SafeHaven.io

...資産を継承可能にする...

ブリュッセル、2017 年 11 月
www.safehaven.io

セーフヘブンチームによって書かれた

目次

図表

図表目录

執行概要

このホワイトペーパーは、SafeHaven.io が何を意味するのかを簡単に理解できるように目的としています。このドキュメントは、安全な避難所プロジェクトの現在および将来の展開を説明する技術白書です。このペーパーは情報提供のみを目的としており、今後の予定に関する記述ではありません。特記しない限り、このホワイトペーパーに記載されている製品やイノベーションは現在開発中であり、配備展開中ではありません。当社は、そのような技術および革新の成功した開発と実施、または本書に記載されているその他の活動成果に関する保証と表明を行わず、法律によって認められる範囲で、法律またはその他の方法により暗示される保証を放棄する。安全な避難所または本書に記載されている技術との相互作用を含め、本書の内容またはそれに由来する推論を誰も依拠することはできません。安全な避難所は、安全な避難所に関する情報や意見に基づいて行動する人物から生じる可能性のあるあらゆる種類の紛失や損害対しても責任がありません（予見可能かどうか）。本書に記載されている安全な避難所 プラットフォームと安全な避難所エコシステム、あるいは過失、債務不履行、とケアの欠如にかかわらず、それ以上のお問い合わせに関連して利用可能となったいかなる情報も含まれます。

1 紹介

ほとんどの人々が知っているが、暗号化通貨は別の発明の副産物として浮上しています。Bitcoin の未知数発明者、Satoshi Nakamoto、最も重要な暗号通貨であり、決して通貨を発明するつもりはありませんでした。2008 年後半に Bitcoin が発表された時、Satoshi が「Peer-to-Peer Electronic Cash System」を開発したと話した。"彼の目標は何かを発明する事でした。 多くの人々がデジタル現金の前に作成することに失敗しました。Satoshi の発明の最も重要な部分は、地方自治体のデジタル現金システムを構築する方法を見つけたことでした。90 年代には、デジタルマネーを作る試みがたくさんありましたが、すべて失敗しました。すべての集中的な試みが失敗するのを見た後、Satoshi は中心実体無しでデジタル・キャッシュ・システムを構築しようとしました。ファイル共有の為、Peer-to-Peer ネットワークのように。この決定は暗号通貨の誕生となった。彼らは Satoshi がデジタルキャッシュを実現する為に見つけた欠けている作品です。理由は少し技術的に複雑ですが、それを入手すれば、暗号化通貨について他の多くの人よりも多くのことが分かります。だから、できるだけ簡単にしようとしましょう：デジタル現金を実現するには、口座、残高、取引を含む決済ネットワークが必要です。それは理解しやすいです。支払いネットワークが解決しなければならない 1 つの大きな問題は、いわゆる二重支出を防ぐことです。あるエンティティが同じ金額を 2 回費やしてしまうのを防ぎます。通常、これは残高を記録している中央サーバーによって行われます。分散ネットワークでは、このサーバーがありません。だから、この仕事をする為にネットワークのあらゆる一つエンティティが必要です。ネットワーク内ですべてのピアは、将来のトランザクションが有効かどうか確認、または二重の消費を試みるかどうかをチェックするために、すべてのトランザクションのリストを持つ必要があります。しかし、これらの企業は記録についてどのようにコンセンサスを維持することができますか？ネットワークの同僚がわずか 1 つの微妙なバランスについて同意しない場合、すべてが壊れています。絶対的な合意が必要です。通常、バランスの正しい状態を宣言する中央権威をもう一度取ります。しかし、中央権威無しでコンセンサスを得るにはどうしたらよいでしょうか？Satoshi がどこにも出現しなくなるまで誰も知らなかった事です。実際、誰もそれがさらに可能であると思っていませんでした。それについて Satoshi が証明された。彼の主な革新は、中央権威無しでコンセンサスを達成することでした。暗号化通貨はこのソリューションの一部です 。このソリューションをスリリングにして魅力的なものとして、世界中に広がるのを助けました。あなたが私たちのホワイトペーパーを読んでいるので、この挑戦的な市場に投資した、それとも投資しようとしていると思います。

2 懸念

何かがあなたに起こるかもしれない日、またはすでに亡くなった日を考えましたか？あなたの家族があなたがいない時、人生に直面しなければならない日を考えたことがありますか？あなたの暗号通貨投資はどうですか？数百の秘密鍵、取引所、財布を持つ困難な市場はどうですか？彼らはあなたがいなくなった時、投資を回収することができますか？ 彼らは何かが間違っていることを恐れることなく、彼らを助ける誰かを信じることができますか？はい、できます！安全な避難所はソリューションを提供しています！最も人気があり安全なブロックチェーンにプラットフォーム/エコシステムを構築しているので、遺産について心配する必要はありません。

3 解決

あなたのデジタル資産を保護する為に、安全な避難所では私たちの自分自身でロックせずにそうするチャンスを与えます。TFC シェア配布キーエスクロープロトコルと信頼アライアンスプログラムのおかげで、種子/秘密鍵/パスフレーズは、利害関係者や子供の間で、透明かつ安全に共有することができます。私たちのプロトコルは、イニシエータが自分の資産を支配するコストを全面的に抑えるような方法でシェアを分配します。

いつかで彼/彼女は亡くならなければならない不幸な日に、トラストアライアンスプラットフォーム（公証人）の登録メンバーは、彼/彼女の子供/ステークホルダーに遺産を渡すため、ブロックチェーンの残りの分を回収することができます。それをどのように達成するのですか？3 ステップのみを含むステップ毎ののガイドと、さらにこのドキュメントで説明されている使用済みのテクニックを確認してください。

3.1 ステップバイステップ

ステップ 1：ユーザーは彼の遺産（暗号資産）を保護することに決め、3 人の子供の間に安全な避難所の透明なブロックチェーンソリューションを使用して、種子/秘密鍵またはパスフレーズを配布する計画を立てます。このプロセスの開始者は、信頼アライアンスプログラムの登録メンバーに送られ、これは必要な検証手順を処理するために安全な避難所と信頼できる関係を持つ法人のグループです。

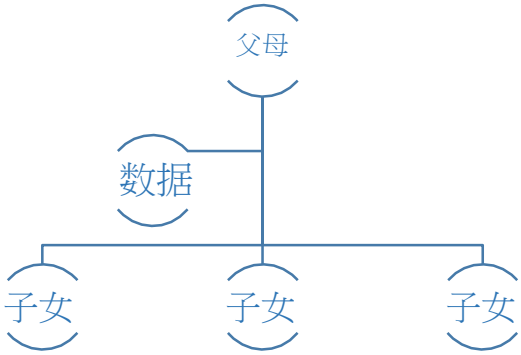


図 1：ファミリーサークル（TFC）

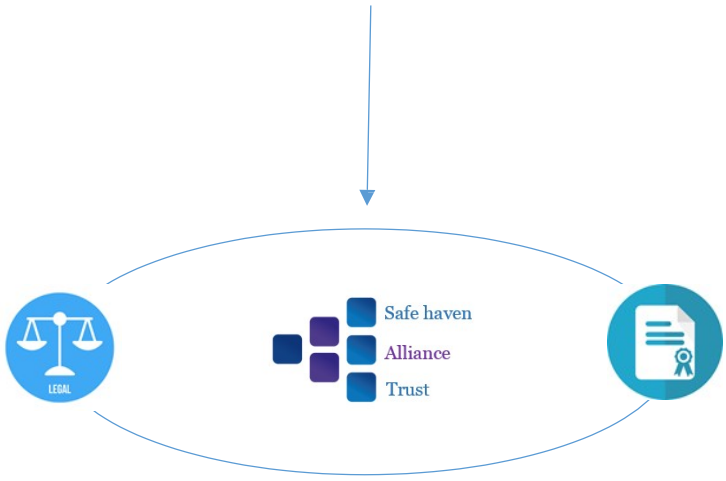


図 2：信頼アライアンス表現

ステップ 2：法人は、安全な避難所のプロトコルでバリデータを保護し、配布する為にデータを分割します（TFC シェア分配プロトコルを参照）。特別として、その使用の為に開発された安全な避難所アプリケーションを使用して、得られたシェアを子供に提供します。この為に使用されるソフトウェアは、メモリ内にもローカルにも、集中データベース内にもデータを保持しません。バリデーターだけが共有します（バリデーターの共有プロセスを参照してください）それてブロックチェーンに送信されます。 明らかなセキュリティ上の理由から、スマートな契約を結んで展開される前にシェアを暗号化および復号化するセキュリティアルゴリズムは明らかにされません。安全な避難所には、バリデータ ID とスマート契約を識別するためのマッピングが用意されていますが、マッピングは分散型ブロックチェーンデータベースに展開されます。これはバックアップバリデーターの場合も同様です（複数のバリデーターの可能性と TFC のフェイルセーフシェアを参照）。

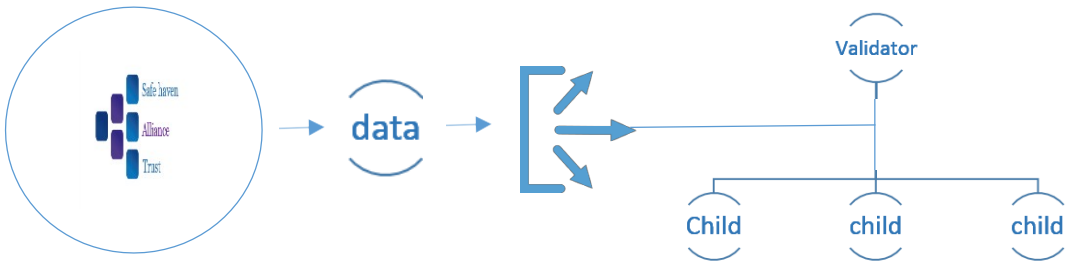


Figure 3 : シェアステップに分割

ステップ 3：子供に配布されたシェアは、法的証明書の形で公証人によって調整されます。親/創始者からの保護される共有は、安全な避難所 アプリ（信頼アライアンスのメンバーのみがアクセス可能）で暗号化され、スマート契約の形でブロックチェーンに送信されます。

図 4：子証明書

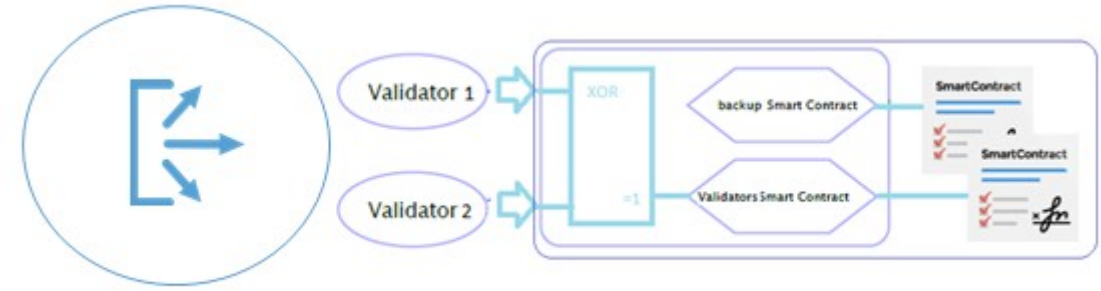


図 5：バリデータ

子のシェアは、証明書の作成と、または本発明者のプロトコルにおけるハードウェア元帳の統合を介して共有することができます。私たちは現在、自身のハードウェア元帳に基づいて、これを達成するために詳細を検討しています。詳細は公開されていませんが、まだプロジェクトの ICO 段階にあります。

ステップ 4：突然死亡した場合や創設者が自ら資産を処理することができなくなった場合、子供または利害関係者が必要な法的書類を公証人に紹介することによって不足分を得ることができます。彼は安全な避難所によって検証されると、ブロックチェインから不足分を取り出せるようになります。私たちのプロトコルは、フェイルセーフ共有とバックアップバリデーターを持つ可能性を扱っています。詳細については、このドキュメントで説明する TFC フェイルセーフ共有と複数バリデータの可能性のセクションを参照してください。

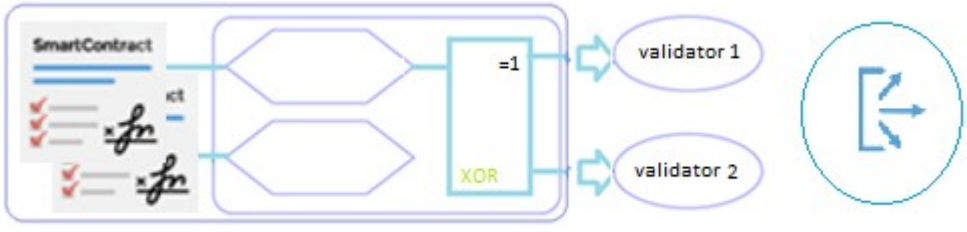


図 6：共有検索プロセス

4 基本原則

4.1ブロックチェーン

ネットワークについて、ブロックチェーンは、価値のユーザー促進業務の間でデジタル信用を確立するためのソフトウェア・イノベーションです。ブロックチェーンを使用すると、デジタル仲介を追跡、検証、承認するための中央仲介の必要無し、ネットワーク全体に信頼を分散することができます。現在、中央仲介機関から信頼を得るという考え方は、民間組織と政府機関の両方の組織を支えていますが、コストがかかりし、遅くって、攻撃に対しても脆弱であることが証明されています。ブロックチェーンは分散データベースとして動作することでこれらの問題を克服し、ブロックと呼ばれるレコードの連続的な増加を維持します。

4.2 スマート契約

オン・チェイン・コンピュータ・コードまたはスマート契約は、契約条項を不要にする契約のパフォーマンスを促進、検証、または実施するコンピュータ・プロトコルである。スマート契約は、しばしば契約条項の論理をエミュレートします。スマートな契約は、仲介者のサービスを避けながら、透明で紛争のない方法で金銭、財産、シェアまたは価値を交換することができます。通常、プロセスは、仲介業者、政府機関、銀行、弁護士または公証人に支払いを要求し、その後、商品とサービスを受け取る前の処理時間を必要とします。しかし、スマート契約技術を使用すれば、すべてを自動化することができます。スマート契約技術は、自動販売機の技術と比較られます。自動販売機では、自動販売機にお金が入金され、所望の商品も回収されて正確な量が寄託されていればよいです。匹敵することができますが、スマートな契約では、トークンの転送を受け取る為に、ブロックチェーン上のエスクローに資金が入金されます。（例えば、家のタイトルのデジタル証明書）、一度条件が満たされると、仲介者のコントロールへ瞬時に転送されます。スマート契約は、従来の契約と同じ方法で契約に関する条件を定義するだけでなく、それらの義務の実施も提供します。

5 テクニックと概念数学

5.1 多項式補間

多項式は、複雑な曲線を近似するために使用することができ、例えば、タイポグラフィにおける文字の形状は、いくつかのポイントが与えられます。 関連するアプリケーションは、自然対数や三角関数の評価である：、いくつかの既知のデータポイントを選ぶルックアップテーブルを作成し、それらのデータポイント間を補間します。 これは、大幅に高速な計算になります。
定義：
2 つの xi が同じでない n + 1 個のデータ点（xi、yi）の集合が与えられると、性質を有する n 次の多項式 p を求める

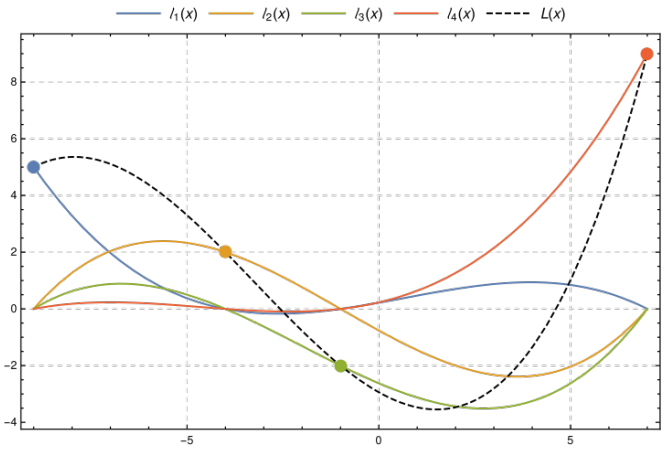
$$p(x_i) = y_i, \qquad i = 0, \ldots, n.$$

定理は、以下の unisolvence ような多項式 p は、存在し、ユニークであり、そして Vandermonde 行列によって証明することができると述べています

定理は、n + 1 の補間ノード（XI）のために、多項式補間は、線形二分を定義することを述べて

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

ここでΠn は多項式のベクトル空間であり（ノードを含む任意の区間に定義される）、次数は最大で n である。



Page

多項式補間はまた、数値直交と数値常微分方程式およびセキュアマルチパーティ計算、秘密分散法におけるアルゴリズムの基礎を形成します。 秘密分散法、我々は我々の目標を達成するために使用するものです。

図 7：多項式

5.2 主なエスクロー

私たちは永遠せず、私たちと一緒にデジタル遺産へのアクセスが消えることが残念になります。株主の突然の紛失は、完全なパスフレーズをリセットするために、問題になることがあります。この記事では、他のケースシナリオを強調するために、家族のサークルや友人の例を継続して使用します。この問題の 1 つの答えは、「特定の条件で「第 3 者がこれらの共有にアクセスできるようにする重要な条件委任条件です。しかし、どのような条件で第三に、そしてそれを道徳的だ技術的に確信することができる方法は何ですか？エスクロー機関はエスクローキーの機密を安全に確保する必要があります。まず、私たちは、保護するデータを暗号化する必要があります。このキーは、秘密鍵または SHA265-512 などのセキュリティ暗号化アルゴリズムがあるシードとパスワードを使用することができます。このパスワードは、共有に分かれて TFC SD プロトコルによって配布されることがあります。

.

5.3 秘密の共有

復号化で、秘密の共有計画は、参加者のグループの間に秘密を分配する方法で、各参加者は、秘密の共有を割り当てられます。秘密は共有が一緒に結合される場合にのみ再構築されることがあります。個別銘柄では、独自に使用していません。より正式には、秘密の共有を計画するには、一人のディーラーと、より多くのプレイヤーがいます。ディーラーは、特定の条件が満たされた場合にのみ、プレイヤーに秘密を提供しています。ディーラーは各プレイヤーにどのようなタイプの t（しきい値）以上のグループが一緒に秘密を再構築することができますが、t 未満のプレイヤーのグループは、共有することができないように共有することによってこのタスクを実行します。これらのシステムを（t、n）しきい値スキームと呼びます。攻撃者が有効な株式を 1 つ保有していることを全く知らないかどうかは、何の違いがないことを証明することができます。彼の株式よりも少ない株式を持っている限り、秘密を調べるための推測よりも良い選択はありません。

秘密の共有のいくつかの使用例：（SHA 保護計画を参照）

- 良いパスワードは覚えにくいです。 ある日、彼は彼のを忘れた場合賢いユーザーはなど、与えられたパスワードの株式のセットを生成し、自分のアドレス帳に 1 株を格納する秘密分散法を使用して自分の銀行預金の安全で 1、友人と一緒に 1 株を残すことができます パスワード、彼は簡単にそれを再構築することができます。 もちろん、アドレス帳に直接パスワードを書き込むと、それは「敵」で盗まれる可能性があるので、セキュリティ上のリスクをもたらすでしょう。 秘密分散法を使用している場合、攻撃者は、別の場所から多くの株式を盗むために持っています。

  このシナリオの典型的なアプリケーションは、暗号化されたバックアップシステムの安全な実装です。 回収はほとんど必要ありません、そのデータを仮定すると、バックアップデータは暗号化された公開鍵をすることができます - これは自動的にユーザーとの対話なしに行うことができます - プライベート回復キーは秘密の共有を経由して保護しながら。
- 「販売代理店は、異なるチャネルを使用して、元の秘密を回復するために必要なすべての共有の水を、単一の受信者に送信することができます。侵入者は秘密を回復するために、すべての共有を傍受する必要があります。1 つのメッセージを傍受より難しい。」
- 銀行の取締役は、銀行の金庫のロック解除コードの株式を作成して、従業員に渡すことができます。ディレクターを使用することができない場合でも、特定の数のスタッフが一緒に作業する場合にのみ、ボルトを開くことができます。ここで、秘密の共有計画は完全に信頼できる人の雇用を可能にします。

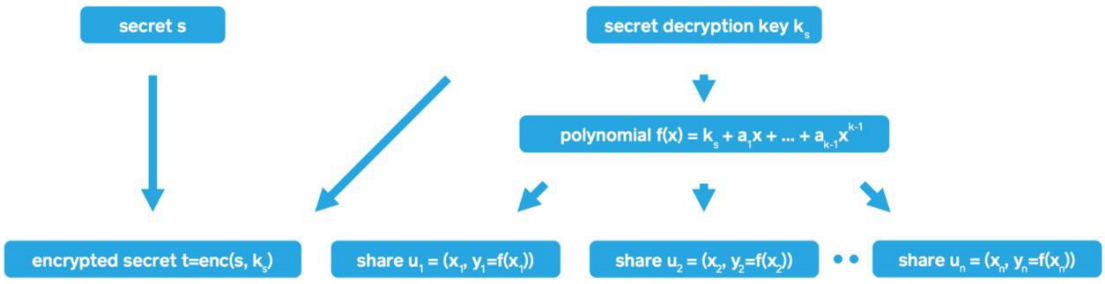


图 8：秘密の共有原則

5.4 二人の男のルール

このルール（2 人ルール）は、核ミサイルを送信して偶発的な攻撃や悪意のある攻撃を防ぐなどの機密性の高い領域で使用されます。暗号化では、安全性の高い通信（COMSEC）のために 1 人の人が暗号鍵にアクセスできないようにするために、アメリカ人は「2 人完全性」（TPI）というフレーズを使用します。

ここでは、エスクロー当局との信頼とセキュリティの問題を解決するのに役立つ興味深い概念があります。エスクローでデータを明らかにするために 2 人の個人が協力することを要求することにより、孤立した悪意のある行為から身を守ります。

エスクローキーのパスフレーズを分割して、ファミリーサークル（TFC）と呼ばれる信頼できる人々のグループにその部分を与えましょう。

このパスフレーズを分割する方法は？ TFC の N メンバー間で N 個の部分を分配するだけで、秘密鍵エスクローを使用するために一緒に会うように強制されますが、そのうちの 1 つが利用できない場合、またはセーズームを回復したい TFC の欠落した株主です。

2 つの点で線を定義し、3 つは放物線を定義し、3 つは立方体のように定義します。もし 6 人の人の間に 1234 という値のような秘密を共有したいのであれば、その秘密を見つけるためには 3 つが必要ですが、ポイント（0,1234）を通過する人の中から放物線をランダムに選ぶでしょう。彼の 6 点の座標をこれらの 6 人の個人に割り当てます（図 9 参照）

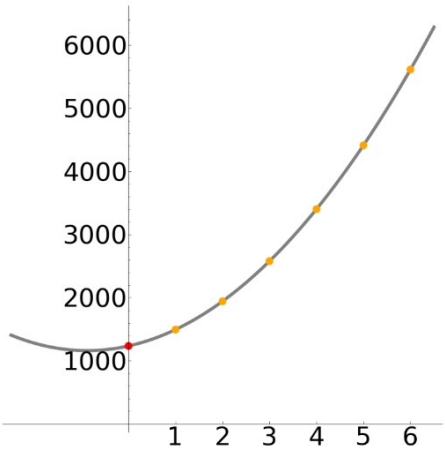


図 9：パラボリックアンパッサンカップル（0、1234）。

その中二人だけの場合、2 と 4 がその座標を共有するために来たとき、彼らは元の放物線を発見することができなかったため、x = 0 の秘密ポイントの値を見つけることができなかった（図 10 参照）。

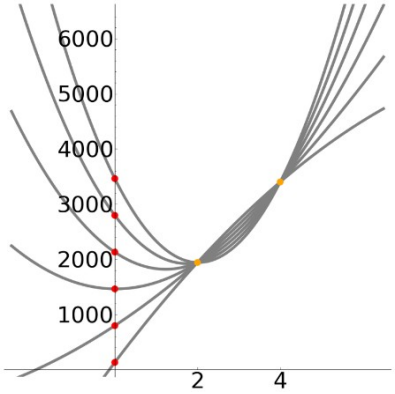


図 10：渡すたとえ話
n°2 の点を通る
そして 4。

したがって、第 3 者の個人がただ一つのたとえを定義して、秘密の値 1234 を明らかにするために、自分の座標を共有することに同意する必要があります（図 11 を参照）。

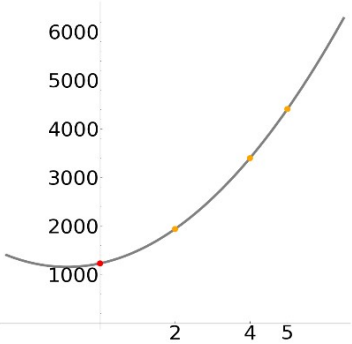


図 11：比喩しただけで 2,4,5 点を通過すること
ができます

5.5 TFC 共有分散プロトコル

家族の円は安全な避難所のグループに所属するメンバーのコンテキストで、このグループは、信頼や友人の単純円の利害関係者は、同社のグループを家族を含めることができます。 TFC SDP は、当社のエコシステムへの信頼の輪を確立するために安全な避難所が開発したプロトコルです。

私たちは、上記の技術を考えると、我々はディーラー（彼の遺産を保護したい人）

とｎ選手（彼の子供たちとバリ[公証人]）を持っています。 ディーラーはプレイヤーに秘密を与えるが、特定の条件が満たされた場合にのみ。 ディーラーは任意のグループトンの（しきい値の場合）以上のプレイヤーが一緒に秘密ができますが、トンの選手未満の無いグループを再構築できるように、各プレイヤーにシェアを与えることによって、これを達成します。 このようなシステムは、（t、n）閾値方式と呼ばれる。

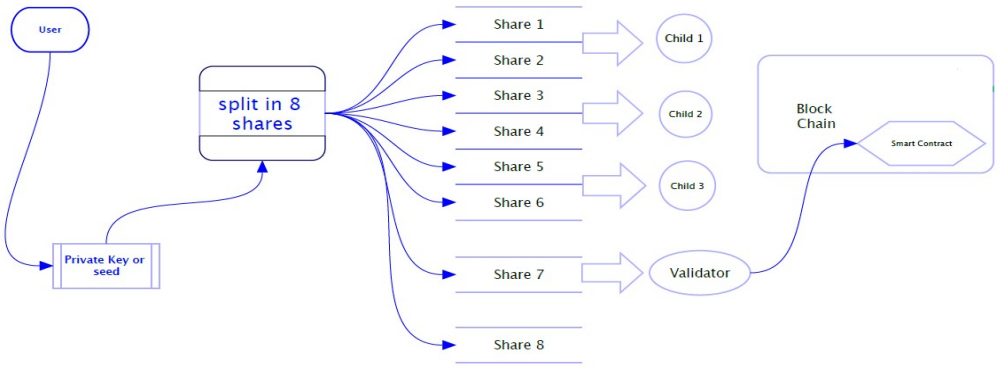


図 12：TFC 共有配布プロトコル

TFC SD プロトコルの基本ルール：

- 共有秘密鍵は、最大 1024 ビットになることがあります。
- 1024 ビットよりも大きな秘密を保護するには、ハイブリッド手法を適用する必要があります。秘密はブロック暗号で暗号化し、秘密の共有だけキーに適用する必要があります（openssl と gpg は有効なツールである）
- 秘密のセキュリティレベルは、短い秘密/シード/キーが若干の塩ビット詰められるための長さの上限を意味することができます。
- I / O は、ASCII 文字の代わりに 16 進数を使用することができますので、バイナリデータは、共有にも保護/分割することができます。
- 共有秘密を分離したり、結合中のプロトコルは、仮想アドレス空間を RAM または個人情報保護の理由でロックします。
- 分散共有エンティティの数は、技術的に 99 個に制限されており、これを 15 個に制限して、各エンティティは、15 個から 99 個まで持つことができます。
- 検証 y は常に n（プレイヤー/サブ）より-1 共有が少なくなります。
- 安全な避難所の生態系の完全な信頼のネットワークを構築するには、少なくとも 1 人の選手と 1 人の検査員が必要です。
- 複数の検証を追加することができます。

5.5.1 TFCSD ケース 1：1 の子供と 1 バリ

私たちの秘密分散法の式に基づいて：

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

秘密を再構築するために必要な最低限の株式の T =しきい値。

Y= は、我々の場合には、それは安全な避難所のアライアンスプログラムの登録メンバーで、プロセスのバリデータを=

X =株主

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

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

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

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

$T = 1 + 2$

$T = 3$ *（完全共有キーを取得するために必要なシェアの最小値。*

株式のマックスは、バリのための子供のための 3（2 と 2（-1）となります。

だから我々は、例えば秘密を取る：「私の共有パスフレーズを」我々は、次の 3 割の株式を取得します.

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

我々は 100％のシェア表現を持っているように、成功のための唯一の可能なシナリオがあります.

- 1 子=（1 x 2）&（2 - 1）バリデータ= 3 = そう OK

私たちの秘密分散法の式に基づいて：：

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

T =秘密を再構築するために必要な最小シェアの閾値。

Y= は、我々の場合には、それは安全な避難所のアライアンスプログラムの登録メンバーで、プロセスのバリデータを=

X =株主

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

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

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

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

$T = 1 + 6$

T= 7（最小完全な共有鍵を取得するために必要とされる株式。

株式のマックスは、バリのために子供のための 8（6 および 2（-1）になります

だから我々は、例えば秘密を取る：「私の共有パスフレーズを」我々は、以下の 8 割の株式を取得します。

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

そして、我々は秘密を再構築するために 8 のうち、7 が必要になります。 だから私たちが

- 3 人の子供= 3×2 = 6 <7 ので NOK
- 子供 2 人+バリデーター1 人= 2 x 2 + 2-1 = 5 <NOK
- 子供 3 人+バリデーター1 人= 3 x2 + 2-1 = 7 =Tそう OK

5.5.3 TFCSD ケース 2：子供 3 名+フェイルセーフ 1 台とバリデーター1 台

私たちの秘密分散法の式に基づいて：追加する(b=x-):

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

T =秘密を再構築するために必要な最小シェアの閾値。

Y= は、我々の場合には、それは安全な避難所のアライアンスプログラムの登録メンバーで、プロセスのバリデータを=

X =株主

$T = (y.n - 1) + (X.n)$ *+ (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（最小完全な共有鍵を取得するために必要とされる株式。

株式のマックスは、子供のための 9（6 と 2 になります（-1）のためのバリデータ+ 2（フェイルセーブ）

だから我々は、例えば秘密を取る：「私の共有パスフレーズを」我々は、以下の 9 割の株式を取得します.

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

そして、我々は秘密を再構築するために 9 のうち、7 が必要になります。 だから私たちが

- 3 人の子供（または 2 +フェールセーフ）= 3 x 2 = 6 <7 なで NOK
- 子供 2 人+バリデーター1 人= 2 x 2 + 2-1 = 5 <NOK
- 3 人の子供（または 2 +フェールセーフ）+ 1 バリデーター= 3 x2 + 2-1 = 7 =Tそう OK

5.5.4 TFCSD ケース 3：3 人の子供と 2 つのバリ

私たちの秘密分散法の式に基づいて：：

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

T =秘密を再構築するために必要な最小シェアの閾値。

Y= は、我々の場合には、それは安全な避難所のアライアンスプログラムの登録メンバーで、プロセスのバリデータを=

-1 =フェイルセーブシェア

X =株主

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

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

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

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

$T = 12$

$T = 12$ 完全な共有キーを取得するために必要とされている株式の（最小。

最大シェアは 13（子供は 9、バリデーターは 4（-1））です

だから我々は、例えば秘密を取る：「私の共有パスフレーズを」我々は、次の 13 分割された株式を取得します

```
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
```

そして、我々は秘密を再構築するために 13 のうち 12 が必要になります。 だから私たちが

- 3 人の子供= 3 x 3 = 9 <12 なので NOK
- 子供 3 名+バリデーター1 名= 3×3 + 2-1 = 10 <NOK
- 子供 3 人+バリデーター2 人= 3 x 3 + 4 - 1 = 12 =Tだから OK

5. 6TFC フェイルセーフシェア(s)

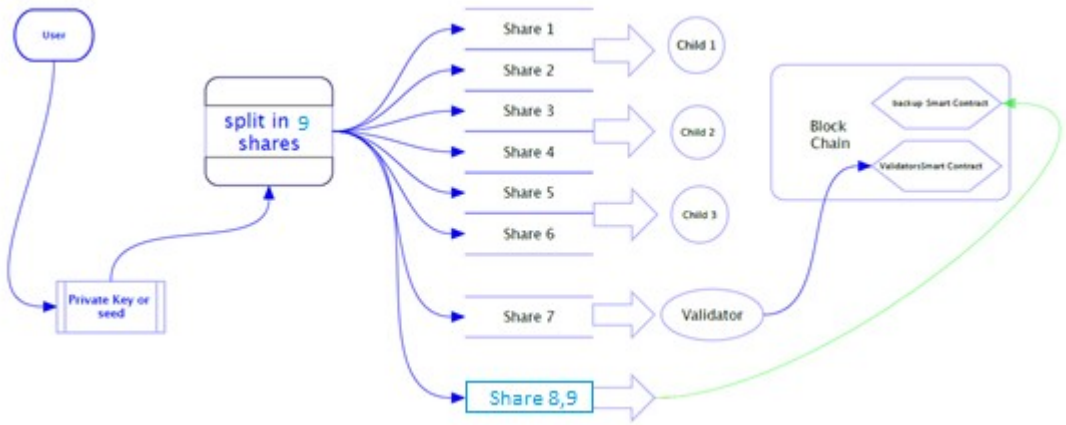


Figure 13 : TFC Fail-safe share

TFC SD フェイルセーフプロトコル：

- 残りの株式は一種のフェールセーフなシェアとして使用される
- これは、n（選手/子供）のうちの 1 人がシェアを失った場合、正当に行動できなくなった場合、または死亡した場合に役立ちます。
- 私たちの議定書では、異なる条件でブロックチェーンに別の "バックアップ"スマート契約が書かれています。
- ユースケース 2（子供 3 人+検証者 1 人）のように、ディーラー（親）による完全な操作設定を危険にさらす可能性があるため、フェイルセーフ共有は n 個のプレーヤー ）子どもたちはバリのシェア（トラフ blockchain スマート契約クエリ）なしのシークレット・シェアを再コンパイルすることはできませんが、あなたは、バックアップの共有を与えるとき、彼らはそうすることができるようになります。
- フェイル・セーブ・シェアを持たない唯一のケースは、ユース・ケース 1（子供 1 人+検証者 1 人）など、利害関係者の 100%のコンセンサスが必要な場合です。

5.7 バリデータは、プロセスを共有します。

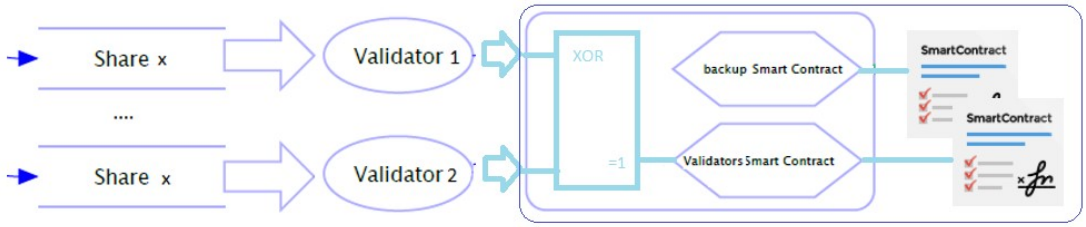


Figure 14 : Validators share process

- バリデータの共有プロセスは、当社のアライアンスプログラムのメンバーである法人のバリのプールで構成されています。
- バリデータは、株式、自身または blockchain に送信されることを意味株式の何も表示は、役割が秘密の株式の展開の面で透明性がありません。
- 彼らは、n に法的な証明書を提供することで、正式な方法で（プレイヤー/子供/利害関係者）n に株式を配布し、透明な方法で blockchain に向けてトランザクションを検証します。
- バリのシェアは、実際に開始するためのプロセスを開始した人の割合で、彼がいる限り、彼が住んでいるような完全なシークレット・シェアの完全な権利を維持し、そう彼の資産にするためにバリデータを経由して blockchain でそれを保護します。
- バリ（複数可）/以下の条件が満たされた場合 blockchain に以前送っ株を取得することができる唯一の 1（S）あるさ.
    - スマート契約条件が満たされていれば、n（選手/子供/利害関係者）の総シェア数が存在しなければなら、必要であれば、バリデータによってもフェールセーフシェアを取得することができる。
    - イニシエータ（親/ディーラー）が死亡した場合、バリデータは、ブロックチェーンに保管されているシェアの取得プロセスを開始するために正当な医療書式を検証する必要があります.
- イニシエータ/親のシェアは、必要に応じて別の正当な人にも譲渡することができます.

5.8 複数の検証ツールの可能性

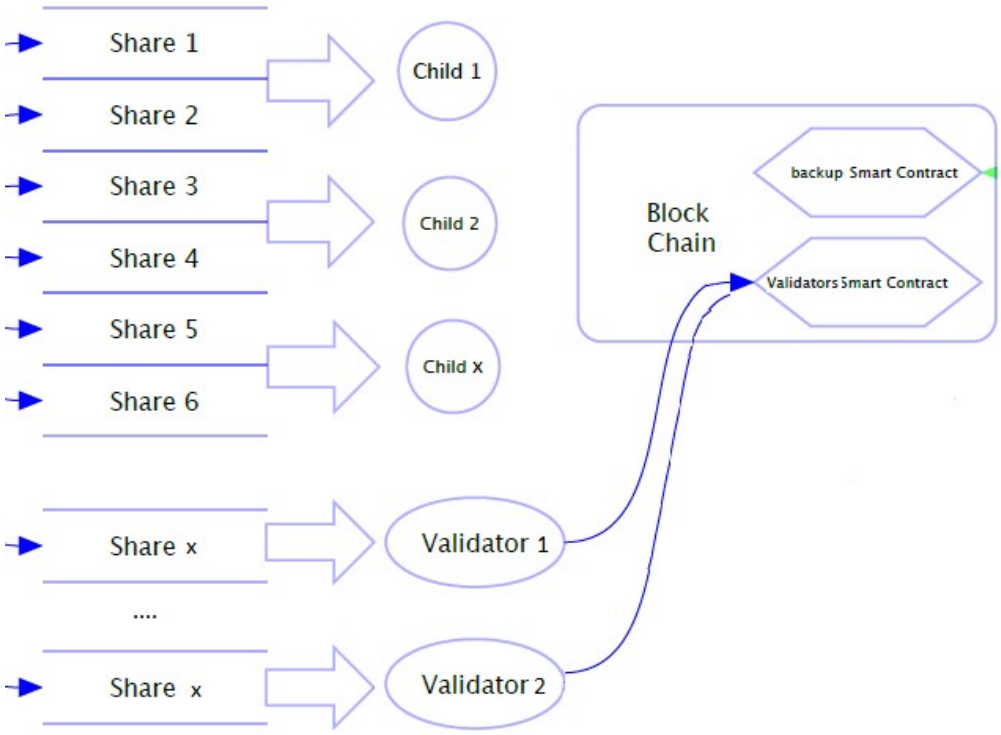


Figure 15 : Multiple validator's scheme

TFC SD **複数のバリデーターの可能性**：

- 誰も永遠ではない、どちらも私たちのアライアンスプログラムに参加した法人です。**我々は以上の 1 つのバリデータを含む信頼のネットワークを構築する機会を提供する理由です。**
- あなたが関与するいくつかのバリデータを持っていることを選択したとき、我々は必要な株式、n 個（**プレイヤー/子供**）-1、**ニバリデーターによって使用することができます保持** blockchain **でバックアップスマート契約を押してください。**
- **これにより、我々は株式分布と検証の面で完全に冗長で信頼のエコシステム**を提供します.

6 SH-アライアンスプログラム

安全なハーベンスアライアンスプログラムは、安全な避難所で審査された法人のグループであり、目標を達成するために必要なすべてのステップを実行し、資産を確保して信頼の未来をスタートさせ、あなたの遺産。

あなたがアライアンスに加わるために借りている法人である場合は、info@safehaven.io までお問い合わせください。私たちが法的基盤を整えるとすぐに連絡を取ります。すべての法的問題に答えるため、早急に専用の信頼アライアンスポータルを立ち上げます。私たちのポータルが立ち上げられるとすぐに、法人は、自分自身を解読できるようになります。もちろん、審査プロセスに役立つ法的証明書が尋ねられます。メンバーは、当社のサービスの購読を得るために年会費を支払うよう求められます。トークンは、スマートコントラクトをブロックチェーンに展開するためのガスとして使用されます。

当社は、現在、当社のアライアンスのメンバーである可能性のある法人の種類を正確に分析しています。私たちは、信頼のサークルに信頼の実体が必要です.

7 SHA 保護計画

1.ファミリーサークルプラン（TFC）

家族サークルプランは親戚を安心させたい人のためのもので、死ぬ日に子供が父親が買収した資産にアクセスできるようにしたい。可能性はほとんど無限であり、秘密を安全かつ透明な方法で保ちながら、行動を柔軟に分けることができます。プロセスにバリデーターを追加するという事実は、プロセスを確実にするために必要な重要な問題に精通しています。私たちは、分権化された部分を維持する私たちのプロセスにブロックチェーンのすばらしい世界を加えます。分散されたインテリジェントデータベースデータベースの検証マッピングは、さらに単純化された次世代秘密交換プロトコルと組み合わせられた追加のセキュリティ機能を追加します。

2.ビジネス継続計画（BCP）

事業継続計画は TFC と非常によく似ていますが、主な違いは、子どもの代わりにステークホルダーの話をしていることと、共有ロック解除の点で検証プロセスが異なることです。公証人は BCP において、私たちのサービスを通して不足している部分を得ることに対する抵抗の医学文書を必要としませんが、彼によって準備された公証法はありません。このプロセス計画は内部的に開発されており、Trust Alliance ポータルがオンラインの瞬間から使用できるようになります。 BCP は、複数の財布、取引所の共有秘密の配布、またはパスワードの保管/インポートのパスフレーズのためにシンプルです。もう一度、可能性は無限です。

3.投資サークル

投資サークルは、友人、家族、またはビジネスに関心を持つ人たちの間で資金を作りたい人のためのものです。 5 人の友人が暗号化に投資し、暗号化された通貨で 1000 ドル相当のものを購入したいとします。あなたのオプションは何ですか？完全に安全であっても、マルチウォレット（最近発見されたすべての障害を含む）を作成するときは、常にグループ内での信頼が必要です…これはどうしたら管理できますか？シンプル！セーフヘイブン株式分配プロトコルを通じて。秘密鍵を数字で表し、パスフレーズを株式に分割し、

利害関係者は同じ金額の株式を受け取る。フェールセーフ機構を持たない公式を考えると、どこにどこに分布するかは、*T*=（y・N-1）+（X・n）、T =（2-1）+（2.5）= 1 + 1 はバリデーター（法人）を介してブロックチェーンに格納されます。この参加を開放するための条件は、価格の閾値からマイルストーンまでの範囲で、単純に 100%のコンセンサスがあることになります。再び、可能性は無限です。

4.安全な避難場所

良いパスワードは暗記するのが難しく、合法的にあなたから親戚に転送することはできません。このパスワードは、Facebook、Gmail またはその他の重要なアカウントからのものであれば何でもかまいません。ご希望の場合は、デジタル遺産があなたと一緒に亡くならないようにしてください。親戚はもはやそこにいなくてもそれらのアカウントにアクセスし、私たちの株式流通プロトコルの 1 つを使用して Safe Haven にブロックチェーンで保存してください。.

8 結論

今日暗号通貨とビットコインへの投資は、多くの時間がかかり、非常に困難である、他の側では、長年にわたって大規模な利益をもたらすでしょう。 これらの資産を確保し、外部から任意の治療に対してそれらを保護することができ、すべてのトレーダーと長期的な投資家は非常に長い時間以来のために求めてきたものです。 私たちは、同じ理由で、このすべての事業である金融独立すると私たちの親類のための安全で安心な未来を築きます。 そのため、私たちは分散型プラットフォームを開発し、世界中にソリューションを提供します。 安全な避難所当社は、あなたのデジタルキーまたは種子を確保し、保存の違いを行います。 安全な避難所のようなソリューションを構築することは、投資家や親戚のために心の中で作品をもたらすでしょう。 私たちは、あなたが当社のプラットフォームとさまざまなソリューションについて確信していると我々は投資家の一人としてあなたを歓迎することができますことを願っています！

9 市場

暗号化通貨は、セキュリティのために暗号化技術を使用するデジタル資産です。暗号化コインは主に商品とサービスの売買に使用されますが、新しい暗号化通貨の一部は所有者に一連のルールや義務を提供する機能もあります。彼らは金のような他の商品と交換できないとい

う意味で、本質的な価値を持っていません。伝統的な通貨とは異なり、中央当局から発行されたものではなく、合法的な入札とはみなされません。

この時点で、暗号化通貨の使用は主に「初回ユーザー」に限定されています。この規模には、世界中に約 1,000 万人の Bitcoin 保有者がおり、投資目的のために Bitcoin が半分程度しかありません。客観的には、政府が支援する通貨が適切に機能するため、暗号通貨は必要ありません。ほとんどのアダプターにとって、クリプトカルトの利点は理論的です。したがって、一般的な採用は、暗号通貨を使用することによる目に見える有益なメリットがある場合にのみ発生します。それらを使用する利点は何ですか？

暗号通貨交換

暗号通貨交換は、他のデジタル通貨または伝統的な通貨でコード化された通貨を購入、販売、交換できる Web サイトです。取引所は、暗号通貨を主要な政府支援通貨に変換し、暗号通貨を他の暗号通貨に変換することができる。最大の取引所には、Poloniex、Bitfinex、Kraken、GDAX などがあり、1 日当たり 1 億ドル以上の交渉が可能です。ほとんどすべての取引所は、政府のマネーロンダリング規制の対象であり、顧客は口座開設時に身元証明を提示する必要があります。

交換の代わりに、商人が個人情報の開示を避けることを可能にする LocalBitcoins のようなサイトを通じて、ピアツーピアトランザクションを使用することがあります。ピエール・ピア・トランザクションでは、参加者は他の仲介業者の参加なしに、ソフトウェアを介して取引において暗号化通信を交換する。

小切手暗号通貨

暗号化された財布を持つ財布は、ユーザーがデジタルコインを送受信し、その残高を監視するために必要です。財布はハードウェアまたはソフトウェアのいずれでもかまいませんが、ハードウェアウォレットはより安全とみなされます。たとえば、Ledger ウォレットは、小型 USB ドライブのように見え、コンピュータの USB ポートに接続します。ビットチェーン勘定のトランザクションと残高はブロックチェーン自体に記録されますが、新しい取引に署名するために使用される秘密鍵は総勘定元帳ウォレットに格納されます。新しいトランザクションを作成しようとすると、コンピュータはウォレットに署名してブロックチェーンに送信します。秘密鍵は決してハードウェアウォレットから離れることはないので、コンピュータがハッキングされたとしてもビットコインは安全です。ただし、バックアップしない限り、ウォレットを紛失すると、所有者の資産が失われます。逆に、コインウォレットのようなソフトウェアウォレットは仮想です。このタイプのソフトウェアデバイスは、追加のリスクを伴うウォレットプロバイダが所有者の資金をオンラインに置くことができます。

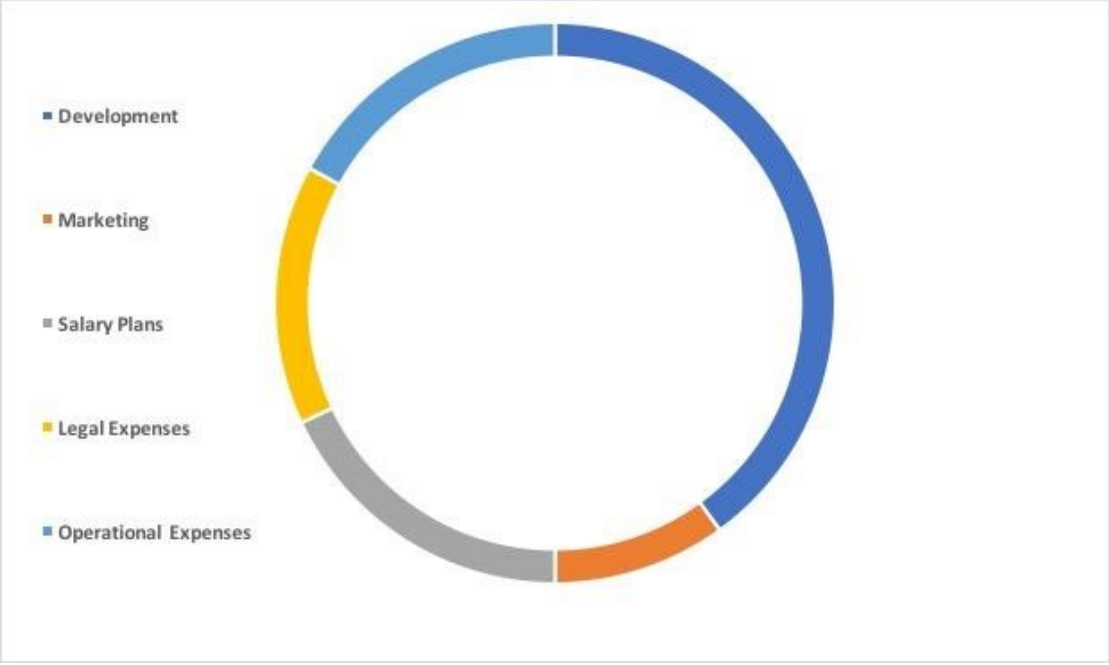
より多くの人々とより多くのお金が暗号化通貨のための市場に流入するにつれて、より多くの人々はバッグまたは財布を開いてプライベートキーを取得しなければならない。 Safe Haven は完璧なソリューションを構築しています。基本的に、財布を開封し、暗号化された通貨を購入する人は、セーフヘイブンの顧客になることができます。この市場で成長する可能性は非常に高いです！ セーフヘイブンは違いを生み出すと確信しています.

10 トークン

SHA-トークンはイーサリアムの上に構築された ERC20 トークンです。 ERC20 規格は、開発者がホイールに新しいトークンシステムが導入されるたびに再発明することなく、箱から出したトークンで動作する分散型アプリケーション（Dapps）を設計することを可能にするためにイーサリアムの blockchain に導入されました。 したがって、ERC20 で、アイデアを持つ人は、プラットフォームの設計プロセス全体を経ることなく、blockchain で製品を展開することができます。 ERC20 では、Ethereum ベースの SHA が遵守するための共通のルールセットを定義できます。 私たちは、トークンが標準に基づいてどのように動作するかを事前に知ることができます。 SHA トークンは、このホワイトペイパーで説明した壊れた市場を癒すために開発されました。 開発の第一段階は、我々が作成しているトークンの量に関係します。 SHA トークンはプロセス中のガスとして使用されます.

11 資金配分

- **開発** 40%
- **マーケティング** 10%
- **給与制度** 18%
- **法的経費** 15%
- **運用経費** 17%



私たちは、プラットフォームの観点で開発を容易にするために調達した資金の大きなシェアを割り当てることを目指しています。 したがって、資金の 40％がこのイニシアチブに向けて移動します。 バウンティキャンペーンやシグネチャキャンペーンなど、さまざまなマーケティング活動を促進するために、資金の 10％が配分されます。 15％が取引所のような法的市場

に割り当てられます。ファンドから 17％が運用コストのためであり、18％が給与プランに割り当てられます。

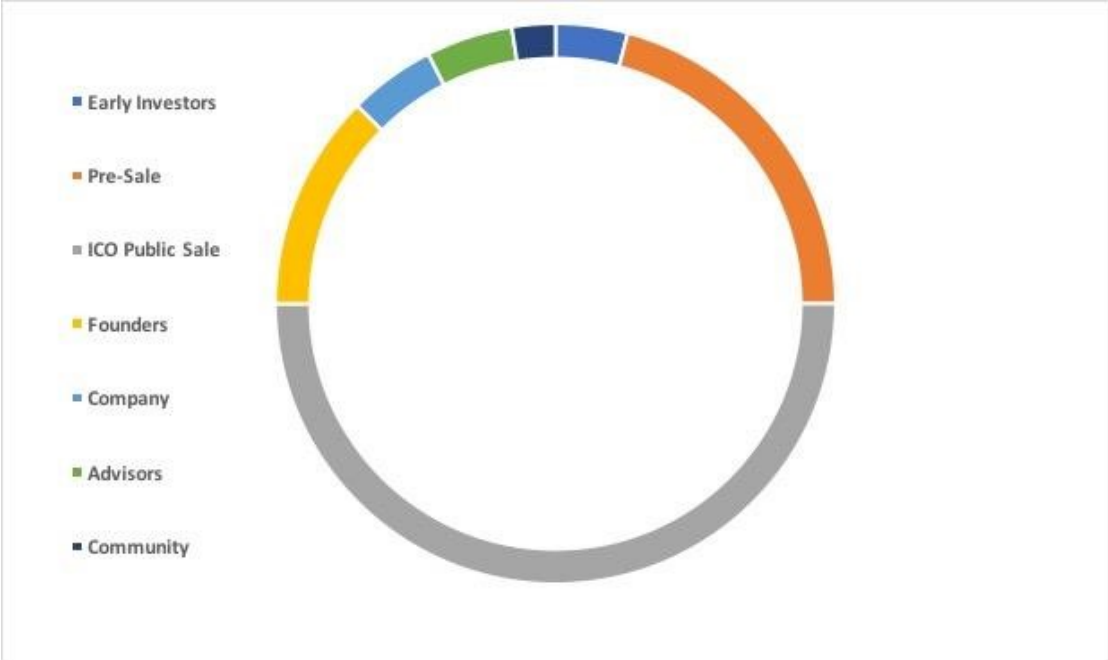
12 ICO パラメータ+トークンの割り当て

ティッカー：SHA
総供給：120,000,000
エテリアムベースのトークン（ERC20）
ICO 開始日：SEE https://ico.safehaven.io
プレセール開始日：https://safehaven.io/#pre-sale を参照してください
初期投資家の為替レート：2500 SHA = 1ETH
為替レートの事前販売：2000 年の SHA = 1 ETH
為替レート ICO：1500 SHA = 1 ETH
最小キャップ：1000 ETH
最大キャップ：54,500ETH

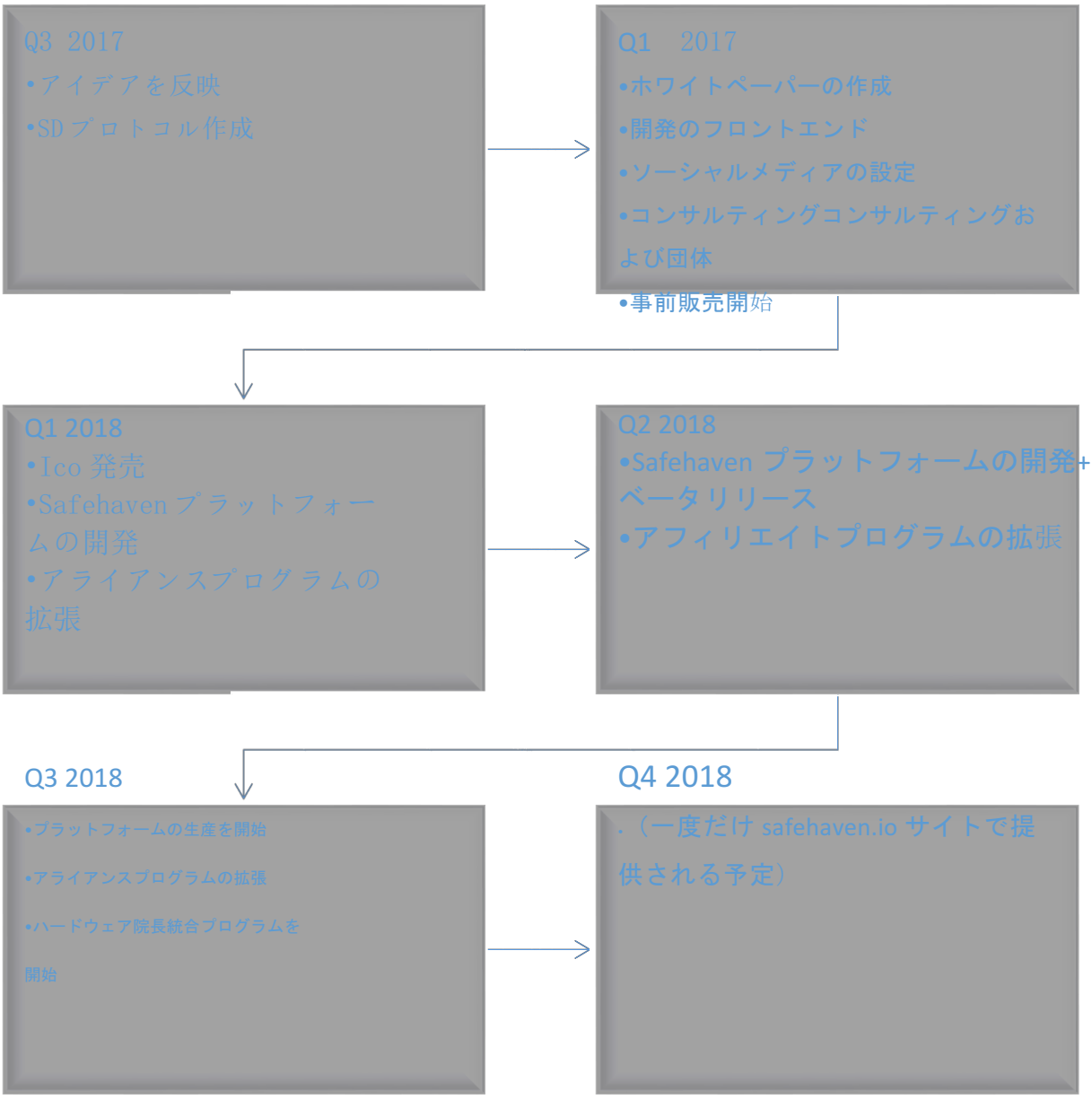
すべての未塗装の土金は焼かれます

トークンの割り当て

ICO 早期投資家：2500 SHA / ETH 合計（5,000,000 SHA）
ICO 前売り：2000 年 SHA / ETH 合計（25,000,000 SHA）
ICO 公開販売：1500 SHA / ETH 合計（60,000,000 SHA）
創業者：15,000,000 SHA
会社：6,000,000 SHA
アドバイザー：6,000,000 SHA
コミュニティ＆バウンティ：3,000,000 SHA


Early Investors
Pre-Sale
ICO Public Sale
Founders
Company
Advisors
Community

13 ロードマップ


Q3 2017
•アイデアを反映
•SDプロトコル作成
Q1 2017
•ホワイトペーパーの作成
•開発のフロントエンド
•ソーシャルメディアの設定
•コンサルティングコンサルティングおよび団体
•事前販売開始
Q1 2018
•Ico 発売
•Safehaven プラットフォームの開発
•アライアンスプログラムの拡張
Q2 2018
•Safehaven プラットフォームの開発+ベータリリース
•アフィリエイトプログラムの拡張
Q3 2018
•プラットフォームの生産を開始
•アライアンスプログラムの拡張
•ハードウェア院長統合プログラムを開始
Q4 2018
.（一度だけ safehaven.io サイトで提供される予定）