



# SafeHaven.io

.....让资产得以继承.....

布鲁塞尔, 2017年11月

[www.safehaven.io](http://www.safehaven.io)

# 目录

---

目录.....	2
图表目录.....	3
执行纲要.....	4
1 概述.....	5
2 关注点.....	6
3 解决方案.....	6
3.1 分步操作.....	7
4 基本原则.....	10
4.1 区块链 .....	10
4.2 智能合约 .....	10
5 数学技巧与概念.....	11
5.1 多项式插值法.....	11
5.2 密钥第三方代管 .....	12
5.3 密钥共享 .....	12
5.4 二人法则 .....	14
5.5 家族圈份额分配协定.....	16
5.5.1 家族圈份额分配案例1：1名子女与1位验证人 .....	17
5.5.2 家族圈份额分配案例2：3名子女与1位验证人 .....	18
5.5.3 家族圈份额分配案例：3名子女+安全保护计划与1位验证人.....	19
5.5.4 家族圈份额分配案例3: 3名子女与2位验证人 .....	20
5.6 家族圈安全保护份额 .....	21
5.7 验证人份额流程.....	22
5.8 多验证人可能性.....	23
6 安全天堂联盟计划.....	24
7 安全天堂联盟保护方案.....	25
8 结论 .....	27
9 市场 .....	27
10 代币.....	28
11 资金分配.....	29
12 首次代币公开发售参数+代币分配.....	30
代币分配 .....	30
13 路线图 .....	31

## 图表目录

---

图1: 家族圈 (TFC) .....	7
图2: 信任联盟表述 .....	7
图3: 份额拆分步骤 .....	8
图4: 子女证书 .....	9
图5: 验证人流程 .....	9
图6: 份额检索流程 .....	9
图7: 多项式 .....	11
图8: 密钥共享原则s .....	13
图9: 一条能看到6个点的过点 (0,1234) 抛物线的右侧 .....	14
图10: 经过2号和4号坐标的抛物线 .....	15
图11: 同时经过点2、4和5的唯一一条抛物线 .....	15
图12: 家族圈份额分配协定 .....	16
图13: 家族圈安全保护份额 .....	21
图14: 验证人份额流程 .....	22
图15: 多验证人体制 .....	23

## 执行纲要

---

本白皮书旨在让您快速了解SafeHaven.io。作为一份技术白皮书，该文本对安全天堂项目的现状及未来发展做出了表述。本白皮书仅供参考用，不是对未来意图的一种表述。除明确表述外，本文所述产品及创新目前均处于开发阶段，尚未投入使用。对于这些技术及创新的成功开发与利用，或本文所提及的任何其他活动的成就，我们不做出任何保证或表述，也放弃做出法律所默认的任何保证或至法律许可范围内的任何保证。任何人都无权依赖本文内容或依据其得出的任何推论，包括与安全天堂的任何互动或本文所提及技术有关的任何内容或其推论。安全天堂拒绝对可能因任何人依据与安全天堂、安全天堂平台或本文所包含的安全天堂生态系统，或通过任何进一步询问获得的任何信息有关的任何信息及意见采取的行动所造成的任何类型（无论是否可预见）的损失或损害承担任何责任，即便是出于任何过失、疏忽或粗心造成的。

# 1 概述

伴随人类的又一次创新，加密货币问世了，尽管了解它的人寥寥无几。中本聪，一个不为人知的全球第一种且仍然是最重要的一种加密货币 - 比特币的发明者，从未打算发明一种货币。

2008年年底，中本聪在自己的比特币声明中宣称开发了“一种点对点电子货币体系。”

数字货币出现前，中本聪的目标是完成许多人没完成的大发明。他发明的关键之处在于找到了构建一种去中心化数字货币体系的方法。上世纪90年代，许多人就一直试图创造数字货币，但都失败了。

看到所有中心化尝试失败后，中本聋试图建立一种无中心实体的数字货币体系，类似于用于文件共享的一个点对点网络。

做出这种尝试的决定使加密货币得以诞生。中本聪发现，没有加密货币就无法创建数字货币。其原因与技术相关，较为复杂，但如果弄清楚了，您对加密货币的了解就会比绝大多数人更为深刻。那么，就让我们尝试把原因尽可能简单地阐述如下吧：

要创建数字货币，您需要一个包含账户、余额与交易的支付网络。这不难理解。每个支付网络必须解决的一个主要问题是防止所谓的重复付款：即防止一个实体将同一笔金额付款两次。通常，对重复付款的防止是由记录余额的中心服务器完成的。

但在一个去中心化网络中，您不会设置这个服务器。那么就需要网络中的每个实体完成这项工作。网络中的每个节点都需要建立一份包含每笔交易的清单，以便确认后续交易是否有效或是否可能出现重复付款。

但如何才能保持这些实体对余额记录的一致认可呢？

即便网络中的节点对一笔较小的余额未达成一致意见，系统也将陷入瘫痪。因此，所有节点需对余额记录绝对地达成一致意见。通常，您会再一次使用中央权威宣布正确余额。但没有中央权威的情况下，您怎样才能实现所有实体对余额的一致认可呢？

中本聪出现前，没人知道该怎么办。事实上，大家都认为这是不可能做到的。

但中本聘认明了这是可以实现的。其主要创新在于实现了无中央权威条件下所有实体对余额的一致认可。作为该解决方案的组成部分，加密货币让方案令人欣喜、充满吸引力，也帮助方案获得了全世界的认可。看过我们的白皮书后，您就会投资或打算投资这个充满挑战的市场了。

## 2 关注点

---

您想过有一天自己会面临重大变故，或您已为自己的身后事做过打算吗？想过有一天，家人将不得不面对没有您的生活吗？想过自己的加密货币投资该如何处理、家人要如何应对那些需要数百把专属密钥、数百次交易和数百个钱包才能完成的繁琐交易、家人是否具备在失去您的情况下收回投资的能力、是否能在不担心犯错的情况下，信任可能愿意帮助他们的任何人吗？是的，他们能够做到这一切。因为安全天堂提供了解决方案。我们正在最流行且最安全的区块链技术基础上，建立一个平台/生态系统。这样您就无需再为自己的遗产担忧了。

## 3 解决方案

---

为了保护您的数字资产，安全天堂为您提供亲自参与保护自己数字资产的机会。我们的家族圈份额分配密钥第三方代管协定和信任联盟计划，让种子/专属密钥/通行短语能以一种透明而安全的方式在利益相关者或子女中共享。

协定分配份额的方式是：发起人对其资产享有完全权利。在发起人不幸去世的那一天，信任联盟平台的注册会员（公证人）可以检索发起人在区块链上的余下份额，以便将他/她的遗产交予其子女/利益相关者。

那么我们是如何完成这一过程的呢？请查看分步操作指南和本文后面内容中所描述的使用技巧。指南包含3个步骤。

### 3.1 3.1 分步操作

第1步: 用户决定保护自己的遗产（加密资产），并计划采用安全天堂安全及透明的区块链解决方案，将其种子/专属密钥/通行短语分配给三名子女。该过程发起人与我们信任联盟计划的一位注册会员取得联系。信任联盟计划是一个合法实体的群组，为执行必要验证步骤而与安全天堂建立了互信关系。

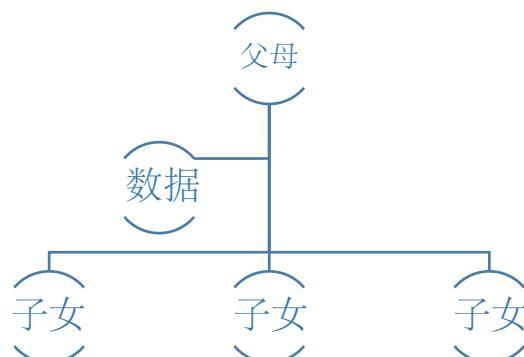


图1: 家族圈 (TFC)

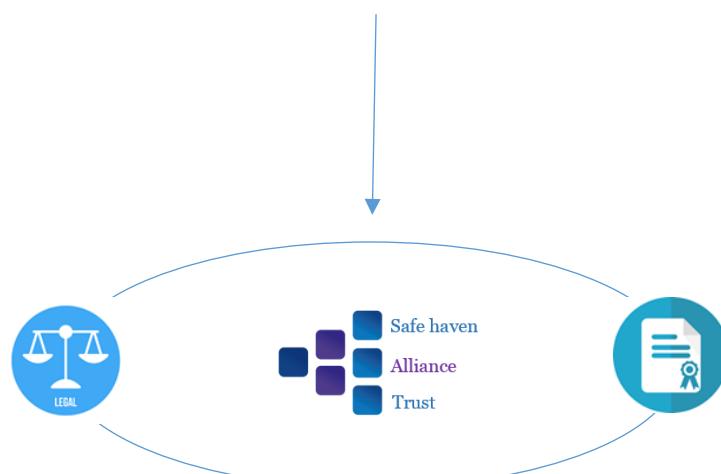


图2: 信任联盟表述

第2步：合法实体，即安全天堂协定中的验证人对数据进行拆分，以便保护获得的份额，并使用安全天堂专门为此开发的应用程序，将获得的份额分配给发起人子女（参见家族圈份额分配协定）。用于此过程的软件将不会在本地或中心数据库中存储任何数据。只有验证人份额（参见验证人份额流程）会被发送至区块链。出于显而易见的安全原因，用于份额加密及解密的安全算法将不会在份额借助智能合约完成配置前被公开。安全天堂将只建立一套映射关系，对验证人身份及智能合约进行识别。映射关系将被配置在去中心化区块链数据库中，这也是对验证人的备份（参见多验证人可能性与家族圈安全保护份额）。

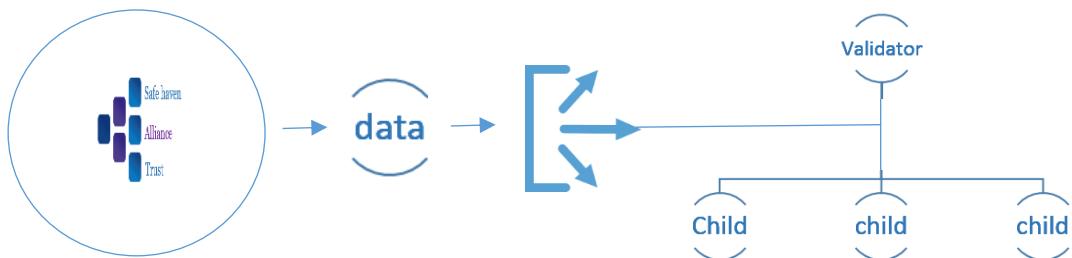


图3：份额拆分步骤

第3步：公证人将份额以法律证书形式协调分配给子女。受到保护、来源于父母/发起人的份额将经过安全天堂应用程序加密（只供信赖联盟会员使用）后，以智能合约形式发送至区块链。



图4：子女证书

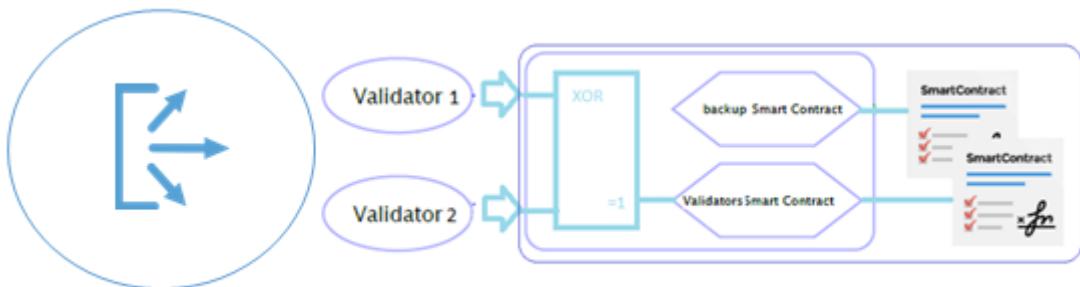


图5：验证人过程

在我们的协定中创建证书及/或整合硬件分类账，即可对子女份额进行共享。为了实现子女份额共享，我们目前正在依据自己的硬件分类账制定详细操作方法。由于项目仍处于首次代币公开发售阶段，因此详细操作方法还未公布。

第4步：如果发起人突然死亡或无法再自行管理其资产，子女或利益相关者可以向公证人提交必要法律文件，以此获得遗失份额。子女或利益相关者将可以在经过安全天堂验证后，检索区块链中的遗失份额。

我们的协定还处理安全保护份额及设置备份验证人的可能性，要了解更多详情，请查看本白皮书后面内容中描述的我们的家族圈安全保护份额及多验证人可能性。

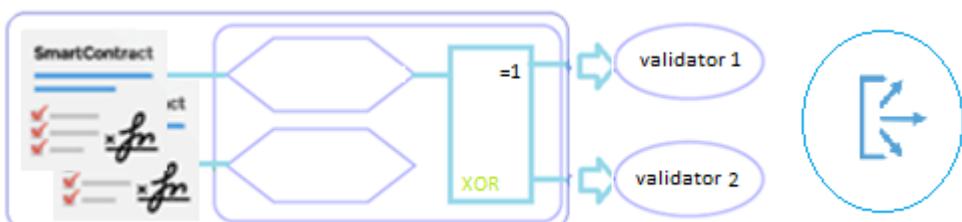


图6：资产份额检索流程

## 4 基本原则

### 4.1 区块链

区块链是一种软件创新，用于建立用户间的数字信任并促进通过网络的价值交易。区块链可以实现信赖在整个网络中的分配，而无需中央中间商对价值的数字交易进行追踪、验证及认可。目前，中央中间商的信赖授权做法对私有及政府机构的架构形成了支持，但现实正在证明这种结构是投入巨大、效率低下且不堪一击的。作为一种去中心化分配数据库运行的区块链，在解决这些问题的同时，保持了被称为区块的记录列表的持续增长。

### 4.2 智能合约

链上计算机代码或智能合约都是计算机协定，用于构成非必要性合约条款，促进、验证或强制合约的执行。智能合约通常效仿合约条款的逻辑性，以一种透明、无冲突的方式实现资金、资产、股票或任何价值物品的交易，而无需中间商提供服务。一般而言，一次产品或服务的交易不仅需要向中间商、政府代理机构、银行、律师或公证人支付费用，还需要耗费一段时间进行处理。但借助智能合约技术，所有这一切都可以自动完成了。智能合约技术堪比自动售货机技术。对于一台售货机而言，当您把钱放入售货机后，只要您放入的金额是正确的，售货机就会释放您想买的商品，让您拿到它。与此类似，使用智能合约时，资金将被存入区块链中的第三方托管机构，用于收取转账代币（如房屋产权数字证书）。代币会在条件满足时，即时转移至对方账户。智能合约不仅以与传统合约定义条款及条件的相同方式，定义了协议条款和条件，还强制执行了协议义务。

## 5 数学技巧与概念

### 5.1 多项式插值法

多项式可用于近似复杂曲线，例如版面排印中给定一些点的字母形状。与多项式相关的一种应用是将其用于自然对数及三角函数的求职：选取一些已知数据点创建一张查找表，并在这些数据点中插入值。这会使计算速度得到极大地提升。

定义：

已知 $n + 1$ 个数据点 $(x_i, y_i)$ ，且其中的 $x_i$ 均各不相同。现要求具有以下性质，且最多有 $n$ 个解的一个多项式 $p$ ：

$$p(x_i) = y_i, \quad i = 0, \dots, n.$$

该式的唯一可解性表明这样一个多项式 $p$ 是存在且唯一存在的，它可以通过如下所描述的范特蒙德矩阵得到证明：

该定理表述为，对于 $n + 1$ 个插入节点 $(x_i)$ 而言，多项式插值定义了一条线性平分线：

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

此处的 $\Pi_n$ 是有最多 $n$ 个解的多项式的向量空间（基于包含节点的任何区间得出的定义）

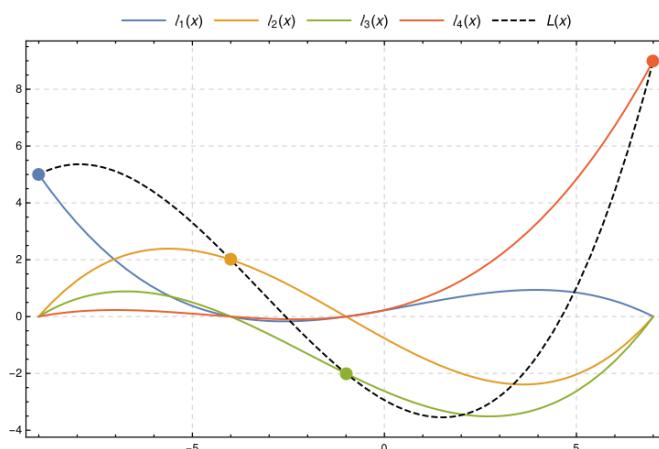


图7：多项式

多项式插值法也构成了数值积分、常微分方程数值、保密多方计算及密钥共享体制算法的基础，而密钥共享体制就是我们为实现数字资产保护这一目标而采用的方法。

## 5.2 密钥第三方代管

---

我们都不会永生，在我们死后获得数字遗产，这会是件憾事。份额持有人意外身故可能会是重建完整通行短语所面临的一个问题。在该白皮书中，我们将继续以家族圈或朋友为例进行说明，以便突出案例的差异所在。针对此问题的一种解决方案就是所谓的密钥第三方代管。密钥第三方代管让第三方得以“依据特定条件”获得这些份额。但谁是第三方、依据的条件有哪些以及如何让我们对第三方的道德及技术充满信心呢？代管权威必须能安全保证代管密钥的机密性。首先，我们应对要保护的数据加密。数据可以是一个专属密钥，也可以是采用安全加密算法，如SHA256-512并同时使用了一个通行短语的种子。那么，通行短语就可以依据我们的家族圈份额分配协定被划分为多个份额并进行分配了。

## 5.3 密钥共享

---

在密码学中，密钥共享体制是一种方法，用于在参与者群组中分配密钥。每位参与者经过分配获得密钥的一个份额。密钥仅可在份额合并后得到重构，个体份额是无法依靠自身重构密钥的。

更通俗地表达就是，一种密钥共享体制包含一个管理者和多个参与者。管理者只有在满足特定条件时，才会将密钥分配给参与者。通过以特定方式将密钥的一个份额分配给每位参与者，管理者完成密钥分配。而特定方式是指包含t个（门限）或更多个参与者的任何群组合并可重构密钥，不足t个参与者的任何群组合并不能重构密钥。这样一种体系被称为 $(t, n)$ -门限机制。

在一个  $(t, n)$  门限体制中，我们可以证明无论是一个拥有  $t-1$  个可任意支配有效份额的攻击者，还是一个完全无份额的攻击者都是不能重构密钥的。只要其份额不足  $t$  个，那他除了通过猜测找出密钥外别无他法。

密钥共享的使用案例：（参见安全天堂保护方案）

- 安全性高的密码都难以记住。一个聪明的用户可以使用一种密钥共享体制，得出适用于给定密码的一组密钥份额，并将一个份额存储在自己的地址簿中，一个存储在自己的银行保险箱中，一个交由朋友存储等。如果某一天他忘记了自己的密码，那么他可以轻松重构。当然，直接把密码写在地址簿中可能存在安全风险，因为地址簿可能会被“不怀好意的人”偷走。而密钥共享体制的使用，会使攻击者不得不为了重构密钥而从不同的地方偷走多个密钥份额。

对加密备份系统实施保护就是这种情况的一个典型应用。假设只有在极少数情况下才需要对数据进行恢复，那么备份数据可以是经过加密的公共密钥 – 这一过程不仅可以在无需用户参与的情况下自动完成，而且专属恢复密钥还能通过密钥共享得到保护。

- “一个管理者可以使用  $t$  个不同渠道，向一个接收者发送  $t$  个份额，而原始密钥的恢复需要的是所有份额。一名攻击者必须截获全部  $t$  个份额才能恢复密钥。与截获一条信息相比，这项任务可能要困难得多。”
- 银行行长可以将用于解锁银行金库代码的密钥分为多个份额，并将这些份额分配给不同雇员。即便行长不到场，金库也可能被打开，但唯一条件是需要一定数量的雇员共同打开。银行密钥共享体制让银行可以聘用并不完全信任的人作为雇员。

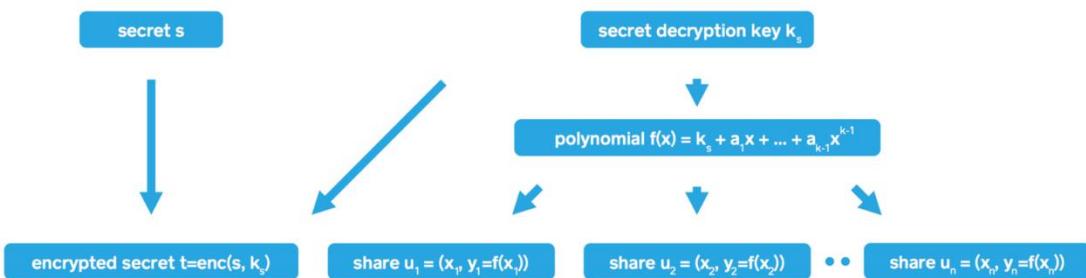


图8：密钥共享原则

## 5.4 二人法则

该法则（二人法则）用于敏感情况，如命令发射核导弹，目的是防止核导弹的偶然或蓄意发射。当说到防止个人获取用于安全通讯的密钥（COMSEC）时，美国人使用密码学中的“二人完整”（TPI）这一表达。

于是这里就出现了一个有趣的概念，它会帮助我们解决代管权威的信任和安全问题。借助要求两个人合并才能使代管数据得以显现，我们得以让自己规避一种独立的恶意行为。

让我们把代管密钥的通行短语进行拆分，并将其份额交给一群值得信赖的人。我们将这群人成为家族圈（TFC）。

那如何拆分这个通行短语呢？那就是简单将通行短语分为N份，再把它们分给家族圈中的N个成员，迫使这些成员在一起时才能使用专属密钥代管。但如果他们中的一个不在，或恰好我们想要恢复密钥的家族圈中的一位份额持有人失踪，那怎么办呢？

两点确定一条直线，三点确定一条抛物线，四点则确定一个立方体，以此类推。如果现在我们希望由六个人共享一个密钥，比如密钥值为1234，并要求他们中的三个人找到密钥，那我们会从经过点（0,1234）的抛物线中随机选择的一条抛物线上，给这6个人每人一个坐标（参见图9）。

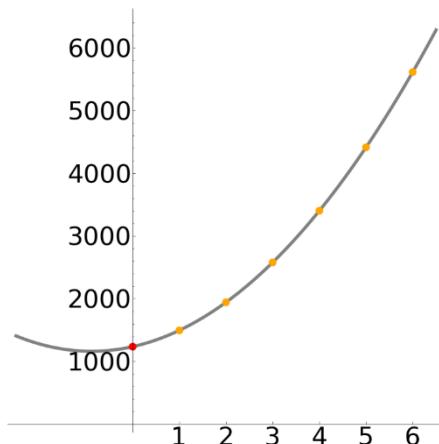


图9：一条能看到6个点的过点  
(0,1234) 的抛物线的右侧

如果只有两人，如2号和4号来共享自己的坐标，那么他们无法确定原始抛物线，因此密钥点的坐标 $x=0$ （参见图10）。

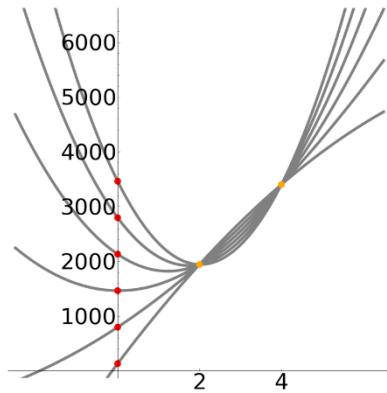


图10：经过2号和4号坐标的抛物线

因此，需要有第三个人同意共享自己的坐标，以便确定唯一的一条抛物线，并让密钥值1234得以显现（参见图11）。

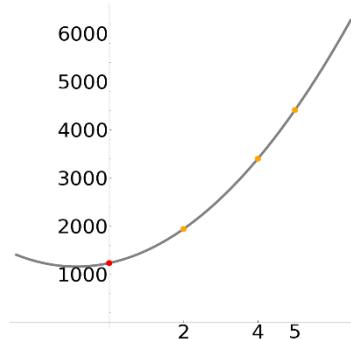


图11：同时经过点2、4和5的唯一一条抛物线

## 5.5 家族圈份额分配协定

家族圈是安全天堂对同属于一个群组的一群成员的称谓。该群组可以包括家庭成员、一家公司相互信任的利益关系人群组或只是一个朋友圈。家族圈份额分配协定是安全天堂开发的一个协定，目的是在我们的生态系统中建立一个信任圈。

考虑以上所描述的技巧，我们设置了一个管理者（希望保护其遗产的人）和n个参与者（管理者的子女和验证程序[公证人]）。管理者在特定条件得到满足时，将密钥分配给参与者。借助以特定方式分配给每位参与者一个密钥份额，管理者完成密钥分配。而这种特定方式就是包含t个（门限）或以上参与者的任何群组合并后可重构密钥，而参与者不足t个的任何群组无法合并重构密钥。这样一个系统被成为  $(t, n)$  门限体制。

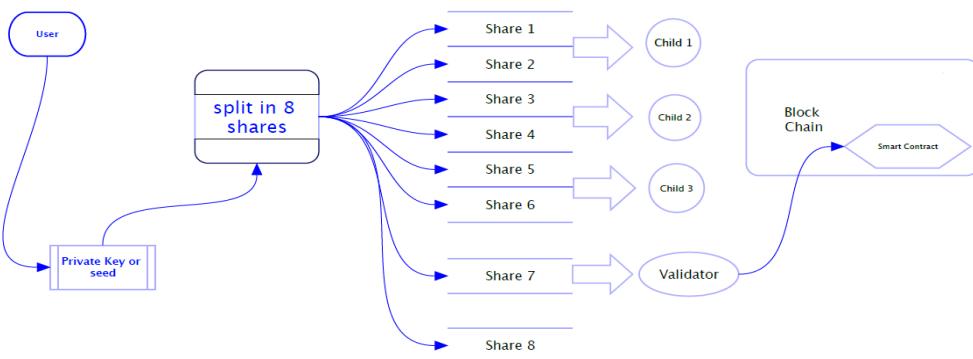


图12：家族圈份额分配协定 TFC SD 家族圈份额分配协定的基本法则：

- 用于份额拆分的安全密钥最大可为1024比特；
- 如果您希望保护的密钥大于1024比特，就必须使用混杂技术，借助分组密码加密密钥，且我们只能对该分组密码实行密钥共享（openssl与gpg都是有效工具）；
- 由于短密钥/种子/密码都包含有部分盐值，因此密钥安全等级对密钥长度具有更强的制约性；
- 我们可以将美国信息交换标准代码字符的十六进制数字用于输入/输出，这样二进制数据也能受到保护/拆分为份额；
- 在拆分或合并共享密钥时，协定会因为隐私原因而将虚拟地址空间锁定在随机存取存储器中；
- 就技术而言，获得份额分配的实体数量不会大于99个。我们可以将该数量进一步缩减至15个，且每一实体可以拥有份额的数量会介于15至99之间；
- 验证人y始终比n（参与者/子女）少1个份额；
- 我们至少需要n个参与者中的1个参与者和y个验证人中的1个验证人才能在安全天堂生态系统中建立一个完整的信任圈；
- 可以添加多个验证人。

### 5.5.1 家族圈份额分配案例1：1名子女与1位验证人

按照我们的密钥共享体制公式：

$$T = (y \cdot n - 1) + (X \cdot n)$$

T = 重构密钥所需的最少份额门限。

Y = 过程验证人，在我们的案例中，它是安全天堂联盟计划的一位注册会员

X = 份额持有人

$$T = (y \cdot n - 1) + (X \cdot n)$$

$$T = (y \cdot 1 - 1) + (X \cdot 1)$$

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

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

$$T = 1 + 2$$

T = 3 (为了获得完整共享密钥所需的最少份额；最大份额将是3 (2份给子女，

2 (-1) 份给验证人。)

因此以密钥“我所共享的通行短语”为例，我们获得了以下三个拆分份额：

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

由于我们有一种份额的完整表述，因此只有一种可行的情况是成功的：

- 所以1名子女 = (1x2) & (2-1) 验证人=3=T是成功的。

## 5.5.2 家族圈份额分配案例2: 3名子女与1位验证人

---

按照我们的密钥共享体制公式:

$$T = (y \cdot n - 1) + (X \cdot n)$$

T = 重构密钥所需的最少份额门限。

Y = 过程验证人，在我们的案例中，它是安全天堂联盟计划的一位注册会员

X = 份额所有人

$$T = (y \cdot n - 1) + (X \cdot n)$$

$$T = (y \cdot 1 - 1) + (X \cdot 3)$$

$$T = (2 \cdot 1 - 1) + (2 \cdot 3)$$

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

$$T = 1 + 6$$

$T = 7$  (为获得共享完整密钥所需的最少份额。最大份额将是8 (6份给子

女, 2 (-1) 份给验证人

因此以密钥“我所共享的通行短语”为例，我们获得了以下8个拆分的份额:

```

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

```

我们需要将以上8个中的7个用于重构密钥。因此，如果我们采用的份额是:

- 3名子女 =  $3 \times 2 = 6 < 7$  是不成功的
- 2名子女 + 1位验证人 =  $2 \times 2 + 2 - 1 = 5 < T$  也是不成功的
- 3名子女 + 1位验证人 =  $3 \times 2 + 2 - 1 = 7 = T$  是成功的

### 5.5.3 家族圈份额分配案例2: 3名子女+安全保护计划与1位验证人

按照我们的密钥共享体制公式并加上 ( $b=x$ ) :

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

$T$  = 重构密钥所需的最少份额门限。

$Y$  = 过程验证人, 在我们的案例中, 它是安全天堂联盟计划的一位注册会员

$X$  = 份额所有人

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

$$T = (y \cdot 1 - 1) + (X \cdot 3) + (b = x)$$

$$T = (2 \cdot 1 - 1) + (2 \cdot 3) + (b = 2)$$

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

$$T = 1 + 6 + 2$$

$T = 7$  (为获得所共享的完整密钥所需的最少份额。最大份额将是9 (6份给子女, 2 (-1) 份给验证人+2份 (安全保护份额))

所以以密钥“我所共享的通行短语”为例, 我们获得了以下9个拆分份额:

```
1-c6bde31ffc0b7474dcc576b0ab66cc3b09d7696a
2-aaaе1588d6b7ddd80a14fac4fb68b7b7b19237f4
3-72061a3daf8af2585d139e37a095cddc35804e54
4-b158248b9dcf57d9c925287741532aa3ea5cc719
5-75516fa7eb1601e44863553254b0c99637392129
6-399bce6c6b29b04cfcf96e5292575f1670ff5b98
7-672c6a3398102ce986e62c46370861ffc6a0964c
8-1270dd67873bae0e21fba54a45e25622cbe7c7e1
9-084c327b0c9b727cd5d68210fe0000ce5da376af
```

我们需要将9个中的7个份额用于重构密钥。因此如果我们采用的份额是:

- 3 名子女 (或2名 + 安全保护份额) =  $3 \times 2 = 6 < 7$  是不成功的
- 2 名子女 + 1 位验证人 =  $2 \times 2 + 2 - 1 = 5 < T$  也是不成功的
- 3名子女 (或 2名 + 安全保护份额) + 1位验证人 =  $3 \times 2 + 2 - 1 = 7 = T$  是成功的

## 5.5.4 家族圈份额分配案例3：3名子女和2位验证人

依据我们的密钥共享体制公式：

$$T = (y \cdot n - 1) + (X \cdot n)$$

T = 重构密钥所需的最少份额门限。

Y = 过程验证人，在我们的案例中，他是安全天堂联盟计划中的一位注册会员

-1 = 未保存份额

X = 份额所有人

$$T = (y \cdot n - 1) + (X \cdot n)$$

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

$$T = ((2 \cdot 2) - 1) + (3 \cdot 3)$$

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

$$T = 12$$

T = 12 (为了获得完整共享密钥所需的最少份额。最大份额将是13 (9份给子女, 4 (-1) 份给验证人)。

因此以密钥“我所共享的通行短语”为例，我们得到了以下13个拆分份额：

```
01-b8d792946afa60b35d53609c03ae96320b78a0f6
02-92769c90836c393d06675d4e25201c3cc2ac0a85
03-9968d3d6e953590dc15363fc92acea7464eb2053
04-92a5e10da6dae5a4353ec755a5febba76023c0fb
05-c0afccce07c511436f83db4c3a7aeaf5f69aa44f
06-a47453a4cd7b887f82df30ccdf864cc91467e738
07-3a95ee802152c02045cb1dc9aa2843291497a19c
08-82e043652371d0e9972520dade32660c6bc6d504
09-d0db492e80b8ebf2a5498867ebf91413864aa73f
10-a334c5ae2f2d00e6cb04dc97be9c1cf08c0e47e9
11-058f661fbe6bb9f94401c4b143888dbb9d58ed92
12-56f805b3d9a83ed57dcfed5014eb92a3c7ad287f
13-6803214791f5621cdb01a6291cc189e7a1b173b1
```

我们需要将13个中的12个用于重构密钥。因此如果我们采用份额

- 3 名子女 =  $3 \times 3 = 9 < 12$  是不成功的
- 3 名子女 + 1 位验证人 =  $3 \times 3 + 2 - 1 = 10 < T$  也是不成功的
- 3 名子女 + 2 位验证人 =  $3 \times 3 + 4 - 1 = 12 =$  是成功的

## 5.6 家族圈安全保护份额

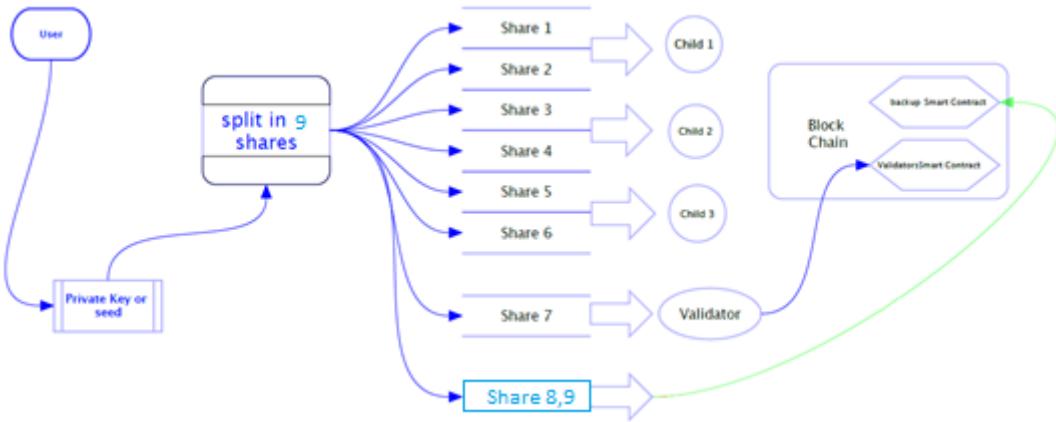


图13：家族圈安全保护份额

### 家族圈份额分配安全保护协定

- 余下份额将作为安全保护份额
- 安全保护份额可用于当n（参与者/子女）中的一位因份额遗失而无法合法拥有数字资产或死亡时；
- 我们的协定提供了区块链上一份写入不同条件的单独的“备份”智能合约；
- 由于安全保护份额会对管理者（父母）做出的完整运行设置造成危害，因此任何情况下，安全保护份额都不能被给予n（参与者/子女）中的任何人。如在使用案例2（3名子女+1位验证人）中，没有验证人份额（通过区块链智能合约查询），子女就无法重新编写密钥份额。但当您将备份份额给予他们后，他们就能对密钥份额进行重新编写了；
- 我们没有设置安全保护份额的唯一案例是我们需要所有利益相关者都完全一致认可密钥拆分时的案例，比如使用案例1（1名子女+1位验证人）。

## 5.7 验证人份额流程

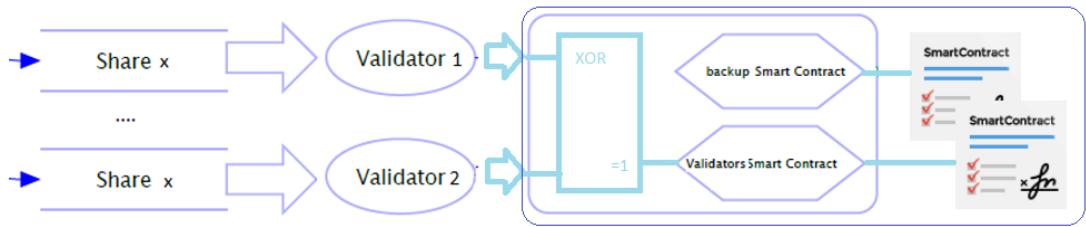


图14：验证人份额流程

- 验证人份额流程由一个合法实体验证人群组组成，这些验证人都是我们联盟计划的会员；
- 验证人不存储、拥有或了解打算发送至区块链的任何份额，其在密钥份额配置中的作用是公开的；
- 借助向n（参与者/子女/利益相关者）交付合法证书，并以公开方式验证针对区块链的交易，验证人以一种正式方式将份额分配给n（参与者/子女/利益相关者）；
- 事实上，验证人份额是发起份额分配流程的人的份额，发起人通过验证人保护区块链中的份额，目的是保持整个密钥份额的完整权利，也保护发起人在世期间的资产；
- 如果以下条件得到满足，验证人是唯一能在向区块链发送份额前，检索份额的人：
  - 必须出示n（参与者/子女/利益相关者）的份额总数，如果未出示且需要出示；如果备份智能合约条件得到满足，验证人也可以检索安全保护份额；
  - 如果发起人（父母/管理者）死亡，验证人必须对合法医疗形式进行验证，以便对区块链中存储的份额发起检索。
- 发起人/父母份额也可在需要时转移给其他合法个人。

## 5.8 多验证人可能性

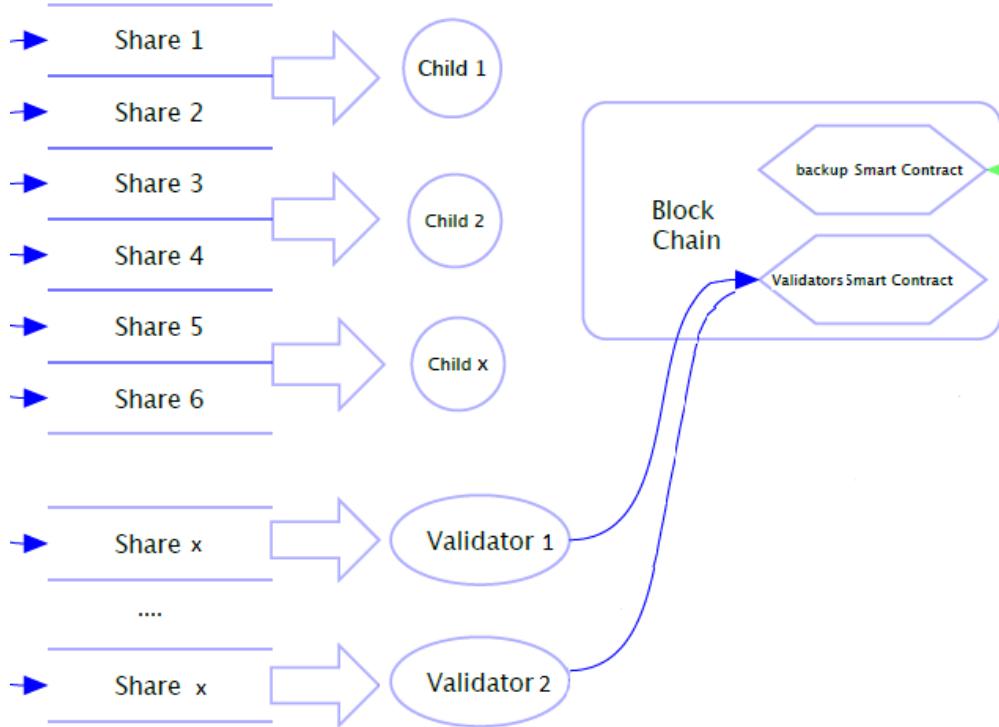


图15：多验证人体制

家族圈份额分配多验证人可能性：

- 没有人可以永生，而也不是每一个合法实体都会参与我们的联盟计划。这就是我们为您提供机会，建立包含一个以上验证人的信任圈的原因所在；
- 当您选择多个验证人参与份额分配时，我们为您提供区块链中的备份智能合约，该智能合约包含 $n$ （参与者/子女）-1份必要份额，可由第二位验证人使用；
- 我们以此为您提供了一个信任生态系统，该系统对于份额分配和验证而言，是完全多余的。

## 6 安全天堂联盟计划



安全天堂联盟计划是一个已经过安全天堂筛选的合法实体群组，筛选的目的是为了执行完成我们目标的所有必要步骤，并通过保护您的资产开启今后的信任，以及确保您亲属、利益相关者及遗产的安全。

如果您代表一家加入了我们联盟的合法实体，请向邮箱info@safehaven.io发送一封询问邮件，我们将在自己的合法平台上线后立即与您联系。我们将很快启用专门的信任联盟端口，对所有的法律问题做出回答。我们的端口一经启用，合法实体将可以自行设置子端口。当然，我们会要求您提供合法证明文件，这将有助于筛选过程。按照要求，联盟会员将支付年费，以便订购我们的服务。代币将被用作瓦斯，用于在区块链中配置智能合约。

目前，我们正在对可以成为我们联盟会员的合法实体的确定类型进行分析。我们的信任圈需要可靠的实体。

## 7 安全天堂联盟保护方案



### 1. 家族圈方案 (TFC)

家族圈方案适用于那些希望让自己的亲属获得保证，以及希望在自己去世时，有子女能获得父母所拥有资产的人。可能性几乎是无限的，份额可在以灵活方式进行拆分的同时，以安全且透明的方式确保密钥的安全。事实上，我们在过程中增加验证人，这可以让过程常用于类似于我们想要有助于确保安全的重要事件。我们在过程中还添加了能实现份额去中心化的神奇区块链。去中心化数据库的验证人 - 智能合约映射与先进且简单的密钥共享协定一起让安全性得到了进一步增强。

### 2. 业务连续性方案 (BCP)

业务连续性方案非常类似于家族圈，两者的主要差异在于我们用利益相关者取代了子女，且就份额解锁而言的验证过程有所不同。在一份业务连续性方案中，公证人无需为了通过我们的服务获得遗失份额而提供粗略的医疗文件，而只需自行准备公正手续即可。目前，我们正在制定该过程方案，该方案将在信任联盟端口上线时提供使用。业务连续性方案可用于多重签名钱包、交易所共享密钥的分配，或简单用于保护输入密码/通行短语的安全。再次重申的是可能性是无限的。

### 3. 投资圈

投资圈适用于那些希望在朋友、家庭成员或商业利益相关者中创建一种基金的人。让我们以5位朋友计划投资加密资产，并每人购买价值1000元加密货币一事为例。他们可以有哪些选择？创建一个多重签名钱包（具备稍后发现的所有缺点），即便这是非常安全的，您也始终需要群组中的相互信任... 那么，我们会如何管理这一过程呢？答案很简单！那就是借助安全天堂份额分配协定进行管理。您加密专属密钥，我们将通行短语拆分为份额，利益相关者将得到等量份额。如果我们认为公式缺乏安全保护机制，那么我们设置  $T = (y \cdot n - 1) + (X \cdot n)$ ,  $T = (2 \cdot 1) + (2.5) = 1 + 10 = 11$  个份额用于分配。其中一个份额将通过验证人（合法实体）存储于区块链中。为了释放这一个份额，用于简单实现对这种份额分配完全认同的一切，从价格阀值到重大事件都可以成为条件。又一次重申的是可能性是无限的。

### 4. 安全天堂金库

安全性高的密码是难于记住的，它也无法不经过任何合法手段而被转移至您的亲属。一切都可以成为密码，包括脸谱网、Gmail或任何其他重要账户。如果您想自行确保数字遗产不会随着自己的去世而消失，确保您的亲属可以在您已去世时进入这些账户，那就请通过安全天堂借助区块链使用我们其中一个份额分配协定存储这些数字遗产吧！

## 8 结论

现在，投资加密货币和比特币耗时多且过程艰辛。而另一方面，这也会在数年后为您带来丰厚的利润。确保数字资产的安全，并使这些资产免于受到外部利用，这是相当长一段时间以来，所有交易人士及长期投资者一直寻求的目标。我们也是出于同样的原因，为了保持金融独立并为自己的亲属打造安全而放心的未来而全心投入了这项事业。这就是我们将开发去中心化平台，为全世界提供解决方案的原因所在。安全天堂公司将在确保及存储您的数字密钥或种子方面，让您拥有不一样的服务。制定如同安全天堂这样的解决方案，将让投资者及其亲属对数字资产的安全放心。我们希望自己的平台及不一样的解决方案能得到您的认可，我们也欢迎您成为我们的投资者之一！

## 9 市场

加密货币是使用了密码的数字资产，而密码是用于安全保障的一种加密技术。虽然一些更新的加密货币也具有为其所有人提供一套规则或义务的功能，但加密货币主要用于购买及出售商品及服务。加密货币不具有固定价值，因此不可兑换为其它商品，比如黄金。与传统货币不同，加密货币不是由中央权威机构发行的，也不被看作是法定货币。

就这点而言，加密货币的使用极大地受限于“其早期接受者”。从规模来说，全世界约有1000万人持有比特币，其中近一半人纯粹是为了投资。客观地说，由于受到政府支持的货币具有充分的功能，因此加密货币并不是必需品。对于加密货币的绝大多数接受者而言，加密货币所具有的优势都存在于理论中。因此，只有在使用加密货币会带来极大的实际意义的时候，加密货币才会为主流社会所接受。那么，使用加密货币的优点在哪里呢？

### 加密货币交易平台

加密货币交易平台就是可以让个人购买、出售或将加密货币兑换为其他数字货币或传统货币的网站。交易平台不仅可以将加密货币转换为受政府支持的主要货币，也可以转化为其他加密货币。包括Poloniex, Bitfinex, Kraken和 GDAX在内的一些大型交易平台每天的交易量都超过了1亿美元（等值）。几乎每一个交易平台都遵守政府反洗钱规定，而且按照要求，客户要在开立账户时提供身份证件。

除交易平台外，人们有时也借助LocalBitcoins这样的网站开展点对点交易，这让交易者得以避免泄露个人信息。在一笔点对点交易中，参与者借助软件，在无需任何其他中间商参与的情况下进行加密货币交易。

## 加密货币钱包

对于用户转账、到账数字货币及管理余额而言，加密货币钱包是必不可少的。钱包可以是硬件或软件，尽管硬件钱包被认为具有更强的安全性。例如，与计算机的USB接口相连的Ledger 钱包看似一个可移动磁盘。比特币账户的交易和余额借助自身区块链得到记录的同时，用于签名新交易的专属密钥被保存在了Ledger钱包内。当您尝试创建一笔新交易时，您的电脑会要求钱包为交易签名，之后才将其发送至区块链。由于专属密钥永远不会离开硬件钱包，因此即便您的电脑受到黑客攻击，您的比特币也是安全的。但除非有备份，丢失钱包仍会导致钱包所有人资产受损。相反，类似Coin base 钱包这样的软件钱包是虚拟的。这类软件设备可以将钱包持有人的资金存放在钱包提供方的网络中，但这就增加了风险。

随着越来越多的人和资金流入加密货币市场，更多人必须进入交易平台或开启钱包并获得专属密钥。安全天堂正在制定一种完美的解决方案。基本上每一个开启了钱包并购买了一种加密货币的人，都能成为安全天堂的客户。我们的市场发展潜力是巨大的！对于安全天堂将为您带来与众不同的体验这一点，我们充满信心！

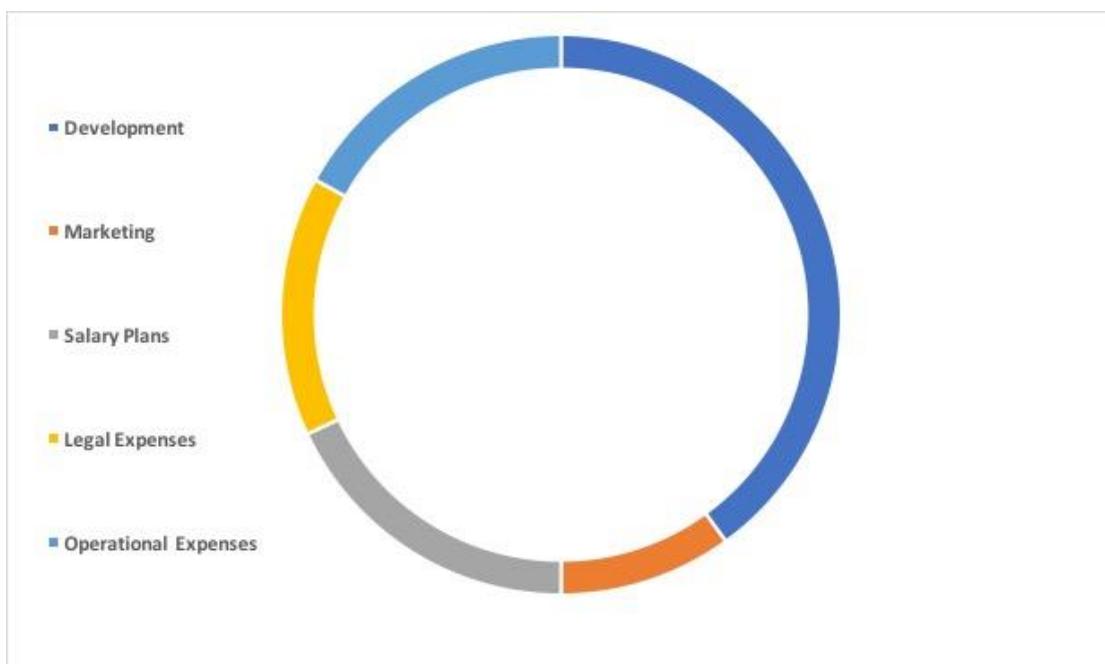
## 10 代币

---

安全天堂代币是以太币为基础建立的一种ERC20代币。将ERC20标准引入以太坊区块链的目的，是让开发人员可以设计直接使用代币的去中心化应用程序（Dapps），而无需在每次引入一种新代币体系时都要对程序进行重新设计。因此，有思路的任何人都可以借助ERC20在区块链上配置产品，而无需进行平台设计。借助ERC20，我们可以确定一套基于以太坊的安全天堂可以依据的一般法则，能够提前知道代币会如何按照标准操作。开发安全天堂代币的目的是拯救在我们本白皮书中所描述的不完整的市场。开发第一阶段以我们所创造的代币总量为关注点。安全天堂代币将被用作过程中的一种瓦斯。

## 11 资金分配

◆ 开发	40%
◆ 营销	10%
◆ 薪资方案	18%
◆ 法律费用	15%
◆ 运营费用	17%



我们旨在对筹集到的大部分资金进行分配，以便促进平台发展。因此，资金中的40%将用于本次首次代币发售；10%分配用于促进各种营销活动，包括赠品活动和签名活动；15%分配用于合法市场，如交易平台；17%作为运营费用而18%将分配用于薪资方案。

## 12 首次代币公开发售参数 + 代币分配

报价机: SHA

供应总量: 120,000,000

基于以太币的代币 (ERC20)

首次代币公开发售开始日期: 参见网站<https://ico.safehaven.io>

预售开始日期: 参见<https://safehaven.io/#pre-sale>

初期投资人兑换率: 2500 SHA = 1以太币

预售兑换率: 2000 SHA = 1以太币

首次代币公开发售兑换率: 1500 SHA = 1以太币

最低总市值: 1000以太币

最高总市值: 54,500以太币

未售出代币将被销毁

### 代币分配

首次公开发售初期投资者: 2500 SHA/ETH 总计

(5,000,000 SHA)

预售: 2000 SHA/ETH 总计 (25,000,000 SHA)

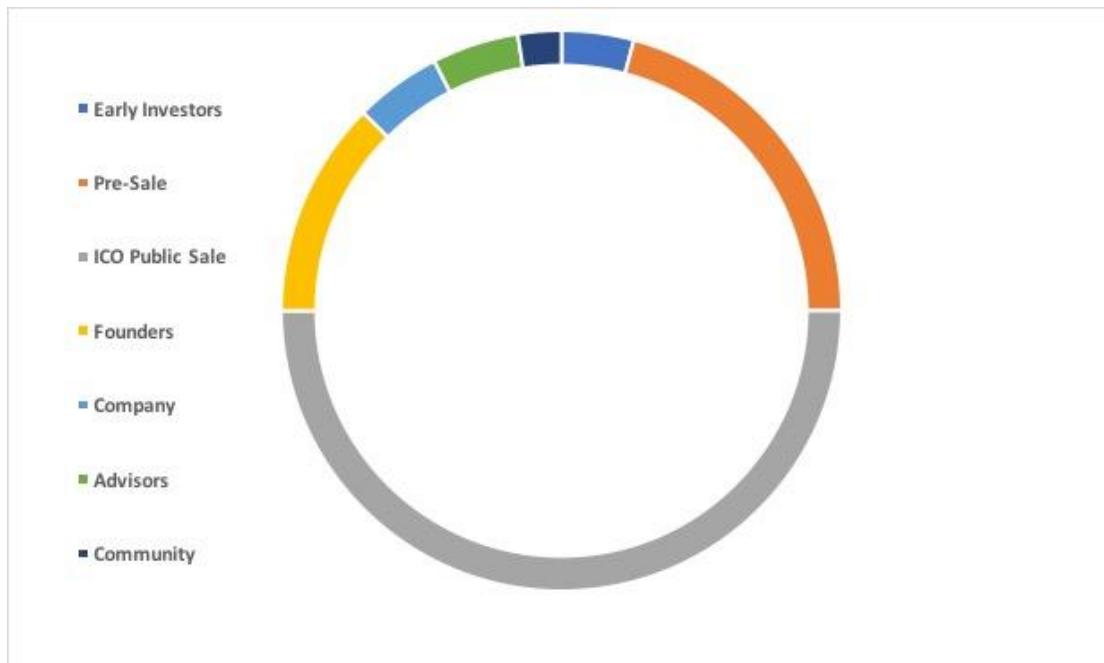
正式发售: 1500 SHA/ETH 总计 (60,000,000 SHA)

创始人: 15,000,000 SHA

公司: 6,000,000 SHA

顾问人员: 6,000,000 SHA

社区与赠品: 3,000,000 SHA



## 13 路线图

