

瓦贝公链白皮书

更安全的去中心化电子现金体系

(version1.0, 2018.07)

目录

1	概述.....	3
2	比特币系统的不安全因素.....	5
	比特币挖矿.....	5
	私钥丢失的风险.....	8
3	瓦贝公链.....	10
	瓦贝账户.....	10
	挖矿.....	10
	反池技术.....	12
4	瓦贝钱包.....	14
5	其他.....	17
	瓦贝公链应用.....	16
	货币和发行.....	17
	结论：最安全的去中心化电子现金体系.....	18

概要

中本聪设计比特币的目的，就是希望能够实现一种完全基于点对点网络的电子现金系统，在没有任何资产担保、内在价值或者中心发行者的情况下维持着价值，并使在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的中介机构。总结来说，他希望比特币能够实现以下这些目标：

- 1、不需要中央机构就可发行货币
- 2、不需要中介机构就可完成支付
- 3、保持使用者匿名
- 4、交易无法被撤销

从电子现金系统的角度来看，以上这些目标在比特币系统中基本都得到了实现。但随着比特币市场的迅速发展，也出现了一些新的安全问题，比如算力集中化、交易账户安全比特币永久丢失导致流通量减小等。于是建立一种没有上述风险的更加安全的电子现金系统就成了瓦贝公链的设计初衷。

最大的威胁来自于算力的集中化，比特币挖矿算法基于一种名为 SHA-256 的加密算法，在挖矿过程中，矿工将比特币的 80 个字节长度的区块头数据进行两次 SHA256 运算，运算结果就是一个 256 位（32 字节）长度的字符串。通过比较与当前难度值的大小判断当前区块是否合法。然而，这种挖矿算法容易被中心化攻击。目前挖矿生态系统被专门设计的因而在比特币挖矿这一特殊任务上效率提高上千倍的 ASICs（专用集成电路）和电脑芯片控制。这意味着比特币挖矿不再是高度去中心化的和追求平等主义的，而是需要巨额资本的有效参与。

电子现金系统之外，比特币技术还有另外一层含义，区块链怎样应用于货币以外的领域。但比特币的智能合约缺少图灵完备，这限制了它在各行各业的应用。瓦贝公链的目标就是提供一个带有内置的成熟的图灵完备语言的区块链系统，用这种语言可以创建合约来编码任意状态转换功能，只要简单地用几行代码来实现逻辑，就能够创建以上提及的所有系统以及许多我们还想象不到的其它系统。

比特币系统的不安全因素

去中心化的数字货币概念，早在几十年以前就被提出来了。1974 年诺贝尔经济学奖获得者弗里德里希·冯·哈耶克《货币的非国家化》就是这一思想的集中体现。但由于市场、技术、模式等方面的限制，直到中本聪提出比特币概念，去中心化的数字货币才逐渐流行开来。

中本聪引入这样一个理念：将一个非常简单的基于节点的去中心化共识协议与工作量证明机制结合在一起。节点通过工作量证明机制获得参与到系统的权利，每十分钟将交易打包到“区块”中，从而创建出不断增长的区块链，拥有大量算力的节点有更大的影响力。尽管比特币区块链模型非常简陋，但实践证明它已经足够好用了。

目前比特币已经是全球最主流的数字货币，拥有千万甚至上亿的持有者、数以千计的矿池、上万种以比特币系统为基础的应用。但市场也在考验着比特币系统，不断地为其创造新的问题。

比特币挖矿

前文已经提到，作为一种去中心化的数字现金系统，比特币将一个基于节点的去中心化共识协议与工作量证明机制结合在一起。比特币的去中心化共识进程要求网络中的节点不断尝试将交易打包成“区块”。网络被设计为大约每十分钟产生一个区块，每个区块包含一个时间戳、一个随机数、一个对上一个区块的引用（即哈希）和上一区块生成以来发生的所有交易列表。这样随着时间流逝就创建出了一个持续增长的区块链，它不断地更新从而能够代表比特币账本的最新状态。依照这个范式，检查一个区块是否有效的算法如下：

- 1、检查区块引用的上一个区块是否存在且有效。
- 2、检查区块的时间戳是否晚于以前的区块的时间戳，而且早于未来 2 小时。
- 3、检查区块的工作量证明是否有效。
- 4、将上一个区块的最终状态赋于 $S[0]$ 。
- 5、假设 TX 是区块的交易列表，包含 n 笔交易。对于属于 $0 \cdots n-1$ 的所有 i ，进行状态转换 $S[i+1] = \text{APPLY}(S[i], \text{TX}[i])$ 。如果任何一笔交易 i 在状态转换中出错，退出程序，返回错误。返回正确，状态 $S[n]$ 是这一区块的最终状态。

区块验证算法的有趣部分是“工作量证明”概念：对每个区块进行 SHA256 哈希处理，将得到的哈希视为长度为 256 比特的数值，该数值必须小于不断动态调整的目标数值。工作量证明的目的是使区块的创建变得困难，从而阻止女巫攻击者恶意重新生成区块链。因为 SHA256 是完全不可预测的伪随机函数，创建有效区块的唯一方法就是简单地不断试错，不断地增加随机数的数值，查看新的哈希数值是否小于目标数值。如果当前的目标数值是 2^{192} ，就意味着平均需要尝试 2^{64} 次才能生成有效的区块。一般而言，比特币网络每隔 2016 个区块重新设定目标数值，保证平均每十分钟生成一个区块。为了对矿工的计算工作进行奖励，每一个成功生成区块的矿工有权在区块中包含一笔凭空发给他们自己 12.5BTC 的交易。另外，如果交易的输入大于输出，差额部分就作为“交易费用”付给矿工。

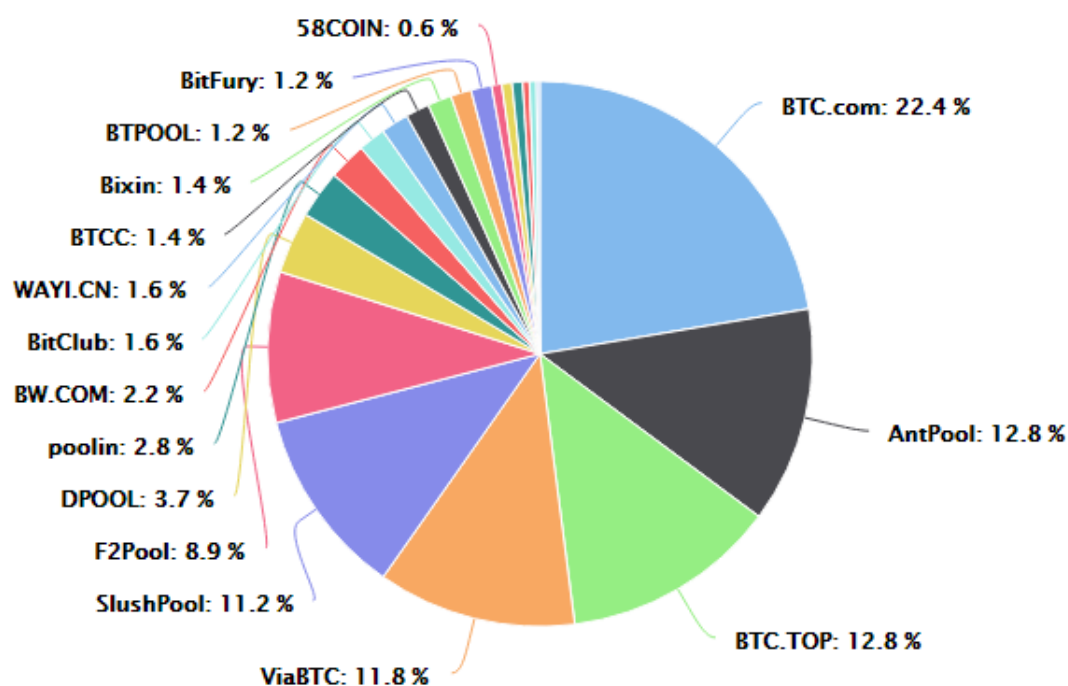
因为比特币的密码学基础是非常安全的，所以攻击者会选择攻击没有被密码学直接保护的部分：交易顺序。攻击者的策略非常简单：为了更好地理解挖矿的目的，让我们分析比特币网络出现恶意攻击者时会发生什么。

- 1、向卖家发送 100BTC 购买商品（尤其是无需邮寄的电子商品）。
- 2、等待直至商品发出。
- 3、创建另一笔交易，将相同的 100BTC 发送给自己的账户。
- 4、使比特币网络相信发送给自己账户的交易是最先发出的。

一旦步骤（1）发生，几分钟后矿工将把这笔交易打包到区块，假设是第 270000 个区块。大约一个小时以后，在此区块后面将会有五个区块，每个区块间接地指向这笔交易，从而确认这笔交易。这时卖家收到货款，并向买家发货。因为我们假设这是数字商品，攻击者可以即时收到货。现在，攻击者创建另一笔交易，将相同的 100BTC 发送到自己的账户。如果攻击者只是向全网广播这一消息，这一笔交易不会被处理。矿工会运行状态转换函数 $\text{APPLY}(S, \text{TX})$ ，发现这笔交易将花费已经不在状态中的 UTXO（未花费的交易输出，Unspent Transaction Output）。所以，攻击者会对区块链进行分叉，将第 269999 个区块作为父区块重新生成第 270000 个区块，在此区块中用新的交易取代旧的交易。因为区块数据是不同的，这要求重新进行工作量证明。另外，因为攻击者生成的新的第 270000 个区块有不同的哈希，所以原来的第 270001 到第 270005 的区块不指向它，因此原有的区块链和攻击者的新区块是完全分离的。在发生区块链分叉时，区块链长的分支被认为是诚实的区块链，合法的矿工将会沿着原有的第 270005 区块后挖矿，只有攻击者一人在新的第 270000 区块后挖矿。攻击者为了使得他的区块链最长，他需要拥有比除了他以外的全网更多的算力来追赶（即 51% 攻击）。

- 算力集中化

理论上，个人或单个组织很难拥有比全网更多的算力来破坏比特币系统的运行。但由于市场原因（大矿池的收益相对来说更加稳定，小矿池的收益往往显示出很大的波动性）以及比特币 ASICs 矿机的流行，算力集中化趋势不可避免，资本有实力也有意愿去构建大型矿池。目前全球前三大矿池占据了全网约 48% 的算力。



比特币算力分布

更严重的事故发生在 2013 年 11 月,比特币矿池 GHash.io 对赌博网站 BetCoin Dice 进行多次付款欺诈。康奈尔大学研究表明,自 2014 年,6 月 3 日以来,GHash 已经达成了至少 5 次超过 51% 的加密散列运算量。在其中某个时期,这一过程甚至持续了 12 个小时。

私钥丢失的风险

尽管比特币的密码学基础是非常安全的,无法被暴力破解,同时控制全网 51% 的算力也存在一定难度,但这并不意味着黑客就没有办法盗取比特币。在一个比特币账户中,有一组 34 个字符的比特币地址,可以用来接收比特币,并且每个地址都有一个相关的 64 个字符的私钥,可以使用它来发送比特币。因此当某人拥有比特币时,他们实际上拥有的是用于解锁区块链上特定地址的私钥。这些私钥可以在线存储,也可以离线存储,它们都有一定的安全级别。私钥必须被安全地管理好,只有你签署一笔转账时才需要用到,比特币地址可以自由地分发到全世界。这就是比特币钱包的原理。当你的私钥是安全的,那么一切都好,如果你失去了你的私钥,那么你的所有资金都没有了。

通常黑客们会用键盘记录、钓鱼软件、货币木马等方式盗取用户的私钥。键盘记录恶意软件会记录用户的按键并将其内容全部发送给黑客,完整的检测到这些恶意程序几乎是不可能的,这些程序往往兼容移动与 PC 端,而你根本没有注意到,他们会复制你输入的每一个 seed、密码和 PIN 码,最终成功破解比特币交易网站后台;钓鱼 APP 会伪造成官方应用程序,通常使用官方标识和现有比特币钱包等信息来欺骗用户,窃取比特币;货币木马则会在感染电脑后会不断扫描用户粘贴板中的内容,当用户复制虚拟货币的支付地址

时，该病毒会自动修改粘贴板中的支付地址信息，从而给大意的用户造成损失。

根据公开信息，被盗的比特币数量约为 200 万枚，占比特币总发行量的 9.5%，并且这一数字还在不断增长。最新的例子是，2018 年 4 月 13 日，印度比特币交易所 Coinsecure 平台，被黑客窃取了 438 个比特币，当时价值 330 万美元。

瓦贝公链

瓦贝公链的目的是创建一个更加安全的去中心化电子现金系统，它基于密码学原理而不基于信用，不仅可以使得任何达成一致的双方，能够直接进行支付，从而不需要第三方中介；并且还能有效的预防算力的中心化，最大程度减少对大型矿池的依赖。

瓦贝账户

在瓦贝公链系统中，状态是由被称为“账户”（每个账户由一个 20 字节的地址）的对象和在两个账户之间转移价值和信息的状态转换构成的。瓦贝公链的账户包含四个部分：

- 1、随机数，用于确定每笔交易只能被处理一次的计数器
- 2、账户目前的瓦贝的余额
- 3、账户的合约代码，如果有的话
- 4、账户的存储（默认为空）

瓦贝是瓦贝公链内部的主要加密燃料，用于支付交易费用。一般而言，瓦贝公链有两种类型的账户：外部所有的账户（由私钥控制的）和合约账户（由合约代码控制）。外部所有的账户没有代码，人们可以通过创建和签名一笔交易从一个外部账户发送消息。每当合约账户收到一条消息，合约内部的代码就会被激活，允许它对内部存储进行读取和写入和发送其它消息或者创建合约。

挖矿

虽然有一些不同，但瓦贝公链的区块链在很多方面类似于比特币区块链。它们的区块链架构的不同在于，瓦贝公链块不仅包含交易记录和最近的状态，还包含区块序号和难度值。瓦贝公链中的区块确认算法如下：

- 1、检查区块引用的上一个区块是否存在和有效。
- 2、检查区块的时间戳是否比引用的上一个区块大，而且小于 15 分钟。
- 3、检查区块序号、难度值、交易根，叔根和燃料限额（许多瓦贝公链特有的底层概念）是否有效。
- 4、检查区块的工作量证明是否有效。
- 5、将 $S[0]$ 赋值为上一个区块的 $STATE_ROOT$ 。
- 6、将 TX 赋值为区块的交易列表，一共有 n 笔交易。对于属于 $0 \cdots n-1$ 的 i ，进行状态转换 $S[i+1] = APPLY(S[i], TX[i])$ 。如果任何一个转换发生错误，或者程序执行到此处所花费的燃料（gas）超过了 $GASLIMIT$ ，返回错误。
- 7、用 $S[n]$ 给 S_FINAL 赋值，向矿工支付区块奖励。
- 8、检查 S_FINAL 是否与 $STATE_ROOT$ 相同。如果相同，区块是有效的。否则，区块是无效的。

这一确认方法乍看起来似乎效率很低，因为它需要存储每个区块的所有状态，但是事实上瓦贝公链的确认效率可以与比特币相提并论。原因是状态存储在树结构中（tree

structure)，每增加一个区块只需要改变树结构的一小部分。因此，一般而言，两个相邻的区块的树结构的大部分应该是相同的，因此存储一次数据，可以利用指针（即子树哈希）引用两次。一种被称为“帕特里夏树”（“Patricia Tree”）的树结构可以实现这一点，其中包括了对默克尔树概念的修改，不仅允许改变节点，而且还可以插入和删除节点另外，因为所有的状态信息是最后一个区块的一部分，所以没有必要存储全部的区块历史-这一方法如果能够可以应用到比特币系统中，经计算可以对存储空间有 10-20 倍的节省。

反池技术

比特币挖矿算法基本上是让矿工千万次地轻微改动区块头，直到最终某个节点的改动版本的哈希小于目标值。然而，这种挖矿算法容易被两种形式的中心化攻击。第一种，挖矿生态系统被专门设计的因而在比特币挖矿这一特殊任务上效率提高上千倍的 ASICs（专用集成电路）和电脑芯片控制。这意味着比特币挖矿不再是高度去中心化的和追求平等主义的，而是需要巨额资本的有效参与。第二种，大部分比特币矿工事实上不再在本地完成区块验证；而是依赖中心化的矿池提供区块头。目前，最大的三个矿池间接地控制了大约全网 48% 的算力。

瓦贝公链现在的目的是使用一个基于为每 1000 个随机数随机产生唯一哈希的函数的挖矿算法，用足够宽的计算域，去除专用硬件的优势。简而言之，瓦贝公链的挖矿算法运算时需要依赖大量内存（相比之下，运行 SHA256 算法的比特币 ASIC 矿机不需要那么多内存，因此其性能仅受限于其处理器），通常，在高带宽总线上转移数据时这些算法的性能会受限，这使得它很难被 ASIC 化。这样的策略当然不会使中心化的收益减少为零，但是也不需要。注意每个用户使用他们的私人笔记本电脑或台式机就可以几乎免费地完成一定量的挖矿活动，但当到了 100% 的 CPU 使用率之后更多地挖矿就会需要他们支付电力和硬件成本。ASIC 挖矿公司需要从第一个哈希开始就为电力和硬件支付成本。所以，如果中心化收益能够保持在 $(E + H) / E$ 以下，那么即使 ASICs 被制造出来普通矿工依然有生存空间。另外，我们计划将挖矿算法设计成挖矿需要访问整个区块链，迫使矿工存储完成的区块链或者至少能够验证每笔交易。这去除了对中心化矿池的需要；虽然矿池依然可以扮演平滑收益分配的随机性的角色，但这功能可以被没有中心化控制的 P2P 矿池完成地同样好。这样即使大部分普通用户依然倾向选择轻客户端，通过增加网络中的全节点数量也有助于抵御中心化。

另外，我们拟对于已形成的，集中全网算力超过 48% 的区域，触发区域算力定位限制，即对区域节点物理间隔限制节点增加，算力过度集中的区域将迫于管理成本上升而放弃扩张，从而实现整个网络动态平衡。

瓦贝钱包

瓦贝公链提供了一个去中心化的钱包系统——Token-S，Token-S 数字资产管理平台里的钱包、私钥都由本地生成，助记词本地加密存储，本地离线签名交易，完全去中心化最大程度阻止了互联网上黑客的攻击。此外 Token-S 还有如下安全特性。



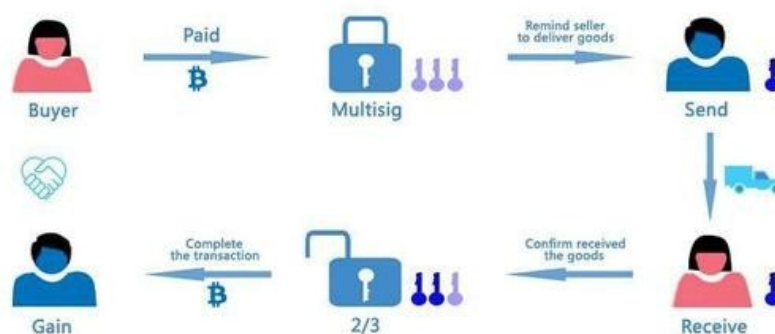
Token-S 轻钱包

智能检测 安全风险超前预警

用户首次登陆 Token-S 钱包，会有针对用户手机设备的智能检测，排查设备是否具有安全风险，提前预警。同时，在初次创建钱包，需设置密码，密码支持不低于 6 位的任意混合字符加密。创建的密码将用于不卸载 APP 情况下找回助记词、发送数字货币。密码不设置找回功能，需要用户牢记密码，密码加密保存于用户本地手机内，而非存放于服务器，完全由用户控制。

多重签名

为了应对黑客盗取私钥的行为，一个简单有效的办法是多重签名。传统的比特币账户中，你的比特币地址中每一个地址都有一个对应的私钥。而多重签名地址，可以有三个相关联的私钥，你需要其中的两个才能完成一笔转账。实际上，你也可以设置成 1/3，5/5，6/11，但是最常见的是 2/3 的组合。



2/3 模式的多重签名

在线钱包中，2 组以上的私钥分别独立存放于不同地点，为了保证钱包安全，钱包 UTC 文件不允许放置于同一地点，否则转账不成功。这样就算任意一个客户端节点被攻破，资金仍然安全。在线钱包是典型的热钱包，与之对应的是冷钱包机制，Token-s 接替了这个任务。

冷钱包

冷钱包是指用户离线完成签名，再通过线上发送签名完成交易，保障密钥永远不触碰网络。具体流程如下，在 Token-s 中可以先离线输入密码，再通过 sendrawTransaction 发送了签名，发送后隔离钱包文件，再次启动网络，这样就可实现密钥不触碰网络的目的，更何况钱包密钥本身就是存放于用户本地。

人工智能验证

瓦贝钱包的去中心化，服务器收到一个待处理的服务时，它会通过复杂的机器学习程序，来检验欺诈模型，考虑到金额，频率，历史，发送 ID 等因素，进行机器交易风险评分。如果风险评分低，交易直接通过。如果风险评分高，节点将向后台反馈，提示人工审核。

全球顶级专业防欺诈系统 打造安全、合规、高信用交易平台

Token-S 采用全球顶级专业防欺诈系统，打造安全、合规、高信用交易平台，交易的数字资产可追溯，资产的来源和去处可查，防止欺诈。同时，Token-S 钱包为了保障用户数字资产安全，将逐步增加了指纹、语音、图案、静脉解锁及复合解锁功能，保证安全的同时使用也更为便捷。

反追溯系统

为了用户资金安全，Token-S 拟将账本 getBalance () 查余通道限制，形成反追溯机制。首先在矿工打包需要查余时，矿工只能知道交易是否符合规则（比如账户余额与即将发生的支出的大小对比），但不能知道具体数额（保护用户隐私）；此外，以太坊等区块链系统提供的 etherscan.io 公共查询浏览器，本身具有安全风险，收款方可以通过匿名查询追溯到用户的每个账户余额，尽管理论上超级计算机需要 65 年才能破解一个用户账户，但现代社会对互联网的高度依赖，人们不得不把一些重要私人信息和行为习惯放到互联网上，大数据带来的安全风险不容忽视，如果黑客获得了大量的用户行为痕迹，破解一个人的账户或许用不了那么长时间。查余通道控制权交回给用户后，黑客失去了觊觎的目标，自然多一份安全。但如此一来我们要对整个传统区块链系统调整，彻底做到这一点是极其复杂而艰巨的。

多链钱包、全币种一站式管理

Token-S 去中心化钱包通过助记词或私钥，可导入创建多个钱包。目前仅支持瓦贝 (WAB) 及其智能合约数字代币，未来将逐步支持比特币及以太坊等各种主流及小众代币，号称全币种管理（比如 ETC、BTC、EOS、DGD 等）。统一管理多个钱包及多种货币，极大的降低了数字货币的使用门槛和管理负担，有效促进了数字资产的灵活应用。

其他

瓦贝公链应用

除了更加安全的电子现金系统，瓦贝公链另一大目的是，使得开发者能够创建任意的基于共识的、可扩展的、标准化的、特性完备的、易于开发的和协同的应用。瓦贝公链通过建立终极的抽象的基础层-内置有图灵完备编程语言的区块链-使得任何人都能够创建合约和去中心化应用，并在其中设立他们自由定义的所有权规则、交易方式和状态转换函数。

一般来讲，瓦贝公链之上有三种应用。第一类是金融应用，为用户提供更强大的用他们的钱管理和参与合约的方法。包括子货币，金融衍生品，对冲合约，储蓄钱包，遗嘱，甚至一些种类的全面的雇佣合约。第二类是半金融应用，这里有钱的存在但也有很重的非

金钱的方面，一个完美的例子是为解决计算问题而设的自我强制悬赏。最后，还有在线投票和去中心化治理这样的完全的非金融应用。

目前瓦贝公链致力于加强非金融类应用的开发，以加强与实体经济的联系，通常这些项目都具有高成长性的特点。目前瓦贝已经在进行白酒项目的数字化，届时瓦贝也可以直接用来购买实体产品。

货币和发行

瓦贝公链包含自身的内置货币瓦贝，瓦贝扮演双重角色，为各种数字资产交易提供主要的流动性，更重要的是提供了支付交易费用的一种机制。

瓦贝公链预制了 2000 枚瓦贝，主链正式上线前将有 200 万枚瓦贝被挖出；上线后，每年都将有约 18.75 万枚，每年密钥丢失、密码忘记、手机丢失、被盗等各种原因导致的损失初步估算在总量的 0.85% 左右，与年产量持平，这就使得瓦贝的整体数量始终保持在 2200 万枚左右。

发行模式如下：

通过发售活动，瓦贝将以每 BTC 500 瓦贝的价格发售。早期购买者会享受较大的折扣，发售所得的 BTC/ETH 等数字货币将完全用来支付开发者和研究者的工资和悬赏，以及投入密码学货币生态系统的项目。

1/3 的瓦贝将被分配给 BTC/ETH 融资或其它的确定性融资成功之前参与开发的早期贡献者，另外一个 2/3 将分配给长期研究项目。

结论：更加安全的去中心化电子现金体系

上述安全机制的使用，使得瓦贝在算力集中和交易安全方面较传统数字货币有更多的优势。它降低了大型矿池的收益，使得联合挖矿成为一件没有必要的事情，因为它并不会显著提高矿工的收益；另一方面，瓦贝提供了更加安全的钱包应用，多重签名、反追溯机制、人工智能的使用，使得再粗心的用户也能有效地防御黑客的攻击。