Vestarin data file systeam官方白皮书（中文翻译）

Vestarin data file：一种去中心化的存储网络的激励机制

Vestarin data file: A Decentralized Storage Network

翻译：Vestarin network foundation

摘　要

随着 5G 技术的到来，互联网正处于一场革命中：集中式专有服务正在被去中心化开放服务所代替；信任式参与被可验证式计算所代替；脆弱的位置寻址被弹性的内容寻址所代替；低效率的整体式服务被点对点算法市场所代替；以比特币为代表的区块链网络通过十年的实践已经证明了去中心化交易账本的有效性。这些系统的参与者们形成去中心化的、没有中心管理机构或者可信任党派的网络提供了有用的数据交互服务。分布式网络技术是新一轮的工业革命，它解放了孤岛数据，网络分区存活，离线工作，审查制度路线，产生了持久的数字信息，真正意义上实现数据永不消失，数据时代的来临，必将迎来人类文明更大的飞跃，推进社会生活生产大变革，社会资源和资本必将重新分配，第四次工业革命正在悄悄来临。人类历史正处于一场新的工业革命时代表格中：数据信息时代（Data information age）已经悄悄来临，正在逐步代替现有的信息时代（Information Age）。

目录

第一章 关于 Vestarin data file

Vestarin data file system 是一个去中心化存储文件系统。这个系统运行在有着本地协议通证（也叫做Vestarin data file）的区块链。区块链中的矿工可以通过为客户提供存储和计算来获取 Vestarin data file token，客户可以通过花费Vestarin data file token 来获得矿工的存储或分发数据资源。

Vestarin data file (VST)是基于 IPFS 协议的一个专门为商品、企业档案、公有云、私有云、企业云等重要数据提供低成本永久性存储做服务的分布式文件系统，在 Vestarin data file system 系统中，对于参与 Vestarin data file 系统生态建设和做出贡献者提供VST 奖励。VST 运行在POC（容量证明）+POST(时空证明,也称为用时用量证明）的证明机制上，有提供存储资源的矿工共同发行。Vestarin data file 协议通过不依赖于单个协调员的独立存储提供商组成的网络提供数据存储服务和数据检索服务。

1.1、基本组件

1.1.1 、去中心化存储网络激励

VST 提供一个存储和检索服务的独立服务商网络机制，Vestarin data file 协议作为激励，可审计和可验证的 DSN 构建;

1.1.2 、证明机制

⑴ 容量证明（Proof-Of-Stak）用户通过验证自己给网络贡献的存储空间和时间获得相应的发行收益；

⑵ “复制证明”（Proof-of-Replication）允许存储提供商证明数据已经被复制到了他自己唯一专用的物理存储设备上了。执行唯一的物理副本使验证者能够检查证明者是否不存在将多个数据副本重复拷贝到同一存储空间；

⑶ “时空证明”（Proof-of-Spacetime）允许存储提供商证明在指定的时间内存储了某些数据。

1.1.3 、可验证市场

将存储请求和检索需求作为两个由 Vestarin data file 网络操作的去中心化可验证市场的订单进行模型进行存储和检索验证。

1.1.4 、有效的工作量

通过“时空证明（用时用量）”来构建有效的工作量证明来应用于共识协议，只有数据存储于网络中，才会占用矿工资。

1.2 协议概述

Vestarin data file 协议是构建于区块链和带有激励通证机制的去中心化存储网络。客户花费通证来购买存储数据和检索数据，而矿工们通过提供存储和检索数据来赚取激励通证。

Vestarin data file DSN 分别通过两个可验证市场来处理存储请求和检索请求：存储市场和检索市场，并采用了“时空证明”和“复制证明”来确保数据的存储。

网络

在每一个纪元 t 的账本 $\mathcal{L}$ 中：

1. 对于每一个新区块：
   (a) 检查区块是否为有效格式
   (b) 检查所有的交易都有效
   (c) 检查所有的订单都有效
   (d) 检查所有的证明都有效
   (e) 检查所有的抵押物都有效
   (f) 如上述任何一个失败则丢弃区块
2. 对于在 t 中引入的每个新订单 o
   (a) 添加 o 到存储市场订单簿
   (b) 如果 o 是报价：锁定 $o.\text{funds}$
   (c) 如果 o 是询价：锁定 $o.\text{space}$
   (d) 如果 o 是成交订单：运行 Put.AssignOrders
3. 对于存储市场订单簿中的每一个 o
   (a) 检查 o 如果过期（或取消）了：
   - 从订单簿中移除 o
   - 退换未动用的资金 $o.\text{funds}$
   - 从分配表中解放 $o.\text{space}$

   (b) 如果 o 是成交订单，通过运行 Manage.RepairOrders 检查预期证明是否存在：
   - 如果有一个失踪，则惩罚 $\mathcal{M}$ 的抵押物
   - 如果证明已经失踪了 Δ_{fault} 个纪元以上，取消订单并且重新将其推向市场
   - 如果无法从网络中取回和重建该碎片，则取消订单并为客户退款

客户

在任何时候：

1. 通过 Put.AddOrders 提交新的存储订单
   (a) 通过 Put.MatchOrders 寻找匹配订单
   (b) 向匹配成功的矿工 $\mathcal{M}$ 发送文件
2. 通过 Get.AddOrders 提交新的检索订单
   (a) 通过 Get.MatchOrders 寻找匹配订单
   (b) 与 $\mathcal{M}$ 构建支付通道

从存储矿工 $\mathcal{M}$ 收到 o_{deal}

1. 签署 o_{deal}
2. 通过 Put.AddOrders 将其提交到区块链

从检索矿工 $\mathcal{M}$ 收到 (p_i)

1. 签署它
2. 向 $\mathcal{M}$ 发送一个小额款项

存储矿井

在任何时候

1. 通过 Manage.PledgeSector 更新过期的抵押
2. 通过 Manage.PledgeSector 抵押新的存储
3. 通过 Put.AddOrder 提交新的询价订单

在每一个纪元 t：

1. 对于订单簿中的每一个 o_{ask}：
   (a) 通过 Put.MatchOrders 寻找匹配订单
   (b) 通过联系匹配的客户开始新的交易
2. 对于每一个被抵押的扇区：
   (a) 通过 Manage.ProveSector 生成存储证明
   (b) 如果有时间发布证明（每个 Δ_{fault} 纪元），将其提交到区块链

从客户 $\mathcal{C}$ 接受到碎片 p：

1. 检查碎片是否具有订单 o_{bid} 中制定的尺寸
2. 创建 o_{deal} 并签署、发送给 $\mathcal{C}$
3. 在扇区中存储碎片
4. 如果扇区满了，则运行 Manage.SealSector

检索矿井

在任何时候

1. 向网络广播询价订单
2. 从网络收听出价订单

从客户 $\mathcal{C}$ 接受到检索请求：

1. 与 $\mathcal{C}$ 开始搭建支付通道
2. 将数据分为多份
3. 只有在收到付款时才发送

图 1：Vestarin data file 协议草图

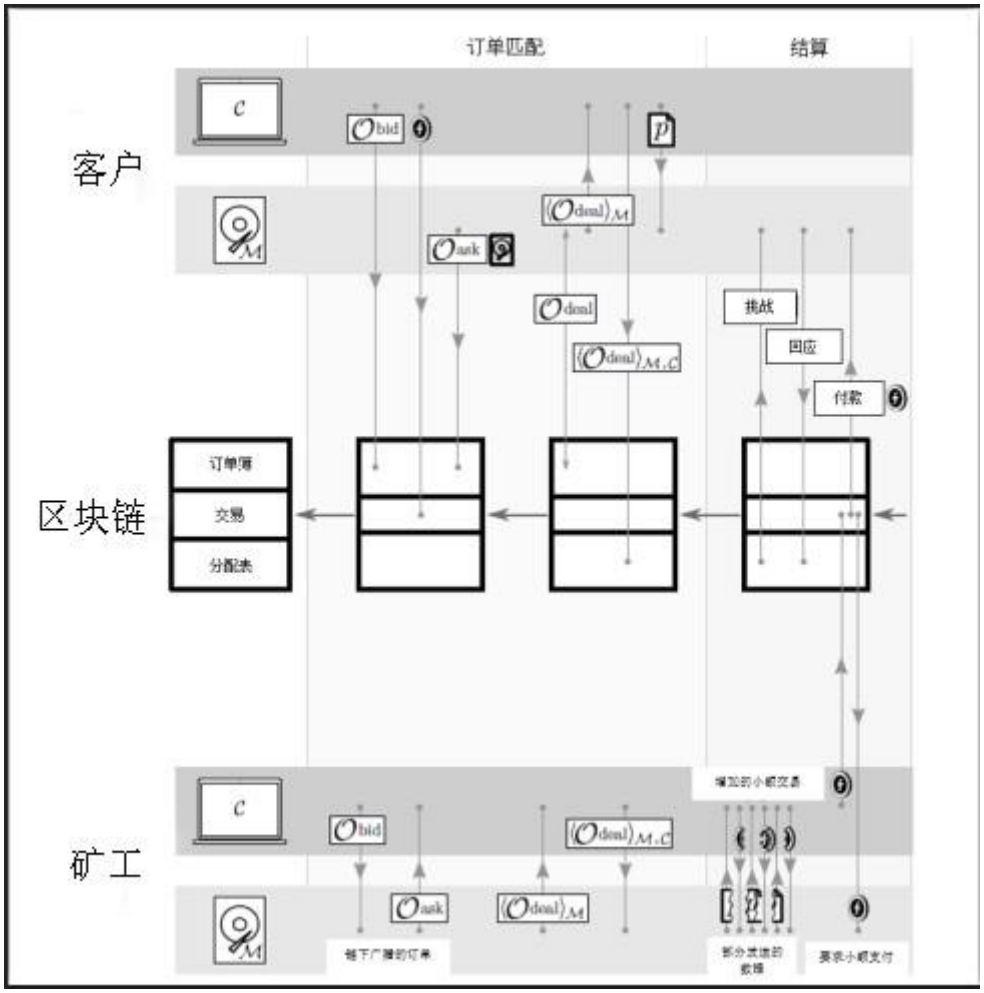

图 2：Vestarin data file 协议实例与用户矿机交互

第二章 去中心化存储网络的定义

去中心化存储网络（DSN）是由多个独立存储提供商提供的存储，并且能自我协调的提供存储数据和检索数据服务给客户。这种协调是去中心化的、智能合约信任的：通过协议的协调与个体参与者能实施验证操作，系统可以获得安全性操作。DSN 可以根据实际的系统需求采取不通的策略。

2.1 DSN 存储提供商和客户运行协议

(Go, Get, Control)

Go data) → key：客户端执行 Go 协议将数据存储生成一个唯一的哈希密钥;

Get(key) → data：终端通过 Get 协议来检索哈希密钥内所存储的数据;

Control（ ）：控制协议：控制可用的存储，检索提供商提供的服务，并且经常与客户或者审计网络结合。

DSN 方案(Π)必须保证数据的完整性和可恢复性，并且能够容忍在后面章节中所定义的管理和存储故障。

2.2 数据完整性和数据同步

2.2.1 数据完整性

客户在 Go 操作结束的时候不接任何被更改或者伪造的数据。

如果有任意成功的 Get 操作将数据 d 设置在键 k 下，呢么客户在对键k 执行 Get 操作结束的时候不再接受非 d 的数据。

2.2.2 数据同步

如果有些数据已经成功存储并且存储提供商继续遵循协议，那么客户最终能够检索到数据；如果有任意成功的 Go 操作将数据 d 设置在键k 下，且存在一个成功的客户 Get 操作通过对键K 执行检索得到数据。

第三章 容量证明与时空证明

在 Vestarin data file 协议中，存储供应商必须让他们的客户确信，客户的付费存储数据已经被他们存储；在实践中，存储供应商们会生成“容量证明”（POC）来让区块链网络（或客户自己）验证。

3.1 容量证明

容量证明（POC），即允许一个将数据外包给服务器（即证明人 P）的用户（即验证者 V）可以反复检查服务器是否依然存储数据 D。用户可以用比下载数据更高效的方式来验证他外包给服务器的数据的完整性。服务器通过对一组随机数据块进行采样和传送少量数据来生成拥有的概率证明作为给用户的挑战 / 响应协议。

3.2 时空证明 Proof-of-Spacetime

容量证明（POC）通过检查存储提供商当时是否已经存储了外包数据。但如何证明数据在一段时间内一直都已经被存储？因此需要一个定时器在特定的时间间隔内对存储提供商进行检索。然而每次交互所需要的通信复杂度会对网络造成重大的负担。

“时空证明”（用使用量证明）提供了科学的解决方案验证存储提供商是否在一段时间内存储了它的外包数据，通过有序的存储序列来作为确定时间，组成递归执行来生成简单的证明。

3.3 存储应用

Vestarin data file 协议采用”时空证明“来审核矿工提供的存储。在 Vestarin data file 中使用POST，任何网络成员都能够验证的非交互式。

第四章 DSN 构建

Vestarin data file DSN 是一个去中心化的存储网络，可审计、可公开验证并根据激励模式进行设计。客户通过消耗矿工网络资源进行数据的存储数据和检索；矿工提供磁盘空间、时间和带宽来换取报酬。矿工只有当网络能够审计他们的服务被正确提供时，才能收到他们的报酬。

4.1 结构

4.1.1 参与者

Vestarin data file 网络的参与者为应用客户、存储矿工和检索矿工，客户在 DSN 中通过Go 和 Get 请求存储数据或者检索数据， 并为此付费。

矿工为网络提供数据存储服务，通过提供磁盘空间和响应 Go 请求来参与 Vestarin data file，并获得 VST 的发行权益和应用收益，矿工通过特定的检索程序进入 VST 网络。为保障矿工提供存储资源的稳定性和确保 Vestarin data file 参与者的质量，矿工可以

通过权益合约（POS）来证明身份的可靠性。除此之外，矿工还需要为网络提供数据检索，提供Go 请求所需要的数据。

4.1.2 网络

运行Vestarin data file 全节点组成了VST 网络。Vestarin data File system 区块链的每个新块,全节点管理可用的存储，验证存储的数据， 审核同步块数据，确保数据永不丢失。

4.2 数据结构

块数据：块数据是客户在 DSN 所存储数据的基础单元，接入 Vestarin data file 网络的数据被划分为许多块数据，每个快数据最大容量为 256 字节，由不同集合的存储矿工来存储。

扇区：扇区是存款矿工向网络提供的一些磁盘空间。矿工将客户数据的碎片存储到扇区，并通过他们的服务来赚取 VST。

分配表：分配表式衣柜数据结构，可以跟踪碎片和其分配的扇区。该表用来保持DSN 的状态，可以快速查找到块数据。

订单：客户向网络提交投标订单来请求服务，并根据空间优先原则分配给矿工。

订单簿：订单簿是订单的集合。

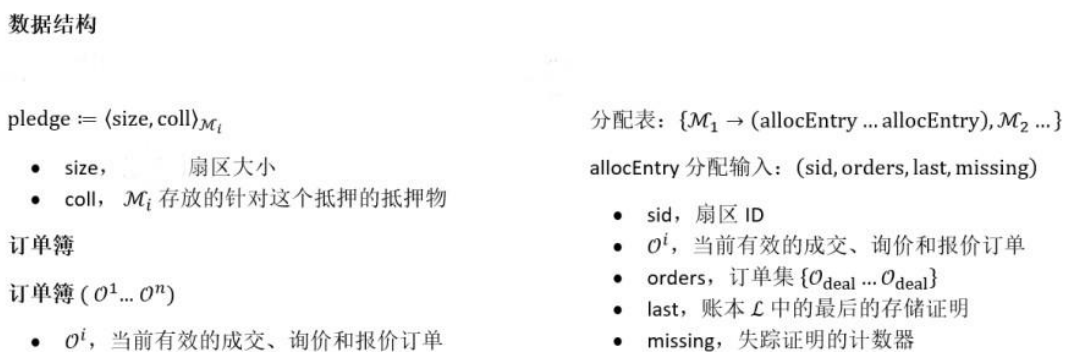

图 3：DSN 方案中的数据结构

4.3 协议

4.3.1 交易

客户通过向Vestarin data file 中的矿工支付Token 来获得数据存储服务和数据检索服务，双方对交易订单进行签名提交到区块链来确认交易成功。

4.3.2 挖矿

1.、提供存储容量：矿工向网络提供存储容量，并通过检索程序来验证可用容量。

2.、接收订单：存储 矿工从存储市场获取存储请求。他们设定价格并通关过 Go.AddOrders 向市场订单簿提交报价订单，一旦抵押交易出现在区块链中，矿工就能在存储市场中提供他们的存储。Go.AddOrders• inputs: list of orders O1..On• outputs: bit b, equals 1 if succe ssful 通过 Go.MatchOrders 来检查是否和客户的报价订单匹配一致。

Go.MatchOrders• inputs:

– the current Storage Market OrderBook

– query order to match

Oq• outputs:

matching orders O1.On

一旦订单匹配，客户会讲他们的数据发给矿工。存储矿工接收到数据的时候，运行 Go.ReceivePiece 。 数据被接收完之后，矿工和客户签收订单并将其提交到区块链。

Go.ReceivePiece

• inputs:

– signing key for Mj

– current orderbook OrderBook

– ask order Oask

– bid order Obid

– piece p

3、封装：把文件分片成矿工存储碎片，把碎片写进矿工的扇区中，网络通过分配表来跟踪每个存储矿工的扇区。当存储矿工的扇区填满了，这个扇区就被有序封装起来，然后将扇区中的数据转换成为副本，再将数据的唯一物理副本与存储矿工的公钥相关联。

4、证明：当矿工分配数据时，必须生成容量证明以保证他们正在存储数据，并由网络来验证。

4.3.3 记账

1、订单匹配：从用户获取数据的请求，向订单簿增加订单，并通过向网络发送报价单来提供数据。

2、数据推送：一旦订单匹配，矿工就将数据发送给客户，当数据被接收完成，矿工和客户就将交易结果提交到区块链。

4.4 数据存储

Vestarin data file DSN 实现完整性、可检索性，可验证性和激励兼容性。

实现完整性：数据碎片以加密哈希命名。一个 Go 请求后，客户只需要存储哈希即可通过 Get 操作来检索数据，并可以验证收到的数据的完整性。

实现可恢复性：在 Go 请求中，客户指定副本因子和代码期望擦除类型。例如分配给 n 个矿工存储数据，最多可允许 m 个故障，则该方式是(m,n)tolerant 存储。通过把数据存储在不同的矿工，以防矿工下线后能迅速进行数据同步，确保数据永不消失。

可验证和可审核性：矿工需要提交其存储的证明到区块链。网络中的任意用户都可以在不访问外包数据的情况下验证这些证明的有效性。另外由于这些证明都是存储在区块链上的，所以操作痕迹可以随时审核。

实现保密性：如果客户希望他们的数据被隐私存储，那客户必须在数据提交到网络之前先进行加密。

第五章 Vestarin data file 市场

有需求就有市场，Vestarin data file 专注于大型档案类资料安全存储的市场，以现有的图书馆、档案室、归档数据为主要客户。客户为矿工存储数据而支付VST 通证费用。

5.1 验证市场

交易市场是促进特定商品和服务交换的协议。它们使得买家和卖家进行交易。交易是可验证的，去中心化网络的参与者必须能够在买家和卖家间验证交易，它没有单一的实体来管理交易，它是透明的， 任何人都可以匿名参与。验证市场协议使得商品/服务的交易去中心化: 订单簿的一致性、订单结算和服务的正确执行可以由参与者——Vestarin data file 里面的矿工和全节点——各自独立验证。

5.2 存储市场

存储市场是验证市场，客户有存储数据的需求，矿工存储空间的供应。

5.2.1 需求

人类有着数千年的文明发展历程，但从文明的传递中，大多数消失在历史的长河中。VST 的使命就是为了数据永不消失。图书巨著

资料、档案、文件封存，这些是当前市场的刚性需求。而 Vestarin data network 分布式存储网以低成本、高稳定、数据永不消逝等特点，给这些需求市场提供最佳的解决方案。

5.2.2 协议

客户和矿工将交易信息提交到订单簿，当订单匹配时，客户将数据碎片传输给矿工，双方将交易结果提交到订单簿。矿工将扇区所包含的碎片封装，并将其定期提交到网络，网络必须验证矿工进行复制广播。

第六章 工作原理

Vestarin data file DSN 协议可以在任何允许验证的共识协议之上实现 Vestarin data file 的证明。Vestarin data file 矿工生成“时空证明”来参与共识，而不是浪费的 POW 计算。如果计算的输出对网络来说是有价值的，而不仅仅是为了保证区块链的安全，矿工在共识协议中所作的工作是有用的。

6.1 Vestarin data file 共识

公开：网络中当前正在使用的存储总量是公开的，通过读取区块信息，可以调取矿工的存储任务，计算出在任意时间点的每个矿工的功率和总功率。

可验证：对于每个存储任务，矿工都需要生成”时空证明“，证明

持续提供服务；通过区块信息，可以验证矿工的功率声明的正确性。

6.2 时空证明

每个矿工们都必须向网络提交“时空证明”，只有网络中大多数功率认为它们是有效的，才会被添加到区块链。在每个区块中，每个节点会更新分配表，添加新的存储分配、删除过期的和标记缺少证明的记录。

节点验证：如果节点拥有完整的区块链记录，则可以从创始块开始运行网络协议直到当前区块，这个过程中验证每一个节点的“时空证明”。

存储验证：客户端可以通过访问广播最新区块的信任源，从网络中的节点访问当前分配表中的记录，该记录被包含在最新区块的状态树中的路径，从创世块到当前区块的区块，这样请客户端就可以将“时空证明”的验证委托给网络。

第七章 智能合约

Vestarin data file 为终端用户提供了 Go 和Put 基元，客户以较低的成本存储数据并从市场中检索数据，通过智能合同的数据碎片的存储或检索请求进行编程。

7.1 系统数据交互

智能合约使得 Vestarin data file 的用户可以编写有状态的程

序，通过消耗激励通证向网络请求存储数据，通过将交易发送到账本触发合约中的功能函数来与智能合约交互。

用户可以将程序关联到其他系统（如以太坊）他们的交易上,他们不直接依赖存储的使用。

7.2 跨链交互

将 Vestarin data file 存储带入其他基于区块链的平台，同时也将其他平台的功能带入 Vestarin data file。

Vestarin data file 进入其他平台：其他的区块链系统，如比特币、Ethereum 和 EOS 等，允许开发人员写智能合约；然而，这些平台缺乏存储能力，因此将存储和检索支持带入这些平台，填补期无存储能力的缺陷。同时，通过接入这些平台，把强大的计算资源利用起来，把原本无用的工作量变成有使用价值。IPFS 协议已经被作为分布式存储的一款国际标准智能合约引用和分发内容来使用，增加到 Vestarin data file 的支持将允许这些系统以交换 Vestarin data file token 的方式来保证存储内容。

第八章 生态计划

Vestarin data file 网络生态的建设是一项长期性的建设，需要通过长期性的努力来进行完善，这项工作将成为去中心化存储系统的重要成员。

8.1 机构成员与发行概况

Vestarin data Lab：是 Vestarin data file 的研发机构，是位于加拿大英属哥伦比亚大学;

Vestarin data foundation：是 Vestarin data file 的研发经费支持和推广机构，是加拿大温哥华Vestarin基金会的一所顶级基金机构;

总量为 1.65亿枚，90 % 由矿工发行，分 41 年发行完毕，每 26 个月发生一次区块发行量减半。

8.2 工作进度

Vestarin data file 的筹备工作从2018 年12 月3 日正式开始， 主网的研发于 2019 年 6 月 17 日开始，目前已经全部开发完毕，正进入应用验证阶段，计划于2020年4月上旬开放矿工基础模型接入，启动测试挖矿；2020 年7月中旬主网上线公测，2020 年10月中旬主网映射正式上线， 并对测试代币进行映射，2020年12月发布基于 POC+POST 的存储网络通证发布平台，提供低技术壁垒，高安全性和公平性的 POC/POST/POC+POST 存储网络发布通证发布，让更多的组织和机构加入到数据存储的市场。

8.3 生态建设

Vestarin data file 的生态系统由 Vestarin data file 主网存储网络生态和 Vestarin data file system 存储通证发布平台（基于

POC+POST 的存储网络发布平台），Vestarin data file 主网专注于图书资料、档案、文件封存等业务存储生态，有 VST 矿工提供完整的存储资源和检索计算；POST 通证发布平台发布的存储网络专注于其本身的存储领域，自建存储资源，由 VST 主网提供数据检索和服务。

第九章 声明

本白皮书允许以研究为目的使用、复制、修改和分发，无需获得研发团队的许可，但不允许任何以营利为目的使用。如果使用，以下两段文字必须出现在拷贝、修改和分发的文件中。在任何情况下，Vestarin data Lab 不接受任何一方的直接的，间接的，特殊的，偶然的， 或相应的损害赔偿，包括利润损失，从这个软件和它的文档的使用所产生的，即使该已被告知此类损害的可能性。在未经 Vestarin data Lab 同意，禁止使用此白皮书从事一切融资活动，并对私自使用此白皮书及其内容保留追究法律责任的权力。这项服务/资产/软件不应被用于非法商品、药品和活动的参与/购买，因为这是严格禁止的。