SafeHaven.io

… The Solution to digital inheritance …

Brussels, November 2017

www.safehaven.io

Written by the Safe Haven Team

Table of Contents

Table of Figures

Executive Summary

The goal of this white paper is to simplify the understanding of what SafeHaven.io is all about. This document is a technical white paper setting out the current and future developments of the Safe Haven project. This paper is solely for informative purposes, and has no intent of talking about future endeavours. Unless intently specified otherwise, the products and innovations set out in this paper are currently under development and are not currently active. We make no guarantees or representations towards the successful development or implementation of such technologies and innovations, or achievement of any other activities noted in the paper, and disclaims any warranties implied by law or otherwise. No one is liable for the contents of this paper or any inferences drawn from it, including (but not limited to) relation to any interactions with Safe Haven or the technologies mentioned in this paper. Safe Haven disclaims all liability for any loss or damage of any kind (whether foreseeable or not) which may arise from any person acting on any information and opinions relating to Safe Haven, the Safe Haven Platform or the Safe Haven Ecosystem contained in this paper or any information which is made available in connection with any further enquiries, notwithstanding any negligence, default or lack of care.

1 Introduction

Few people know, but crypto currencies emerged as a side product of another invention. Satoshi Nakamoto, the unknown inventor of Bitcoin (the first and most important crypto-currency) never intended to invent a currency to begin with.
In his announcement of Bitcoin in late 2008, Satoshi said he developed “A Peer-to-Peer Electronic Cash System. “
His goal was to invent something that many people failed to create before.
The single and most important part of Satoshi‘s invention was a decentralized digital cash system. In the nineties, there were many similar attempts to create digital currency, but they all failed.
After seeing all the centralized attempts fail, Satoshi tried to build a digital cash system without a central entity. Like a 'Peer-to-Peer Network' for file sharing.
This decision became the birth of crypto-currency. It was the missing piece Satoshi found to implement legitimate digital cash. The idea is complex and can be difficult to understand, but if you understand it, you will know more about crypto-currencies than most people. So, let‘s try to make it as easy as possible:
To sum it up, digital cash is a payment network with accounts, balances, and transactions. That part is easy to understand. One major problem every payment network must solve is to prevent "double-spending" (when one entity spends the same amount twice, with only one of those transactions reflecting a change in the account balance). This is usually done by a central server who keeps record about the balances. In a decentralized network, you don‘t have this server. So, you need every single entity of the network to do its job. Every peer in the network needs to have a list with all transactions to check if future transactions are valid or if there is an attempt to double spend.
But how can these entities keep a consensus about these records?
If the users of the network disagree about only one single, minor balance, everything is broken. They need an absolute consensus. Usually, you have a central authority to declare the correct state of balances. But how can you achieve consensus without a central authority?
Nobody knew until Satoshi emerged out of nowhere. In fact, nobody believed it was even feasible.
Satoshi proved it was possible. His major innovation was achieving consensus without a central authority. Crypto-currencies are a part of this solution – the part that made the solution thrilling, fascinating and helped it change business as we know it. Since you are reading our white paper, you have invested or are about to invest in this challenging market.

2 Concerns

Have you ever thought about how, at any second, something could happen to you? Have you ever thought about the day your family will face life without you? What about your crypto currency investments? What about those difficult markets with hundreds of private keys, exchanges and wallets? Will they ever be able to recover your investment without you? Can they trust anyone who would help them without the fear of something going wrong? Yes, they can! Safe Haven provides the solution! We are building a platform on the most popular and secure block chains so that you can stop worrying about your legacy!

3 Solution

We at Safe Haven give you the opportunity to secure your digital assets without locking yourself out. Thanks to our TFC Share Distribution Key, Escrow Protocol and the Trust Alliance program, 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 and unavoidable day that he/she should pass away, a registered member of the Trust Alliance Platform (notary) can retrieve the remaining share on the block chain to pass the investor's legacy down to his children / stakeholders.

How is this accomplished? Check out the step-by-step guide, which includes only three steps, and the techniques described further in this document.

3.1 Step-by-Step

Step 1: The 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, in order to process the necessary validation steps.

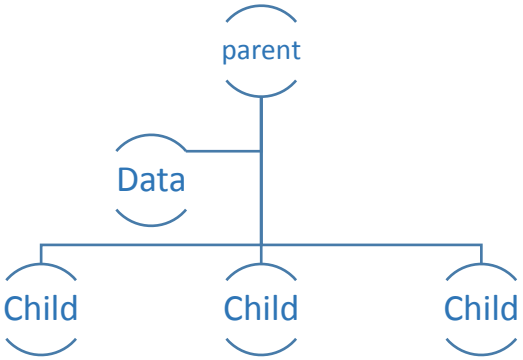


Figure 1 : The Family Circle (TFC)

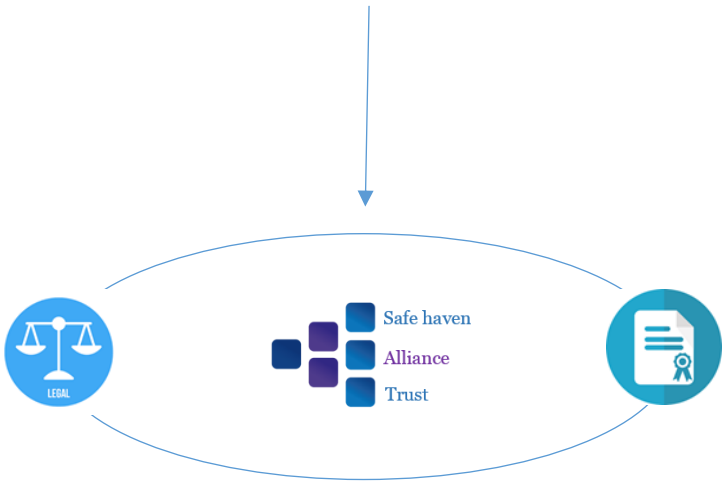


Figure 2 : The Trust Alliance Representation

Step 2: The legal entity, which is (in Safe Haven's protocol) 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 specially developed for this use. The software used for this will not keep any data in memory nor in centralized databases. Only the validators share (see the validators 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 block-chain database. This will also be the case for the backup validators (see Multiple Validators Possibility & TFC Fail-Safe Share(s)).

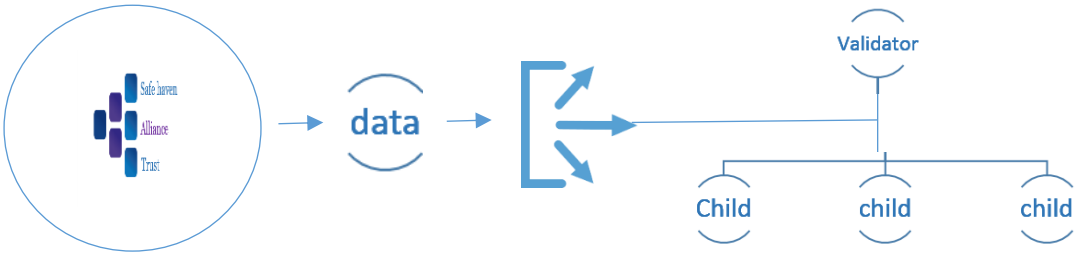


Figure 3 : Split In Shares Step

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 send to the blockchain in the form of a Smart Contract.

Figure 4 : Child Certificates

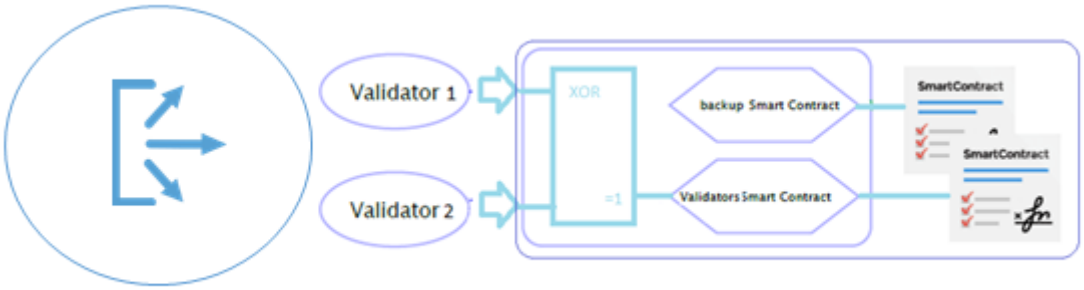


Figure 5 : Validators Process

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.

Step 4: In the case of a sudden death or in the case that the investor is not able to handle his assets on his own, the children or stakeholders can obtain the missing share by introducing the necessary legal documents to his notary. He 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 sections described further in this document.

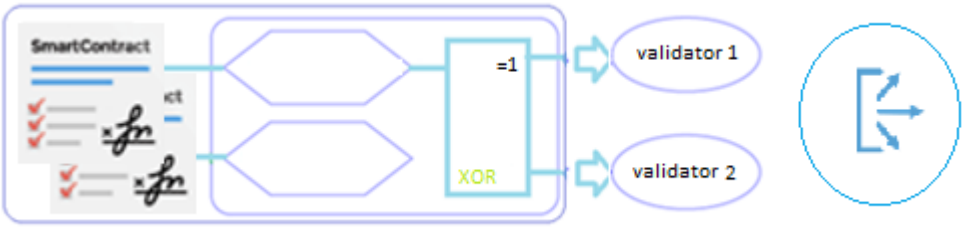


Figure 6 : Share Retrieval Process

4 Basic Principals

4.1 Blockchain

The blockchain is a software innovation for establishing digital trust between users facilitating 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.

4.2 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, with smart contract technology it can all be automated. Smart contract technology can be compared to an automated vending machine. With a vending machine, money is deposited into the machine and the desired item drops for collection, if 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.

5 Techniques & Conceptual mathematics

5.1 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.

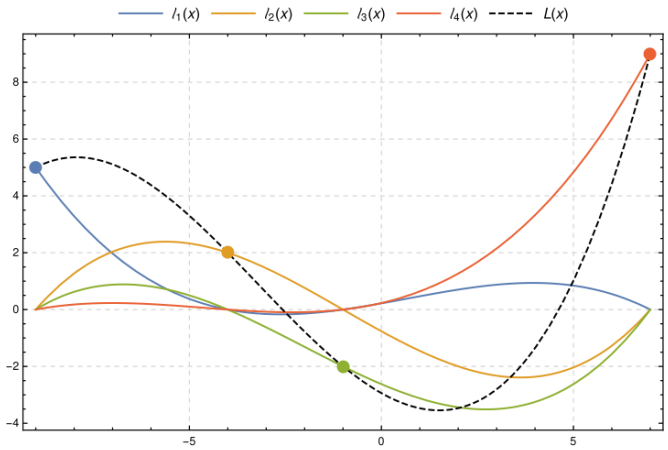


Figure 7 : Polynomials

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

5.2 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.

5.3 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 use 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 by an "enemy." If a secret sharing scheme is used, the attacker 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 unlocking code and hand them out to his employees. Even if the director is not available, the vault can be opened, but only, when a certain number of employees do it together. Here secret sharing schemes allow the employment of not fully trusted people.

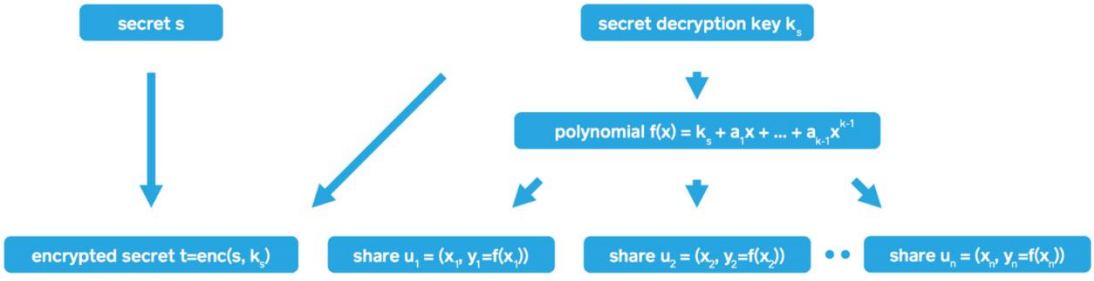


Figure 8 : Secret Share Principles

5.4 Two Man Rule

This rule (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).

So here is an interesting concept that would help us to resolve these issues of trust and security with the escrow authority. By requiring that two individuals collaborate to reveal the data in escrow, we shelter ourselves from an isolated malicious act.

Let's divide the passphrase of the escrow key and give the pieces to a group of trusted people that we call the family circle (TFC)

How to break up this passphrase? Simply distributing N pieces between the N members of the TFC forces them to meet together to use the private key escrow, but if one of them is unavailable or is precisely the missing shareholder of the TFC whose shares we want to recover.

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 points to these six individuals (see Figure9).

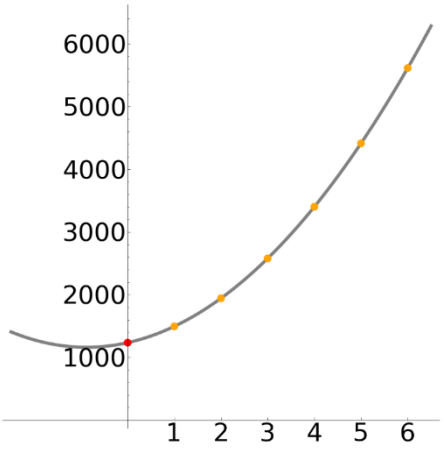


Figure 9: Parabolic Passant Couples (0, 1234) one six seen points.

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 Figure10).

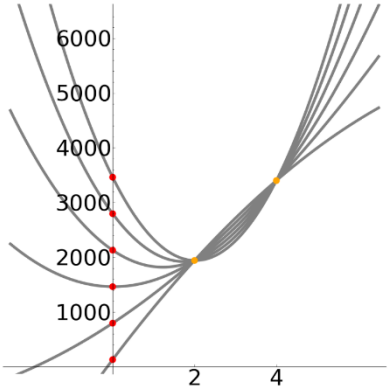


Figure 10 : Parables passing through the points of the n ° 2 and 4.

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).

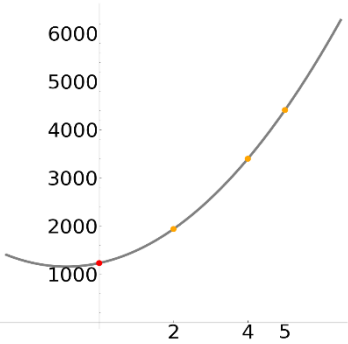


Figure 11 : Only one parable can pass through the points of the 2, 4 and 5.

5.5 TFC Shares Distribution Protocol

The family circle is, for Safe Haven, 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 eco-system.

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.

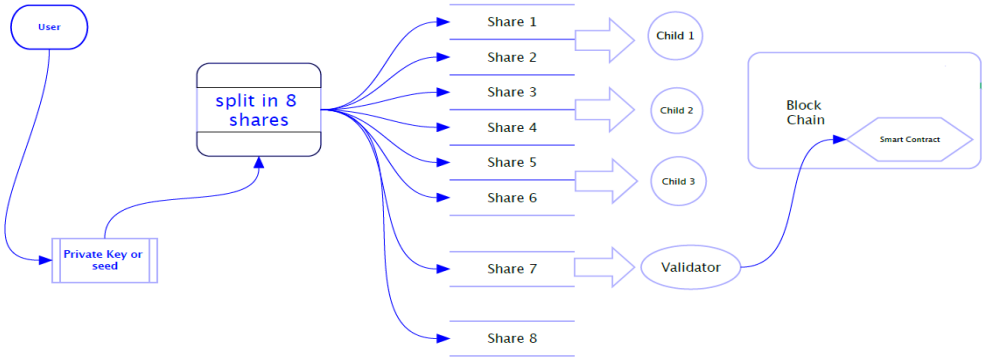


Figure 12 : TFC Share Distribution Protocol

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 eco-system.
- Multiple validators can be added.

5.5.1 TFCSD Case 1: 1 child and 1 validator

Based on our secret sharing scheme formula:

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

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) & (2 – 1) validator = 3 = T so OK

5.5.2 TFCSD Case 2: 3 children and 1 validator

Based on our secret sharing scheme formula:

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

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 complete 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
```

And 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 so NOK
- 2 children + 1 validator = 2 x 2 + 2-1 = 5 < T so not OK
- 3 children + 1 validator = 3 x2 + 2-1 = 7 = T so OK

5.5.3 TFCSD Case 2: 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 Alliance Program

X = the share holders

$T = (y.n - 1) + (X.n)$ *+ (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 so not OK
- 2 children + 1 validator = 2 x 2 + 2-1 = 5 < T so not OK
- 3 children (or 2 + fail-safe) + 1 validator = 3 x2 + 2-1 = 7 = T so OK

5.5.4 TFCSD Case 3: 3 children and 2 validator's

Based on our secret sharing scheme formula:

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

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 share holders

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

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

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

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

$T = 12$
$T = 12$ (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 so not OK
- 3 children + 1 validator = 3 x 3 + 2 - 1 = 10 < T so not OK
- 3 children + 2 validators= 3 x 3 + 4 - 1 = 12 = T so OK

5.6 TFC Fail-Safe Share(s)

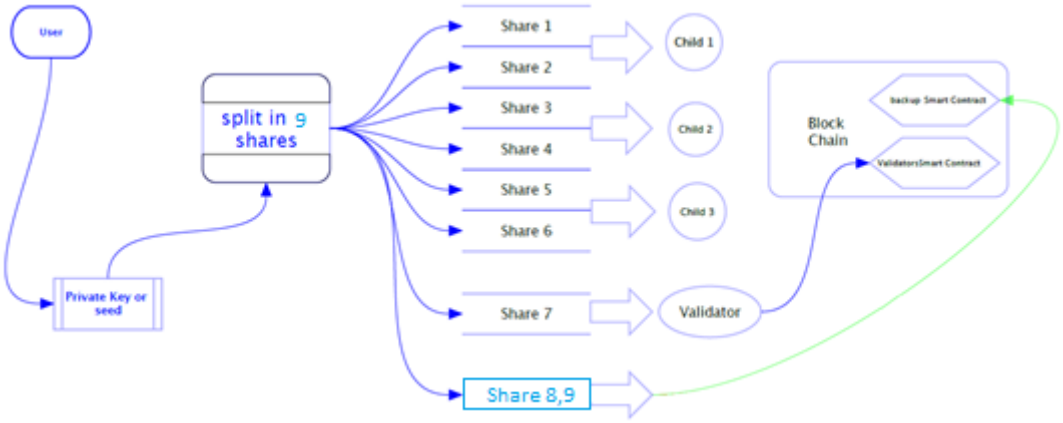


Figure 13 : TFC Fail-Safe Share

TFC SD Fail-safe Protocol:

- The remaining shares will be used a sort of "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 rightful 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

5.7 The validators share process.

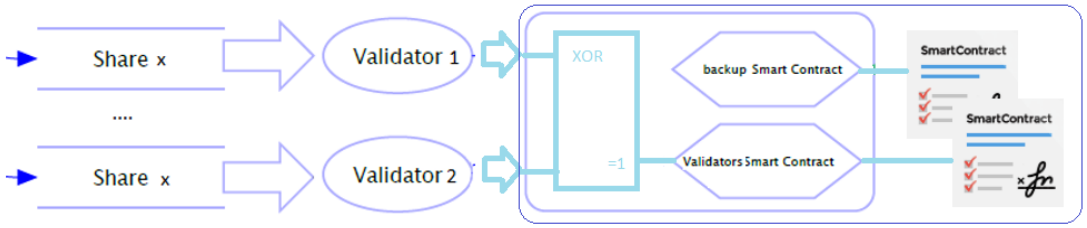


Figure 14 : Validators Share Process

- The validators 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 actually the share of the person that initiated the process to begin with; he safeguards it in the blockchain via a validator in order to keep full rights of the complete secret share, so 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.

5.8 Multiple Validators Possibility

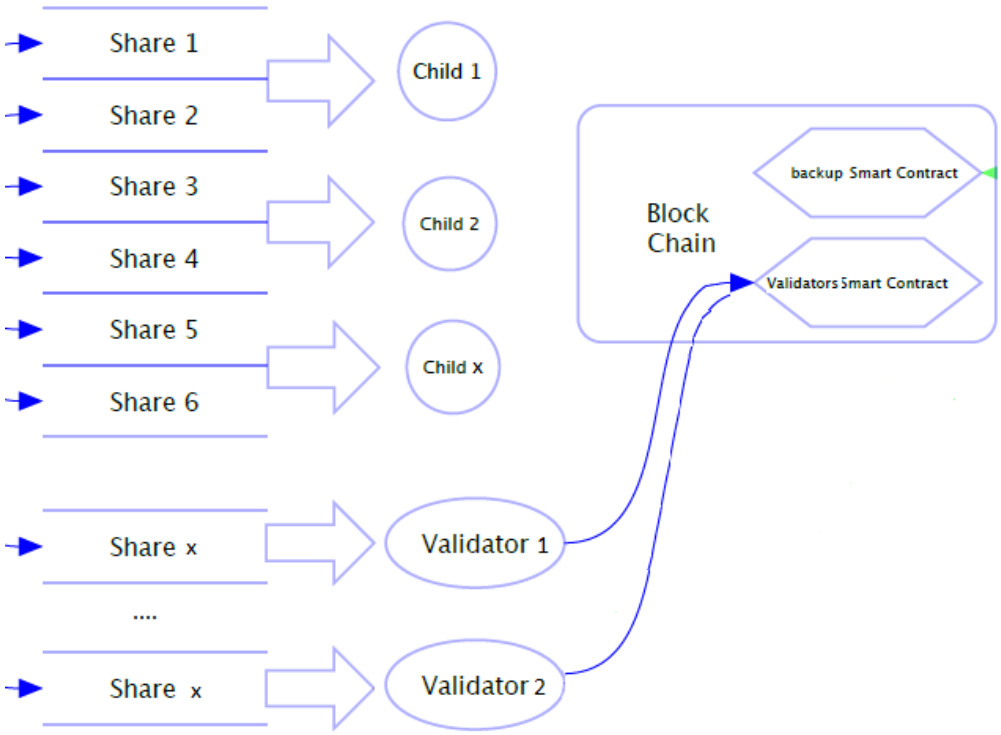


Figure 15 : Multiple Validator's Scheme

TFC SD Multiple validator's possibility:

- No one is immortal, neither are the legal entities participating in our Alliance Program. 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.
- By doing this we offer a system of security which is completely derived from share distribution and validation.

6 SH- Trust Alliance Network

Safe Haven's Trust Alliance Network is a group of legal entities which have been screened by Safe Haven in order to perform all the necessary steps to accomplish our goal, starting the future of trust by securing your assets - and by doing that reassuring your relatives, stakeholders, and your legacy.

If you are a legal entity willing to join our Alliance, please send an inquiry to info@safehaven.io and we will get in touch with you as soon as we work out our legal platform. We will be launching a dedicated trust Alliance portal very soon in order to answer all the legal questions. As soon as our portal is launched, legal entities will be able to subscribe themselves, of course legal certification documents will be asked which will help the screening process. The members will be asked to pay an annual fee to obtain a subscription to our services. The Tokens will be used as fuel to deploy the smart contracts on the blockchain.

We are currently analyzing exactly which kind of legal entities could be members of our Alliance. We need entities of trust in our Circle of trust.

7 SHA Protection Plans

1. The Family Circle Plan (TFC)

The family circle plan is for those that want to reassure their relatives who want- on the day they pass away, their children to be able to access the assets acquired by the parent. The possibilities are almost endless, shares can be divided in flexible way, while safekeeping the secret in a secure and a transparent way. The fact that we add validators in our process keeps the process familiar for important matters like the ones that we want to help secure. We add the wonderful world of "blockchaining" 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, still simplistic, secret sharing protocol.

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. This process plan is currently being developed internally and will come available for use from the moment the Trust Alliance portal is online. BCP can be useful for the distribution of multi-sig wallets, exchanges, or simple for safekeeping of import passwords/passphrases.

3. The Investment Circle

The Investment Circle is for those willing to create a fund amongst friends, family members or business stakeholders. Let's say that 5 friends want to invest in crypto-currencies, and buy each for $1000. What are their options? Creating a multi-sig wallet (with all the flaws that were discovered lately). Even when it's completely secure, you will always need trust within the group... Ok, how are we going to manage this? Simple! Through Safe Haven Share Distribution protocol. You encrypt the private key and we split the passphrase into shares, the stakeholders will receive equally the same number of shares. If we consider the formula without a fail-safe mechanism, we have $T = (y.n - 1) + (X.n)$, T = (2 -1) + (2.5) = 1 + 10 = 11 shares to distribute where 1 will be stocked on the blockchain via the validator (legal entity). The conditions, in order to liberate this share, can be anything from price thresholds, to milestones, to simply having a 100 % consensus to do so. Again, the possibilities are endless.

4. Safe Haven Vault

Good passwords are hard to memorize and can't be transferred, not in a legal manner anyway, from you to your relatives. This password can be anything, from Facebook, to Gmail or any other important account. If you want to be sure that your digital legacy doesn't die with you, that your relatives can access those accounts even when you are not there anymore, store them through Safe Haven on the blockchain using one of our Share distribution protocols.

8 Conclusion

Investing in crypto-currency and Bitcoin today takes a lot of time and is very challenging, on the other hand it will bring massive profits over the years. Securing those assets and being able to protect them against any treat from the outside is something all traders and long term investors have been asking for since a very long time. We are all in this business for the same reason, be financial independent and build a safe and secure future for our relatives. That is why we will develop our decentralized platform and provide our solution worldwide. The Safe Haven Company will make a difference in securing and storing your digital keys or seeds. Building a solution like Safe Haven will bring peace in mind for the investor and their relatives. We hope that you are convinced about our platform and solutions, and that we can welcome you as one of our contributors!

9 Market

Crypto-currencies are digital assets that use cryptography, an encryption technique, for security. Crypto-currencies are primarily used to buy and sell goods and services, though some newer crypto-currencies also function to provide a set of rules or obligations for its holders. They possess no intrinsic value; in that they are not redeemable for another commodity, such as gold. Unlike traditional currency, they are not issued by a central authority and are not considered legal tender.

At this point, use of crypto-currencies is largely limited to “early adopters.” For scale, there are around 10 million Bitcoin holders worldwide, with around half holding Bitcoin purely for investment purposes. Objectively, crypto-currencies are not necessary because government-backed currencies function adequately. For most adopters, the advantages of crypto-currencies are theoretical. Therefore, mainstream adoption will only come when there is a significant tangible benefit of using a crypto-currency. So, what are the advantages to using them?

Crypto currency Exchanges

Crypto-currency exchanges are websites where individuals can buy, sell, or exchange crypto-currencies for other digital currency or traditional currency. The exchanges can convert crypto-currencies into major government-backed currencies, and can convert crypto-currencies into other crypto-currencies. Some of the largest exchanges include Poloniex, Bitfinex, Kraken, and GDAX, which can trade more than $100 million (equivalent) per day. Almost every exchange is subject to governmental anti-money laundering regulations, and customers are required to provide proof of identity when opening an account.

Instead of exchanges, people sometimes use peer-to-peer transactions via sites like LocalBitcoins, which allow traders to avoid disclosing personal information. In a peer-to-peer transaction, participants trade crypto-currencies in transactions via software without the involvement of any other intermediary.

Crypto currency Wallets

Crypto-currency wallets are necessary for users to send and receive digital currency and monitor their balance. Wallets can be either hardware or software, though hardware wallets are considered more secure. For example, the Ledger wallet looks like a USB thumb drive, and connects to a computer's USB port. While the transactions and balances for a Bitcoin account is recorded on the blockchain itself, the private key used to sign new transactions is saved inside the ledger wallet. When you try to create a new transaction, your computer asks the wallet to sign it and then broadcasts it to the blockchain. Since the private key never leaves the hardware wallet, your Bitcoins are safe, even if your computer is hacked. Still, unless backed up, losing the wallet would result in the loss of the holder's assets. In contrast, a software wallet such as the Coinbase wallet is virtual. This type of software device can place the holder's funds online in the possession of the wallet provider, which has added risk.

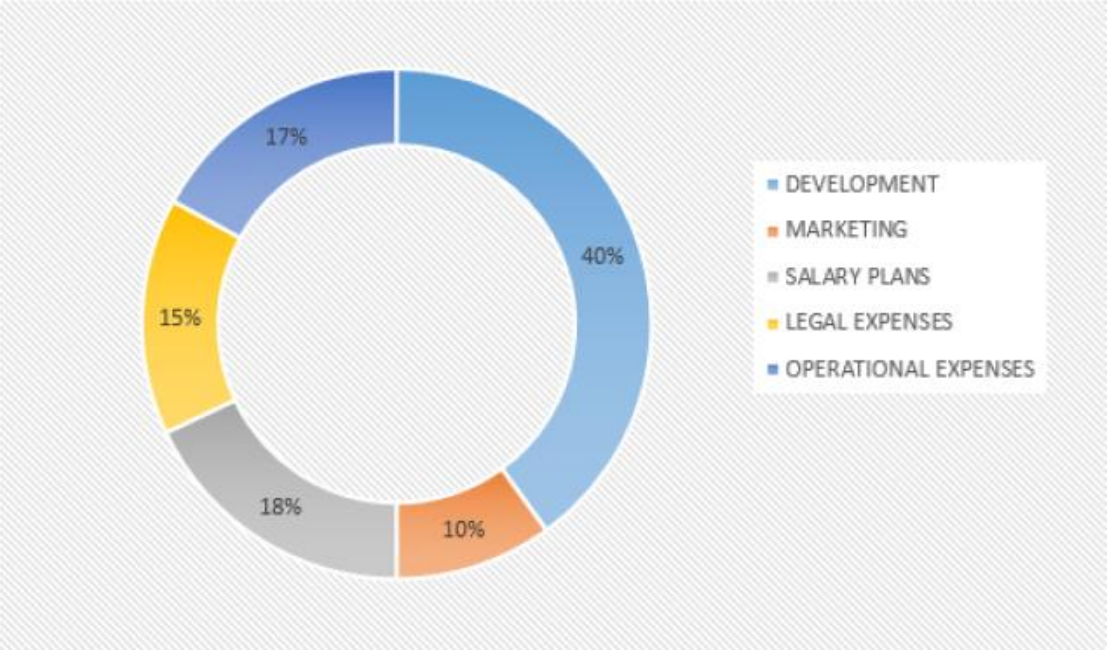
With more people and more money flowing into the crypto-currency market, more people have to open exchanges or wallets and get private keys. Safe Haven is building the perfect solution. Basically, every person that opens a wallet and buys a crypto currency can be a Safe Haven client. Our potential to grow in this market is huge! We are confident that Safe Haven will make a difference.

10 Token

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 whitepaper. 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.

11 Funds Allocation

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



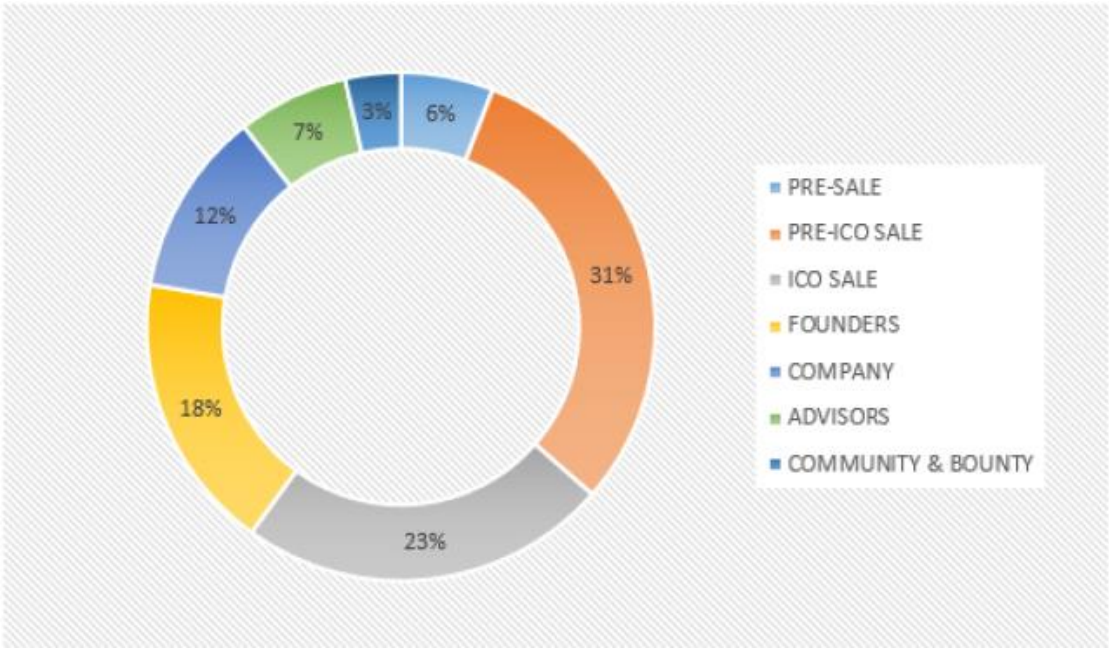
We aim to allocate a large share of funds raised to facilitate of development of the platform. Therefore, 40% of the funds will go towards this initiative. 10% of the funds will be allocated to facilitate various marketing activities, including bounty campaigns and signature campaigns. 15% will be allocated to legal markets like exchanges. 17% from the funds are for Operational Expenses and 18% will be allocated to Salary Plans.

12 ICO Parameters + Token Allocation

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

Token Allocation

PRE-SALE:	2500 SHA/ETH TOTAL (5,000,000 SHA)	6%
PRE-ICO SALE:	2000 SHA/ETH TOTAL (26,000,000 SHA)	31%
ICO SALE:	1500 SHA/ETH TOTAL (20,000,000 SHA)	23%
FOUNDERS:	15,000,000 SHA	18%
COMPANY:	10,000,000 SHA (Locked for 12 months)	12%
ADVISORS:	6,000,000 SHA	7%
COMMUNITY & BOUNTY:	3,000,000 SHA	3%



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
Q2 2018
• Safehaven platform development + beta launch
• Alliance program expansion
• Wallet
Q3 2018
• Platform Production Launch
• Alliance program expansion
• Hardware ledger integration program launch
Q4 2018
• (will be published once available on safehaven.io site)