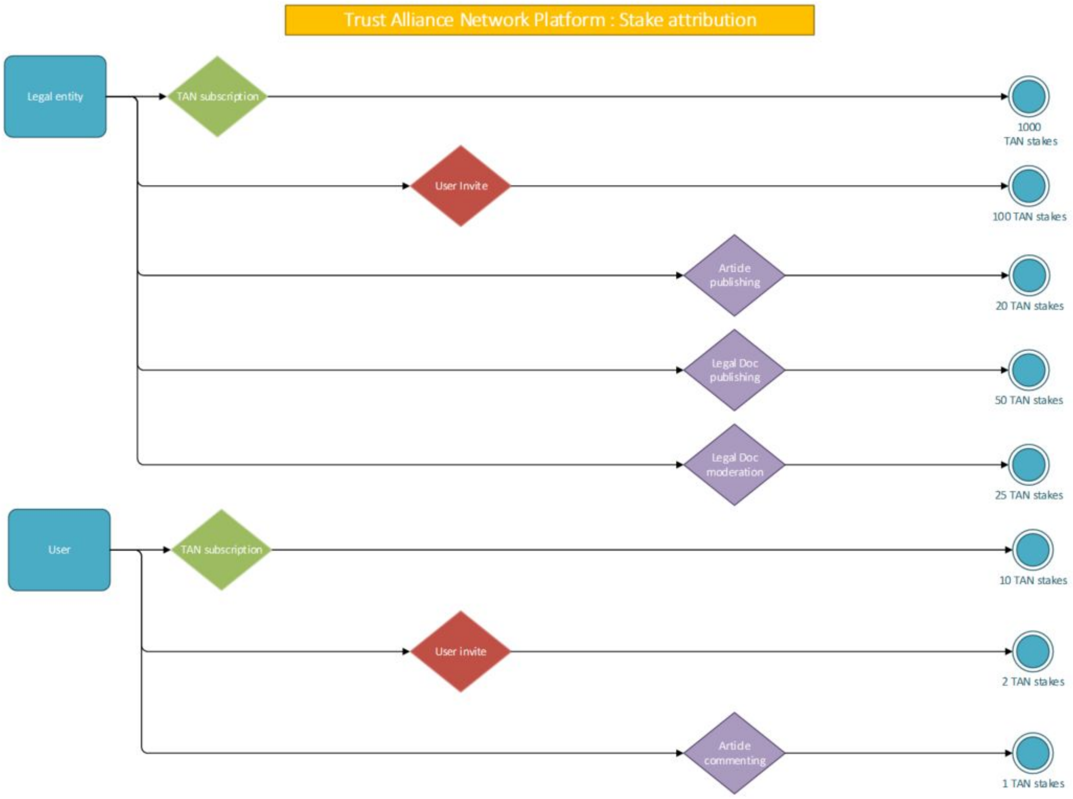
Other services not related to inheritance will be added over time. A likely example would be Identity Services and lending circles, or any other blockchain project that needs our TAN or some dispute handling.



5.6 TAN REWARDING SYSTEM

We included a rewards system (TAN Tokens) to provide for and secure the growth of the TAN over time. We grant stakes for actions performed by a legal entity and/or user on our platform. The TAN token is a minable Proof of Work token.

More details about this will become available in the next upcoming weeks/months.



https://github.com/Safehaven-io/TAN-chain

6. SHA Protection Plans

We created 4 different protection plans to serve the needs of various stakeholders.

1. The Family Circle Plan (TFC)

The Family Circle plan is for those who want- on the day they pass away, their children to be able to access their assets. The possibilities are almost endless; shares can be divided in flexible way, while safekeeping the secret in a secure and a transparent manner. The fact that we add validators in our process keeps the process suitable for the most important matters, like our families. We add the wonderful world of "block-chaining" in our process, which keeps the share decentralized. The decentralized database validator (smart contract mapping) adds an extra security feature combined with a state-of-the-art, simple, secret sharing protocol.

The advantage of this solution is that we do not store 100% of the shares on the blockchain, only a small part, depending on the different options chosen by the initiator. In order to fully understand the different shares processes and our TFC SD protocol, we kindly invite you to read our White Paper Section 5.

The release and/or execution of the shares protected by smart contracts rely on a third-party involvement, more specifically known as our Trust Alliance Network.

2. The Business Continuity plan (BCP)

The Business Continuity plan is quite similar to the TFC. The main difference is that we speak about stakeholders instead of children and that the validation process is different in terms of share unlocking. In a BCP the notary does not need medical rustication documents to obtain the missing share through our services, but rather notarial acts prepared by himself. The initiator can also choose whether to include our TAN (Trust Alliance Network) or have an entirely automated process.

3. The Investment Circle

The Investment Circle is for those willing to create a fund amongst friends, family members, or business stakeholders. For example: Five friends want to invest in crypto-currencies, and each buy in for $1000. What are their options? Creating a multi-sig wallet is not an option with all the flaws discovered lately. Even when it is completely secure, one will always need trust within the group... So how can this be fixed? Simple: through Safe Haven's Share Distribution protocol. A holder encrypts the private key and Safe Haven splits the passphrase into shares. The stakeholders will receive equally the same number of shares. If we consider this formula (without a failsafe mechanism), we have $T = (y.n - 1) + (X.n)$, T = (2 -1) + (2.5) = 1 + 10 = 11 shares to distribute where 1 will be protected on the blockchain via the validator's (legal entity) share. The conditions to liberate/release this share can be anything from price thresholds, to milestones, to simply having a 100 % consensus to do so. Again, the possibilities are endless. The group may choose whether or not they include our TAN as well.

4. Safe Haven Vault

Strong passwords are hard to memorize and cannot be transferred, not in a legal manner anyway, from a holder to his or her relatives. If you want to be sure that your digital legacy does not die with you, and that relatives can access those accounts even when after death, store them through Safe Haven on the blockchain using one of our Share distribution protocols. With Safe Haven's Vault, you have the possibility to protect any digital asset (crypto keys/seeds/passwords) on our blockchain. The release of the shares happens by the initiator him/herself, or he/she can even add a watchdog mechanism that transfers the shares to another user of our platform in an autonomous way. One example of the conditions that can be set is "keep-alive" functions. Smart contracts are triggered once the contracts are overdue and monitoring stops.

SafeHaven protection plans with third party involvement:

Description	**TFC**	**BCP**	**Investment Circle**	**SH Vault**
100% Decentralized	NO	NO	NO	YES
Full Process Automation	NO	NO	NO	YES
Third Party Involvement (TAN)	YES	YES	YES	NO
Upgradeable Smart Contracts	YES	YES	NO	YES
Proof of Stake Options	YES	YES	NO	YES

Safehaven protection plans without third party involvement:

Description	TFC	BCP	Investment Circle	SH Vault
100% Decentralized	N.A.	YES	YES	N.A.
Full Process Automation		YES	YES	
Third Party Involvement (TAN)		NO	NO	
Upgradeable Smart Contracts		YES	NO	
Proof of Stake Options		NO	NO	

7. Token Utilization

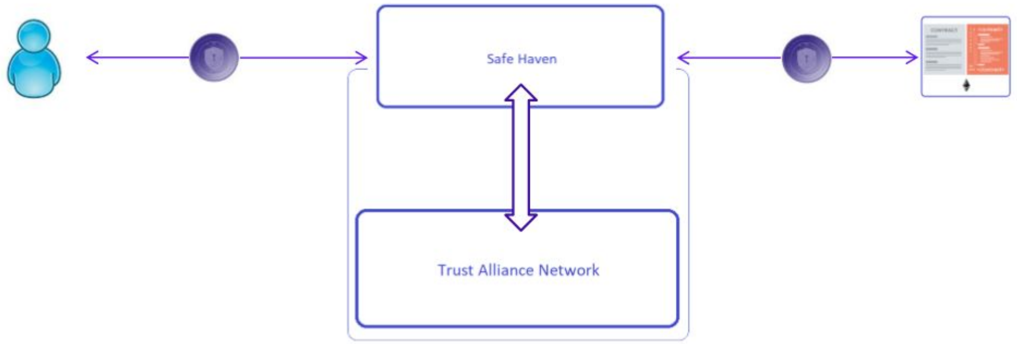
The SHA-token is an ERC20 token built on top of Ethereum. ERC20 standard was introduced on the Ethereum blockchain in order to allow developers to design decentralized apps (Dapps) to work with tokens out of the box without the need to reinvent the wheel every time a new token system is introduced. Therefore, with ERC20, anyone with an idea can deploy a product on the blockchain without having to undergo the whole process of designing the platform. With ERC20, we are able to define a common set of rules for the Ethereum-based SHA to adhere to. We can know in advance how the token will behave based on the standard. The SHA token is developed to heal the broken market we described in this white paper. The first phase of development concerns the amount of tokens we are creating. The SHA token will be used as a fuel in the process.

The TAN-token is an ERC20 token built on top of Ethereum.. The TAN token is developed to award subscribers of our TAN to comment, add documents and articles on our TAN network. The TAN token will be a minable token.

7.1 FUEL

SHA token is used as fuel for creating/executing each of the following smart contracts on the blockchain.

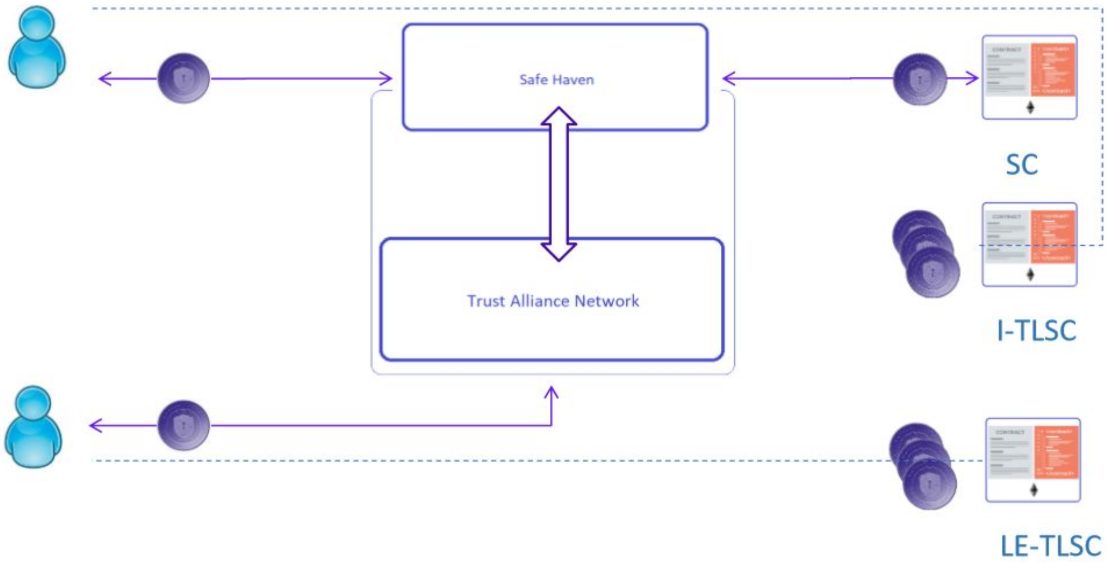
Fail Safe Share(s) Contracts
Validator Share(s) Contracts



Backup Validator Share(s) Contracts

7.2 Token Utilization

In order to use Safe Haven's Services and platform, the initiator will need to deposit SHA tokens in a time-locked smart contract (I-TLSC). The SHA tokens will be released over-time relative to the conditions written in the smart contracts after validation within our Trust Alliance Network (TAN). Those locked tokens will become inheritable as soon as the release procedure is initiated. A legal entity will need to lock more tokens than a standard user in order to use the TAN to foresee his customers with services. These tokens will be locked into Legal Entity – Time-Locked Smart Contracts.



The number of tokens that will need to be locked depend on the terms & conditions of the smart contract.

- While we lock tokens, the circulating supply will decrease so the value of the SHA DA (digital assets) will increase.

- Without the SHA DA’s, our ecosystem will not function.

- In order for legal entities to subscribe to our TAN, they must lock up a certain amount of SHA DA for 365 days.

- Locked SHA will become inheritable as soon as the conditions of the associated smart contracts are fulfilled, and by doing this SHA will become the world's first inheritable Digital Asset.

- Tokens locked for our Investment Circle will be distributed amongst all stakeholders from the moment that all associated smart contracts conditions are fulfilled.

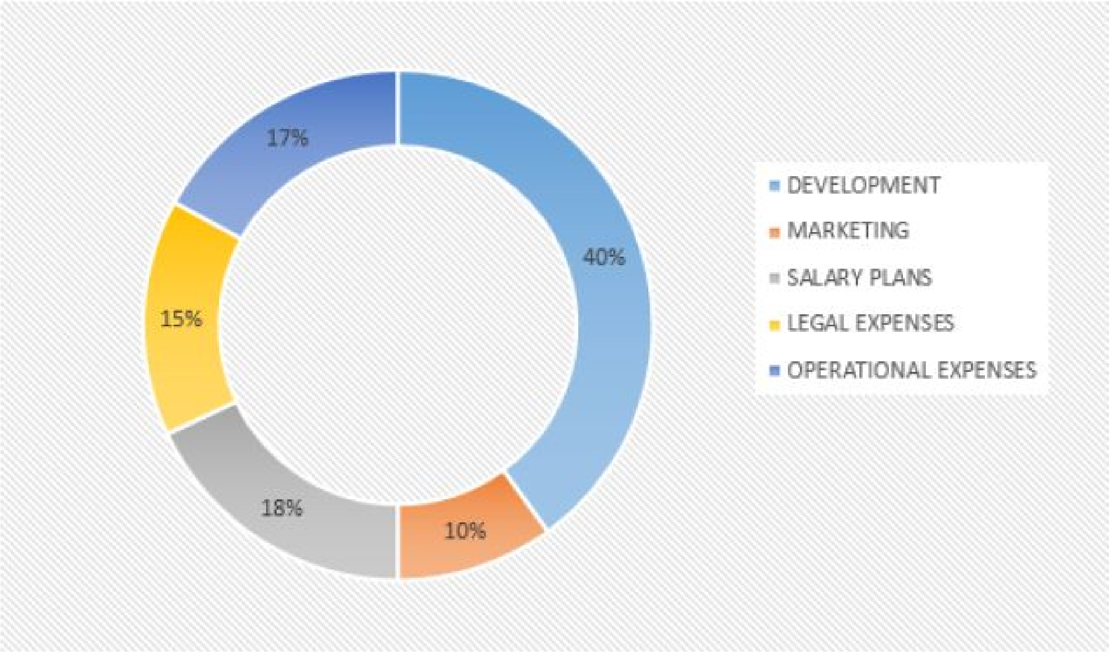
7.3 Staking

- Safe Haven is currently working on a staking solution inside our ecosystem.

- Users that have locked-up tokens will be rewarded for holding the SHA DA’s

8. Funds Allocation

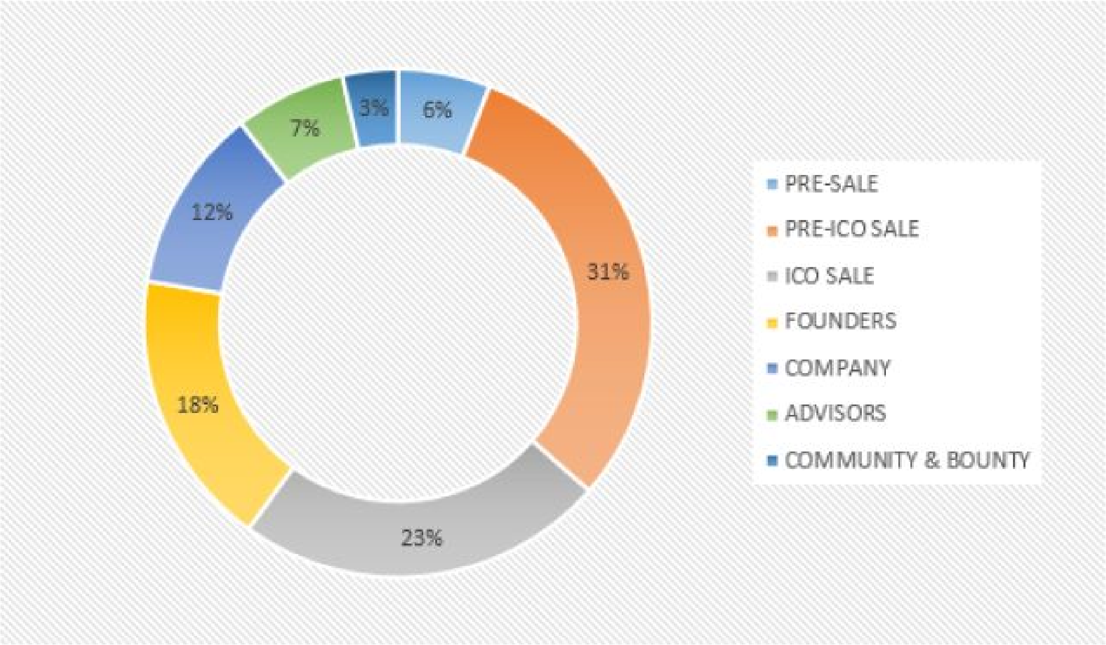
Development	40%
Marketing	10%
Salary Plans	18%
Legal Expenses	15%
Operational Expenses	17%



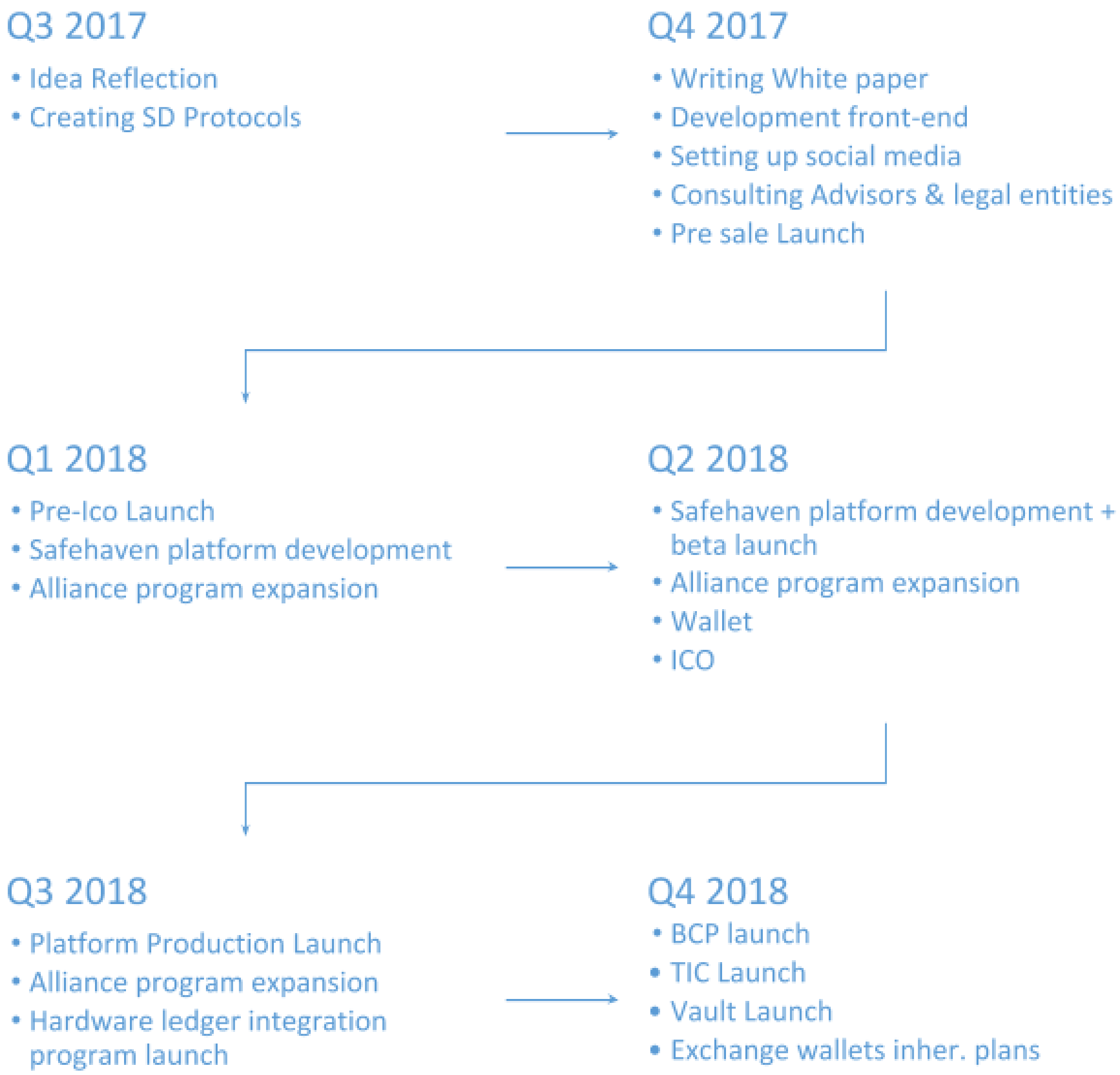
We aim to allocate a large share of funds raised to facilitate of development of the platform. Therefore, 40% of the funds will go towards this initiative. Ten percent of the funds will be allocated to facilitate various marketing activities, including bounty campaigns and signature campaigns. 15% will be allocated to legal markets like exchanges. 17% from the funds are for Operational Expenses and 18% will be allocated to Salary Plans.

9. ICO Parameters

Ticker: SHA
Total supply: 85,000,000
Ethereum Based Tokens (ERC20)
ICO Start Date: SEE https://ico.safehaven.io
Exchange rate Private Investors: 2500 SHA = 1ETH
Exchange rate presale: 2000 SHA = 1 ETH
Exchange rate ICO: 1500 SHA= 1 ETH
Minimum Cap: 3000 ETH
Maximum Cap: 25.000.000 $



10. 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

- Pre-Ico Launch
- Safehaven platform development
- Alliance program expansion

Q2 2018

- Safehaven platform development + beta launch
- Alliance program expansion
- Wallet
- ICO

Q3 2018

- Platform Production Launch
- Alliance program expansion
- Hardware ledger integration program launch

Q4 2018

- BCP launch
- TIC Launch
- Vault Launch
- Exchange wallets inher. plans