区块链项目白皮书

目　录

1. 前言

IT From Bit, 万物源自比特，一切都是信息。当今世界，信息化和数字化是不可逆转的大势。区块链作为一场对传统互联网的数据民主化革命，为数据确权，数据自由流转，价值无限制交换等提供了强大的技术保障。

数据作为未来数字经济社会的基础生产资料，如同现代社会的土地、劳动力及资本。构建民主、安全、自由交换的数据市场，是未来社会的重要基础。

去中心化存储代表了大规模存储发展的方向，因为其效率和经济上巨大优势。去中心化存储消除中心化的控制，允许用户自由存储和分享数据；去中心化存储消除了数据缺失和服务中断的风险，同时增加数据存储的安全性和数据隐私保护。

尽管目前全球有很多团队在构建这样的去中心化存储系统，但大都不尽人意。根据我们在 PB 级存储系统方面的经验，我们提出了构建去中心化的、模块化的、可扩展的去中心化存储网络——Fermat Blockchain Network。

2. 区块链

2.1 比特币及区块链

比特币——一种点对点的加密数字货币，是对人类“铸币厂”的数字化模拟，将铸币权返还于个人。实现公平、公正，实现对私有产权的保护。比特币的精神指引万千信徒组成“护币”远征队，以技术创新 + 金融创新，开启价值互联网的征程。

如果你于 2010 年在比特币的价格为 0.1 美元左右的时候，用 1 美元投资比特币，可以获得 10 枚比特币，现在的价值将超过 100,000 美元。据美国银行最新报告，这是本世纪最佳投资机会，没有之一。

虽然比特币现今仍是一种高度投机性的投资，但不阻碍其高速发展。在过去十年中，比特币已成为最受欢迎和广泛认可的加密数字货币，越来越多的零售商接受比特币作为支付方式，一些投资公司和交易所已经开始使用比特币进行期货交易。2018 年以来，美国、欧洲、俄罗斯和中国都加快在加密数字货币领域的立法，以促进加密货币行业发展，争夺行业制高点。

2018 年下半年以来，加密货币行业发展进入了新的阶段，成为大国博弈的前沿领域。美国针对加密货币领域进行了无数场的听证会，中国政治局常委集体学习区块链，将其提到国家战略高度。具体的，Facebook（FB）计划推出的 Libra 数字货币计划，中国人民银行正在准备推出的中国人民银行数字货币（DECP），欧洲正在紧锣密鼓的推出欧洲央行数字货币等，进一步在许多投资者的心中验证了比特币和其他加密货币。

区块链，作为比特币的底层技术，现在已成为最前沿的科技。

区块链的本质是去中心化的数据库账本，以技术及经济激励机制确保区块链网络的 100%安全性，以保证账本数据库可信、安全、透明、不可篡改、可溯源等。从而在时间和空间上对基于区块链网络的加密货币（token）资产价值形成广泛的共识。

以区块链技术，人类在历史上第一次真正用技术手段实现了私有财产的神圣不可侵犯；以区块链的技术及共识，人类有望打破地域与意识形态的隔离，实现价值互联互通，降低信任成本，协同共进，实现人类社会的伟大进步。

总的说，区块链是技术创新与金融创新的结合，加密货币（token）是其创新的结晶，共识是加密货币（token）存在的基础，技术及经济模型是对共识的保证。因此，所有

没有共识的区块链都是伪区块链，没有强大的共识机制保驾护航，区块链项目也不可能行为致远。

2.2 区块链与私有产权

拥有定义清晰明确的且受到严格保护的财产权是一切社会的最基础，在此之上，市场买卖双方可以自由匹配，进而实现专业化和分工，从而实现社会经济的繁荣发展，创新发展。

如果我们把区块链视为一种新兴的组织方式，它将释放哪些权力呢？我们都知道比特币的“社会契约”规则：任何人都可以无需许可的使用比特币网络（无审查），且只有拥有比特币的人才可以进行交易（无法没收），此外，没有任何政府可以随意的发行比特币从而从其他人那里窃取购买力（没有通货膨胀），最后，任何人可以在接受付款之前验证是否遵守了规则（无法造假）。而且这一切都经得起考验，可以不依赖国家，可以不依赖中央集权机构或传统法律结构而存在。

在未来，区块链网络以及它的加密数字货币（token）将使人类比历史上任何时候都拥有最高形式的财产权利。它将不仅使得人有财产权力，甚至机器都将拥有财产权力。

它使产权脱离了法律体系，摆脱了暴力的垄断。 第一次，我们可以拥有不依赖于当地政府强制执行和保护的财产。隐藏、捍卫、分割、转移和验证都很容易——全部由您自己完成，可以使您拥有最高的个人主权。

产权曾经牢固地依赖于社会制度体系的其他层面，特别是对暴力和法律制度的垄断。如果产权根基稍有不稳定，则不能拥有强大的产权，社会动荡随之而来。但是由于区块链完全独立，它可以为世界上的任何人带来最高水平的产权，无论其下层机构，政府或法律制度的质量如何。

如今，人类社会正在加快进入数字经济时代。在未来，类似于现代生产关系中的土地、劳动力和资本一样，数据将成为基本的生产资料。如何给数据确权？如何为数据建立数据交易市场，是数字经济时代最根本的问题。这不仅关系着生产关系，更关系这分配机制，关系着人类社会的长远发展，和平稳定。

区块链，将赋权数字经济时代，将数据所有权赋予其生产者（所有者）。

2.3 区块链的发展之路

到 2020 年，区块链发展了十年，中间经历了三个不同的时代。

协议时代（2008-2013 年）。协议时代达到顶峰时，比特币凭借其相对简单的经济主体成为网络空间经济的主导。在这个时代，引入新类别的经济主体（脚本）存在很大的障碍。此外，在这个时代，改变经济规则（分叉）存在重大障碍。这些弊端是新网络空间经济出现的主要动力，具体为协议的改变和新型经济主体的出现。

智能合约时代（2014 - 2019）。随着以太坊成为主导的网络空间经济，智能合约时代达到了顶峰。这个时代通过降低引入新型经济主体的壁垒，并允许在更大的网络空间经济中创造子经济，为协议时代的弊端提供了解决方案。以太坊虚拟机（EVM）及其可编程智能合约催生了新的专业经济代理人（智能合约）和子经济体（token）的爆炸式增长。更重要的是，这个时代带来了所谓的内部互操作性：即这些子经济体之间的互操作性，但仍在更大的网络空间经济范围之内。智能合约平台的容量（成本，吞吐量）的限制是替代智能合约区块链出现的主要驱动力，协议的改变和新的经济主体的出现都是如此。

如今，我们正处于第三个时代的时间口。

互操作性时代（>2020）。目前的大多数区块链处于自给自足的完整状态，每个区块链项目很少与其他区块链项目或者现实的经济活动相联系。 但是，行业出现了重大创新的明显迹象，许多项目正在朝着更开放的网络空间经济取得重大进展。一方面是日夜兼程，努力研究，开发互操作性、跨链通信及原子交换等新技术；另一方面是通过数据确权、预言机、概率性随机验证等技术及机制，与实体经济相联系，也就是日常大家所说的“实体经济上链”。

总结

基于我们对行业的理解及分布式存储领域的经验。我们提出了 Fermat 区块链协议。

Fermat 协议以 POC 共识算法为核心的，将构建去中心化的、模块化的、可扩展的去中心化存储网络，建立全球分布的数据中心，强大的分布式云存储服务能力，繁荣的数据交易市场，致力于成为来来数字经济社会的基础设施。

3. Fermat 网络框架

Fermat Blockchain Network 系统将使用 P2P 网络通信、数据加密、IPFS 网络协议、跨链通信与互操作等技术，同时开发支付系统，满足数据市场的百万级交易支付需求。

3.1 框架概览

Fermat Blockchain Network 的基础组建如下：

数据存储：将数据存储到网络中时，客户端会对数据加密后将其切割成多个数据碎片。这些碎片将被随机分配到整个网络的节点上。 同时，将生成元数据，元数据中包含有关在何处查找该数据的信息等。

数据检索：从网络中检索数据时，客户端将首先引用元数据以标识先前存储的数据片段的位置。然后碎片将被检索，原始数据将在客户端的本地计算机上重新组合。

数据维护：当冗余量降至某个阈值以下时，丢失碎片上的必要数据将被重新生成并替换。从而保证了数据的完整性和长期存储。

支付系统：发送一定量的 Fermat 代币以换取服务，包括数据存储和检索，以及数据交易市场。

进一步的分解后将包括以下部分：
1. 存储节点
2. P2P 通信
3. 冗余度
4. 元数据
5. 数据加密
6. 审核及声誉
7. 数据修复
8. 支付

3.2 存储节点

存储节点的作用是存储数据和提供数据。除了提供可靠的数据存储之外，节点还需要提供网络带宽以满足服务需求。存储节点的存储能力影响因素有：ping time、延迟、吞吐量、带宽、硬盘空间、地理位置、响应时间等。

作为提供存储服务的需求，网络为存储节点提供一定的奖励，用户为数据存储支付存储费用。

由于存储节点的选择有诸多因素，节点的选择是不确定性的。因此在每次存储完数据之后必须生产元数据以跟踪存储节点。

3.3 P2P 通信

所有网络节点通过标准协议进行通信，要求满足：
1. 即使面对网络防火墙，也可以访问。这意味着需要有对应的技术。
2. 提供与 Kademlia 类似的身份认证，让节点间互相识别。每个节点都以加密的形式提供身份认证和通信，以避免中间人攻击。
3. 绝对的隐私安全。协议应该保证客户端和节点在没有任何窃听者的情况下相互通信。

此外，协议还需要提供查阅节点身份地址的方式，以便节点间互相连接，这有点类似于 DNS 域名系统。但是没有中心化的注册。

3.4 冗余度

假设在任何时间点上，每个存储节点都有永久关闭的可能性。冗余策略必须保证：即使有一定数量的节点掉线，亦可以提供对存储数据的大量访问。如果一个节点审计失败或者不可到达，我们就发起一个网络复制过程，通过把网络上一个现有的副本转移到一个新的节点上。因此，网络就能在每次审计之后恢复正常。

为了达到特定级别的耐用性（即使面对一定量的节点故障时数据仍然可用），目前的大多数系统都是使用简单的复制备份，但这样的方案将网络的耐用性与存储成本联系在一起，大大增加了数据存储成本。

例如：假设达到某一级别的数据耐用性需要复制 8 个备份，这意味着需要 8 倍的硬盘空间和带宽，结果是 800%的成本增长.

作为对简单复制方法的替代，擦除编码提供了解决冗余问题的更好方案。擦除编码是一种编码方案，用于解决数据耐用性而不将其与带宽使用连在一起，而且相比复制方法大大提高了数据修复能力。更加重要的是，在提供耐用性时没有导致成本的增长。

擦除编码用于许多流媒体数据中，例如音频和卫星通信，因此必须指出，使用擦除编码在设计要求上没有太大难度，而且和未来技术发展趋势深度融合。

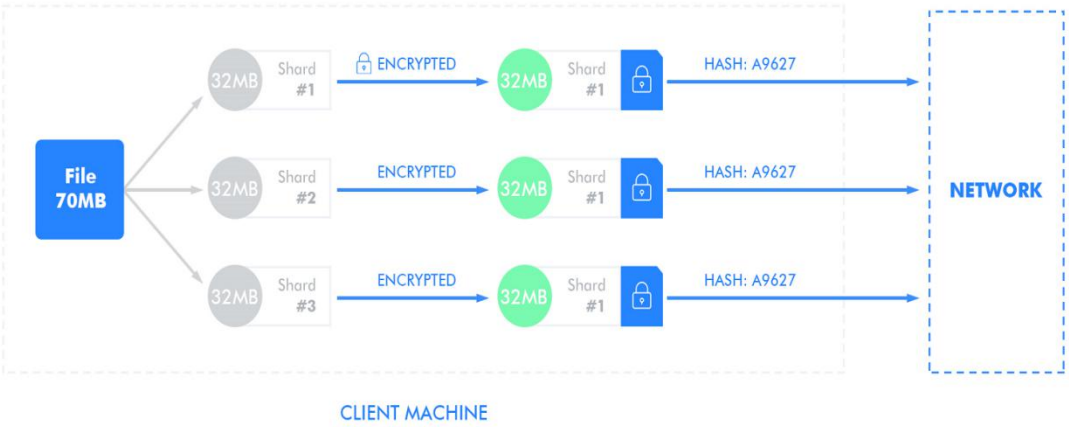
3.5 元数据

一旦我们以擦除编码方式将一定数据存储到特定的存储节点上，我们需要追踪选定的这些节点。我们允许用户根据地理位置、硬盘空间、性能等因素选择存储节点。为此，我们选择使用一个显式节点选择方案，例如基于目录的查找。

为此，我们设计了元数据存储系统，支持：分层对象（带前缀的路径），每个对象的键/值存储，任意大文件，任意数量的文件、用任意键存储和检索等等。

3.6 数据加密

为满足绝对的安全性和隐私保护，所有数据或者元数据都将被加密。因此，在数据上传到网络之前就需要对其进行加密，我们为用户提供多种加密方案。同样提供对元数据的加密，允许用户用适当的解密机制恢复数据、或者更新数据。



把文件切割成标准化的碎片，节点以碎片的形式随机存储，且没有一个节点拥有完整的碎片，这样更好的保证数据的安全性。对于同一文件，每一个碎片都用同样的方法加密，或者用户定义的方法，如外部加密密钥。
同时为了支持丰富的数据管理功能，使用多种安全密钥。还允许用户共享对某些文件的共同访问权等功能。

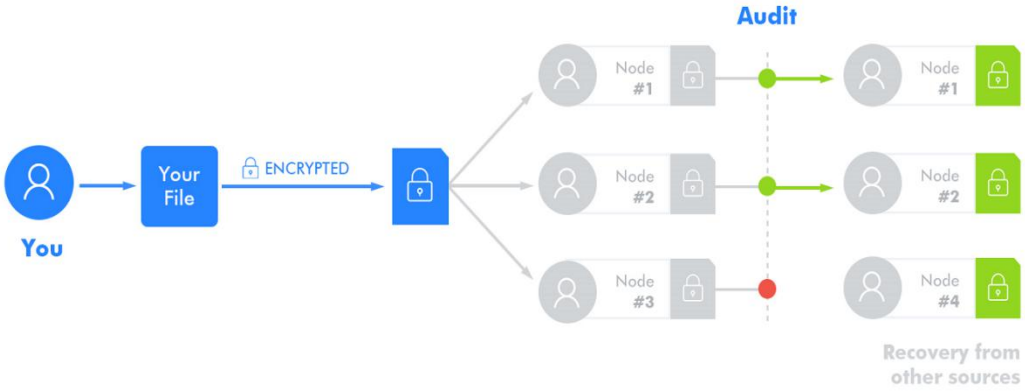
3.7 审查及声誉

激励存储节点准确存储数据对于整个系统来说意义重大。关键在于能够验证和审查节点准确存储了用户的数据，即表明存储节点行为良好，可以存储其声明的数据，并且不易受到硬件故障或其他的影响。大部分存储系统使用概率抽查方法，即可复制证明。我们采用通用的基于文件可检索性的概率证明机制，范围覆盖所有的节点和其存储的文件，其确定性更高，成本更小。

审查机制用于确定存储节点的稳定性，审查失败的结果是存储节点被标记为不良，同时用于确定哪些文件需要修复。存储节点被标记为不良，将受到一定的惩罚，并将影响到数据在节点间的分配。

3.8 数据修复

在任何去中心化存储系统中，数据丢失都是一个永远存在的风险。 虽然有很多原因可能导致文件丢失。但存储节点关停或者离开是最大的风险。因为审查机制一直在验证节点是否正确存储了数据，所以剩下工作就是检测存储节点何时停止正确存储数据或正常运行。然后通过擦除编码从其余部分重建数据，然后重新生成丢失的部分，然后将它们重新存储到网络中的新存储节点上。



3.9 支付

支付、价值衡量、竞价系统对于维护去中心化存储网络生态的健康发展非常重要。当然，去中心化的支付系统尚处于早期发展阶段，不能满足百万级支付需求。为了使得我们的支付网络满足低延迟和高吞吐量，支付系统不能依赖于区块链，即为了满足存储系统的性能要求，不可能等待区块链上的支付确认。当操作以毫秒级衡量的时候，等待节点群验证区块链账本是不可能的。

为此我们设计了支付系统，以支付渠道的方式满足支付需求（类似于 Lightning Network）。客户可以为矿工设计不同的奖励策略，例如合约可以设置为随着时间推移向矿工支付越来越高的费用，或者合约可以设置可信预言机告知的存储价格。

4. Fermat 区块链网络

4.1 Fermat 共识算法

比特币的诞生，使得分布在世界各地的上万个计算节点通过互联网共同维护一个数据库成为可行，并基于此实现了货币的去中心化发行和通货膨胀的可预测性。但在比特币的 POW 共识算法下，矿工为了争夺出块权以获得区块奖励，必须不断的开发新技术、扩大挖矿规模、寻找最便宜的电力资源。这样使得比特币的算力生态发生了重大变化：技术垄断化、能源资源化。

比特币也从原来由人人平等参与演化成由财团垄断资源和技术，最后导致局部人、少数人参与的共识。

POW 共识算法的使命已经结束。区块链未来十年的重大重新，必须探索新的共识算法。这一新的算法——要推动区块链的进一步发展、实现区块链去中心化的愿景，更应该保证安全、高性能、可扩展性、透明、公平、人人可以参与、透明、节能、方便可用。

POC 共识算法的构建基础是硬盘的数据存储与读取。数据的产生源于人类社会经济活动，因此其分布（去中心化）与人口分布大体相似，相应的提供数据存储服务的基础设备（硬盘）也是去中心化分布的。这样使得我们基于 POC 共识算法建立一个下一代的区块链成为可能。

Fermat 采用 POC 共识算法，当节点向网络提交区块时，它必须提供有效的容量证明。没有相应的数据存储，节点不可能生成有效的存储容量证明，同时，网络中的任何节点都可以轻易验证所提交的证明的有效性。如果存储的数据和提交的证明均有效，则该区块将被网络中的所有节点接受，并作为新的区块被添加到区块链网络。

提供证明的过程如下：在初始化阶段，根据协议生成一系列哈希数据，并将其保存在存储容量中。当要生成一个新块时，将根据随机数的值在容量中查找数据，该数据将被用于生成证明，并参与竞争产生下一个块。整个过程包括五个阶段：初始化，构建区块，块的接收，主链选择和惩罚机制。

- 初始化：矿工首先需要初始化硬盘并生成两个 HashMap，将它们保存到硬盘。
- 构建区块：验证最新区块时间戳后，矿工从最新区块获取挑战参数，在 HashMap 中找到满足条件的数据，生成容量证明。若容量证明的质量大于全网难度，则获得出块权。矿工对区块哈希进行签名，并将区块广播到其他节点。
- 块的接收：节点接收到最新产生的区块后，会进行一系列验证，如时间戳、公钥、签名、容量证明、证明质量、交易合法性等。
- 主链选择策略：当网络中接收到多个符合上述规则的区块后，需要按照一定的规则来选择主链区块：依次按累积难度最大、Timestamp 最小、证明质量最优来选择。
- 惩罚机制：在 Fermat 容量证明共识协议中，通过多挖惩罚的机制来抵御多挖攻

击，如果节点收到两个不同的 Header 中有相同的 proof，则证明出该块的人在双挖，该节点可以构造一个惩罚交易，使得多挖矿工的 Pk 被加进黑名单，永远无法再出块。

Fermat 的 POC 共识算法的两个特点，一是更加去中心化，硬盘分布远比芯片（ POW ）和资本（ POS ）的分布要更加普及，更加公平。二是节能，硬盘挖矿能耗低，硬盘资源可重复利用。这两个特点使得 POC 挖矿门槛低，人人都能参与。

Fermat 的 POC 共识算法为开发下一代区块链系统提供最完整的基础。在人人可以挖矿的基础之上，可以构建一个更加开放、更加去中心化的网络，同时推动物联网、人工智能、云计算、大数据等行业的发展。

4.2 Fermat 的 POC 算法技术基础

Fermat 的 POC（Proof-of-Capacity）共识算法背后的核心理念，便是在存储资源上，"证明者（Prover）低效，验证者（Verifier）高效"，以达到验证者可以花费很少的存储资源，在较少的计算时间内，验证证明者（Prover）拥有一定存储空间的目的。

我们将简单介绍基于数学模型的系统设计。

Fermat 的 POC 共识算法中最为关键的一个问题，即证明者（Bob 代指）如何向验证者（Alice 代指）证明，其拥有某个特定文件大小的文件 F 始终存在于 Bob 的磁盘之中。

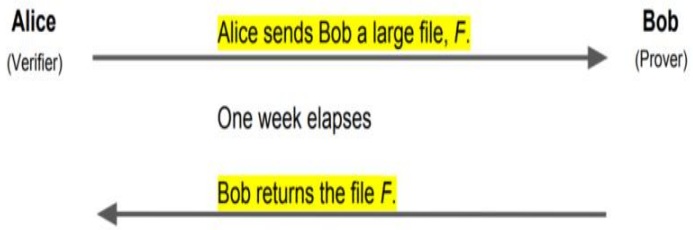
一个最简单直观的方式，我们可能会想到 Alice 在事先将 F 发送给 Bob，其后 Bob 在需要证明时返回同样的文件 F。

如下图所示，Alice 接收到文件后，校验其是否与之前发送给 Bob 的文件一致。但这样做显然违背了"对存储资源，验证高效"的特性。

同时，在 P2P 网络中，利用有限的带宽发送 POC 共识需要的大容量文件显然也是不现实的。

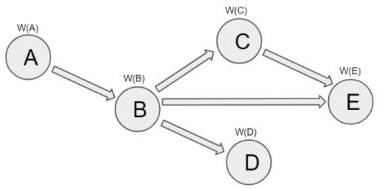
所以，我们需要设计一种对存储资源和网络资源来说都高效的算法，以达到"校验高效

"的目的。



在 Fermat 的 POC 的范畴内，文件 F 的目的只是为证明 Prover 确实使用了一定量存储空间的工具，也即我们可以对文件 F 的内容做任何形式的要求（可以联想 POW 中的 CPU 计算过程本身，并不与任何特定非区块链应用相关）。

在 Fermat 提出的 POC 算法中，文件的内容是一种有向无环图（Directed Acyclic Graph,DAG）结构，以 V 代表图中所有节点，定义 W（V），要求其满足一个特性 W（V）=Hash（V，W（V'））， 其中 V'为 V 在图中的直接前驱节点。



W(A)=Hash(A)
W(B)=Hash(B, W(A))
W(C)=Hash(C, W(B))
W(D)=Hash(D, W(B))
W(E)=Hash(E, W(B), W(C))

如上图所示，图中简单解释了有向无环图结构，其每个节点的 W 值都是经过一次 hash 计算的长二进制串。

Prover 需要将每个节点的 W 值存储，以供 Verifier 在验证阶段随机抽取检验。
Prover 与 Verifier 的交互流程如下：

初始阶段：

Verifier 与 Prover 协商复杂有向无环图 G，同时 Prover 计算所有 W（V），并存储计算结果（此步骤需要的计算时间与存储空间，和图的节点数目成正比）。

Prover 将所有 W（V）的值组成默克尔树（Merkle Tree），同时将树根节点的值Φ发送给 Verifier。

验证阶段：

Verfier 随机抽取节点 V，要求 Prover 给出其 W（V）的值，同时揭示其在 Merkle Tree 中的路径。

Prover 提取其存储中的特定 W（V），同时揭示其在 Merkle Tree 中的路径

Verfier 验证其 W（V）的合法性，同时验证其是否存在以Φ为根的 Merkle 树中。

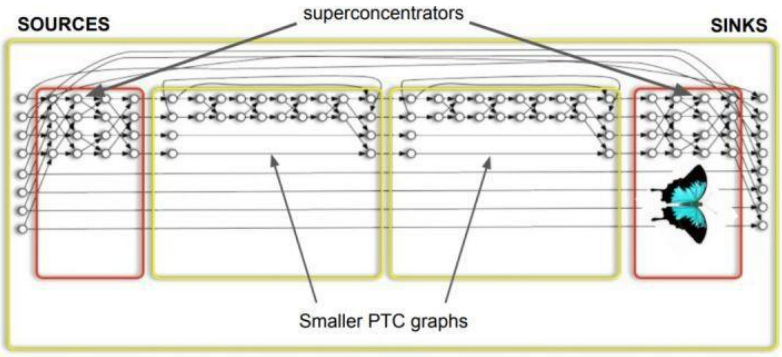
在初始阶段，类似 POW 算法中利用 hash 达到证明 CPU 的使用量，POC 在初始阶段要求诚实的 Prover 存储每个按照图结构计算出的节点 hash 值。

由于在实际应用中，图节点数远远比上图要多，同时图的连接关系也比上图更加复杂，考虑到最有可能的 Prover 作弊的情况是，Prover 在初始阶段不使用大量的存储将 Hash 运算后的结果存储在磁盘上，而是在验证阶段重新使用 CPU 资源进行 Hash 的运算。

这样的以“时间换空间”的作弊行为显然是行不通的，因为在有限的验证时间内，投入巨大的运算资源重新计算每个节点的 Hash 值，既是不经济的，更是不现实的。

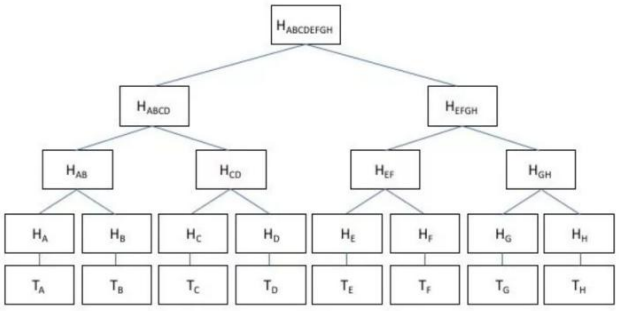
Fermat 中选取 Random Bipartite Graphs 与 Superconcentrator Graphs 两类特定类型的 DAG，两类图形的数学特性保证了节点间的连接关系的高度复杂性。

通过建立的 Pebble Game 模型，证明一个不诚实的 Prover 如果不存储与图节点相同数量的 Hash 值时，在常数有限时间内，不可能正确的通过验证者的验证。



上述两阶段交互既是 Fermat 的 PoC 算法的核心。

细心的读者可能会注意到在初始阶段的 b 与验证阶段的 b、c 两个步骤中，涉及关于 Merkle Tree 的计算和验证，此处的核心思想在于利用 Merkle Tree 的性质，简化验证者的验证复杂度，从而达到对验证者来说"验证高效"的目的。



如上图所示，Prover 将每个节点的 W 值作为 merkle 树的叶子节点，计算出 merkle 树的树根，作为参数之一，在初始节点发送给 Verifier。

在验证阶段，Verifier 只需要验证某个节点的 W 值是否存在第一步初始阶段发送的 Merkle 树中即可。

其算法流程与区块链系统中常见的轻钱包验证交易完全相同，使验证工作的复杂度大大降低。

4.3 Fermat 的 POC 算法技术细节

4.3.1 Fermat 硬盘利用与 Plot 文件

Plot 文件即每一个参与出块的节点或是矿工需要在硬盘中存储的文件，其内容由大量特定结构的 Hash 值组成。Plot 文件包含以下的几个基本概念：

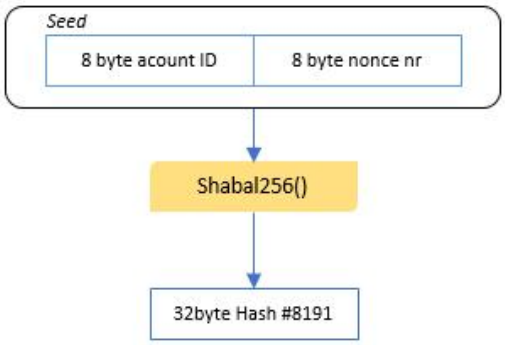
Shabal256：Shabal256 是 Fermat 所使用的 Hash 算法，相比 SHA256 等 Hash 算法，Shabal 需要更多的 CPU 计算时间和计算量。结合上一章节的内容我们可以了解，Fermat 选用 Shabal 一方面是因为在出块阶段矿工并不需要进行大量的 Hash 运算，另一方面也可以通过计算代价来防止可能的恶意矿工在每个出块阶段临时计算需要的 Hash 值而非存储中的 Hash 值。

Nonce：Nonce 是 Plot 文件中拥有固定编号的基本单元，由 256KB 的数据构成，是矿工用来参与 POC 过程的基础逻辑单元。

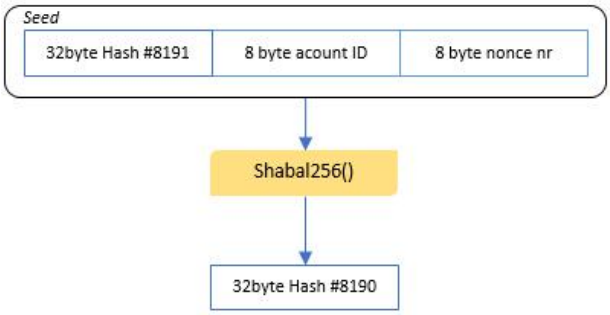
Scoop：每个 Nonce 文件由 4096 个 Scoop 文件构成，同样拥有编号，其编号范围为 0-4095。而每个 Scoop 文件包含 2 个 Hash 值，也即一个 Nonce 文件包含 8192 个 Hash 值。

Nonce 的生成流程如下：

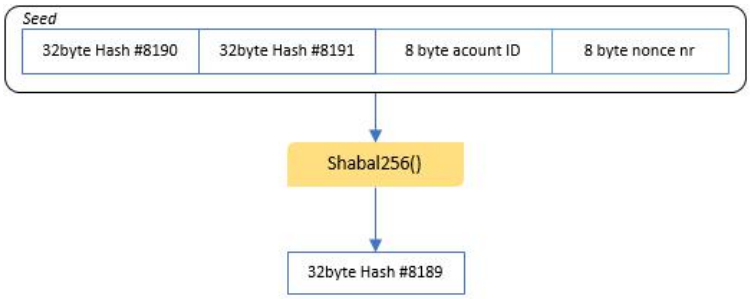
1. Nonce 文件的种子由 Account Id（即 Fermat 网络中的用户地址或者用户 Id） 与 Nonce Id（即 nonce 编号）组成，经过第一次 Hash，生成 Hash #8191，即 Non 中的编号为 8191 的 Hash 值。



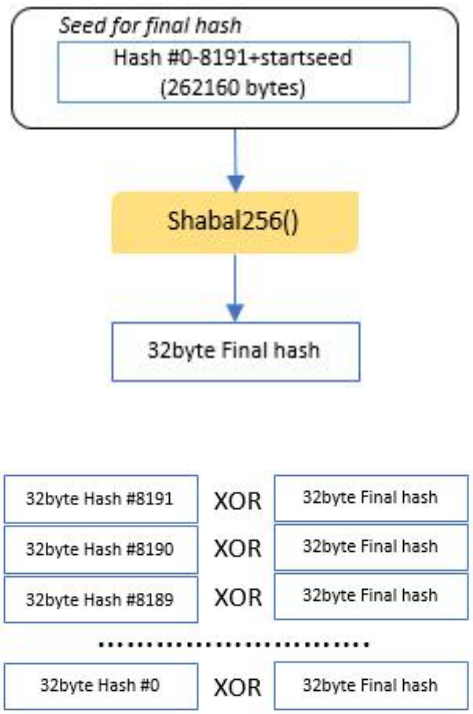
2. #8190Hash 值由之前一个#8191Hash 值与 Account Id，Nonce Id 生成。



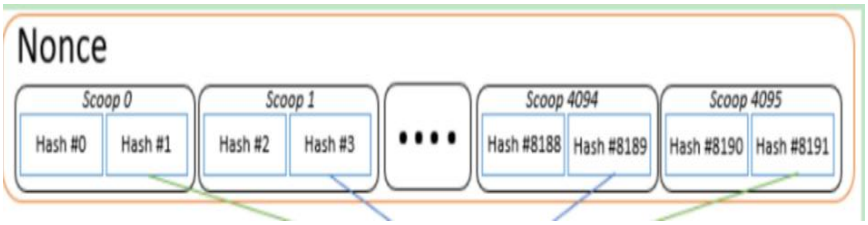
3. #8189Hash 值由之前两个#8191Hash，#8190Hash 值与 Account Id，NonceId 生成，依次类推，每下个 Hash 值，都有其之前计算的所有 Hash 值与 AccountId，Nonce Id 生成。如果过程中超过了 4096 个 bytes，则取最近生成的 4096bytes 作为下一次的 Hash 函数输入参数。



4. 最终 Hash 的生成，由 Hash#0-8191 与 Account Id，Nonce Id 共同生成，之后对 8192 个 Hash 值都分别对其进行异或操作，作为每个 Hash 最终的值。



5. 得到了 8192 个 Hash 值后，Scoop 文件的结构如下图所示：



至此，我们生成了 1 个完整的 Nonce 文件，一个 Nonce 文件包含 8192 个 Hash 值，占用空间 256KB。

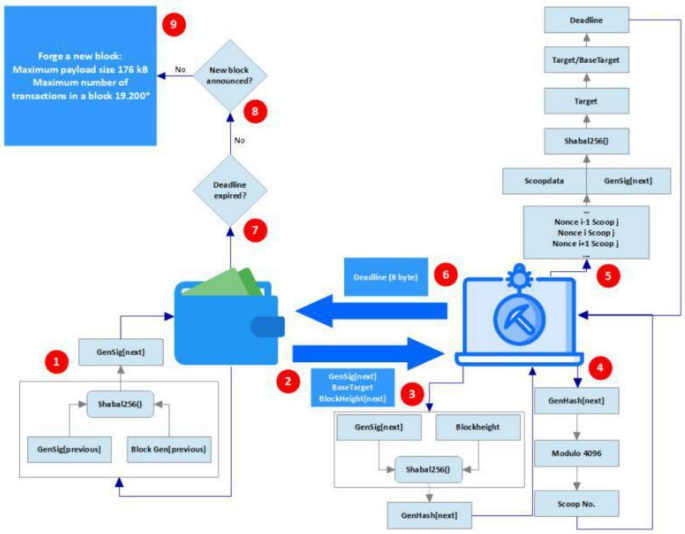
这同时也是矿工参与挖矿的最低门槛，即只要有大于等于 1 个 Nonce 文件即可参与挖矿。

而一般的家用主机以 500G 为例，可以存储 200 万个 Nonce。

故在 Fermat 的世界里，低算力基本也都是以参与矿池的形式参与挖矿的过程。

4.3.2 Fermat 共识与出块

我们将 Fermat 为区块链完整的挖矿流程是怎样的，同时探讨几个共识中的核心问题。



上图是一个完整的 Fermat 区块链的出块流程，下面我们将结合图示分别介绍其每一个

步骤。

步骤 1-2，GenHash 的生成：GenHash 类似于 BitCoin 中 BlockHash 的概念，用于形成前后相继的区块链结构。

Fermat 中，由于该 Hash 同时参与共识过程中参数的建立，其将概念拆分为两个：

GenSig 由上一个区块中的 GenSig 与上个区块的出块者做 Hash 得出，GenHash 由 GenSig 与快高信息做 Hash 得出。通过这样两次 Hash 计算，即将当前区块前的所有区块形成了不可修改历史区块的链式结构，同时也得出了 POC 共识中的重要参数 GenHash。

步骤 3-4， Scoop Number 的计算：钱包生成 GenHash 后，将此值发送给矿工，矿工由此计算本次出块需要的 Scoop Number。GenHash Modulo 4096 即 Scoop Number 的值。该 Scoop Number 用来定义本次出块中，全网的所有矿工应当查询自己拥有的所有 Nonce 中的 Scoop 的数据。结合上一章节内容我们可以得知，也即其拥有的某个 Scoop 中两个 Hash 的值。

步骤 5，计算 target，deadline：首先，矿工需要遍历磁盘，找到自己拥有的所有 nonce 中对应于上一步计算出的 Scoop Number 的两个 hash，记为 scoopdata，使表达式 target=Hash（scoopdata, GenSig）的值最小。之后利用该最小值 targer，计算 target/BaseTarget 得出 deadline。target 类似 bitcoin 中的 difficulty target 参数，控制全网挖矿难度，而 dealine 决定了了该矿工产生的区块在全网中是否成功得到该区块铸造权。

上述每个参数：

deadline：是一个整数类型数值，一个拥有特定 deadline 的区块，在全网中需要等待对应于该 deadline 所指定的时间之后，才可以被作为一个合法的区块。举例来说，如果 deadline 为 60，则代表在上一个块出块时间一分钟后，这个块可以被允许添加到主网作为合法区块。由此我们可以得知，计算得出 deadline 越小的矿工，越有胜算得

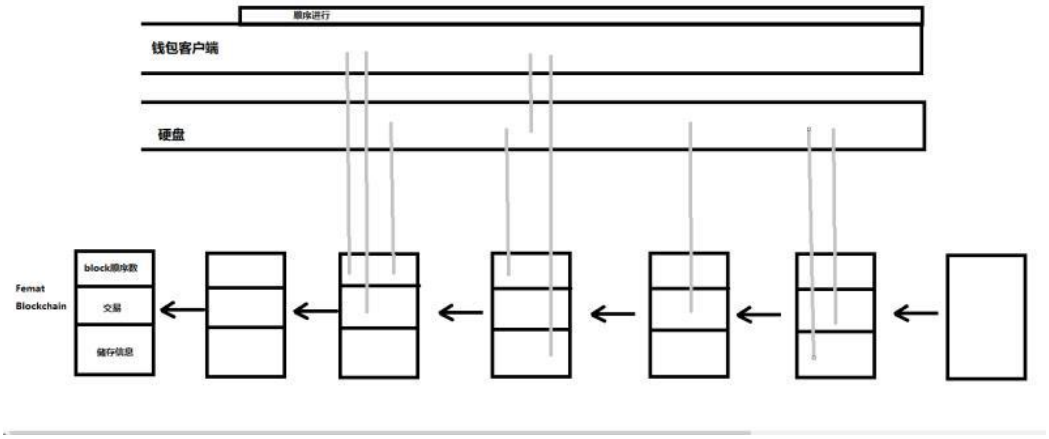
到当前块的铸造权。而 deadline 的计算过程是矿工通过遍历自己所有随机生成的 Nonce 中的值计算得出，也即代表所拥有 Nonce 个数越多，磁盘占用空间越大，获取数值更低的 deadline 的概率更大，从而得到铸块权的概率也更大。

BaseTarget：Fermat 设定的全网平均出块时间为 4 分钟，全网的存储算力是波动，如何在波动的算力下控制全网平均出块时间？类似与 BitCoin，BaseTarget 代表挖矿难度，其值越小，说明全网挖矿难度越高。在 Fermat 中，最小的 target 需要除 BaseTarget 得到最后 deadline。所以对 BaseTarget 的动态调整，可以直接控制全网的区块间的间隔，也即区块时间。

步骤 6-9，打包交易，铸造区块，广播区块。此过程与所有区块链系统类似。值得一提的是，Fermat 的区块负载大小限制为 176KB，平均可以承载 19k 个左右的交易，不难得出其理论 tps 上限控制在 80 左右，与 Bitcoin 和 Eth 等 POW 类型的区块链系统相比，其性能量级也是相类似的。

4.4 Fermat 分布式存储协议

Fermat 分布式存储协议底层存储由 ipfs 实现，上层网络由 Fermat 的 POC 共识协议搭建。用户通过 Fermat 钱包把文件传输到 ipfs 网络，上层 Fermat 区块链网络永久保存用户传输的文件信息。Fermat 分布式存储协议定义了一套文件标准，可以安全保护用户文件的安全性与隐私性。在存储文件时，用户根据 Fermat 支付系统支付相应的费用，节点会获得挖矿以外相应的存储费用。



储存的文件会加密切割成多个数据碎片，然后通过特定的网络传输通道，传输给其他节点以做备份，生产相应的元数据。即使储存数据的节点出现意外，文件也会被网络中的其他节点储存（Fermat 冗余策略及数据修复机制保证数据安全及访问性能）。

Fermat 分布式储存协议可以和与物联网相结合，帮助完成信息上链、信息备份、信息存储及实现远程信息共享。

5 Fermat 激励机制

Fermat 提出了创新性的激励机制，以实现网络与生态的可持续高速发展。这种激励机制使每个参与者所追求的理性利益与整个生态系统的利益一致，最后实现高度去中心化的、稳定的网络系统。

Fermat 作为对生态参与者的经济奖励和惩罚的手段，防止恶意节点作恶和智能合约中可能出现的无限循环的逻辑炸弹，Fermat 生态内的支付结算货币，以及 Fermat 生态与其他大型公链生态发生链上经济活动的锁定和支付结算方式。

Fermat 经济模型	
代币总数	1,002,144,000
减产周期	半年
减产比例	25%
抵押票	根据快高分为若干个抵押周期，在一个周期内锁定一定量 Fermat 代币可以生成一张票。如果持票挖矿，获取全额奖励，不持票挖矿产出比例根据社区反馈自我调节。
Staking	项目运行一定周期后，由社区启动 Staking 池，以加强整个网络的稳定性。

6 Fermat 应用生态

6.1 Fermat 与 ipfs 生态数据存储

6.1.1 IPFS 生态概况

IPFS 全称为「Inter Planetary File System」，中文名为「星级文件系统」。IPFS 是一个底层的网络传输协议相当于目前互联网世界中的 HTTP（超文本）协议。HTTP 是一个较为简单请求-响应协议，用于用户与服务器间的交互。

IPFS 的功能与 HTTP 类似，但将 p2p 网络的架构特点加入了其中。与 HTTP 协议相比，IPFS 协议更为高效。HTTP 为单线程通讯，每次在一个服务器上只能进行一个任务，而 IPFS 使用 p2p 的方式进行多线程下载，可以节省超过 50%的带宽成本。同时，因为现在的互联网服务器的中心化属性，网络中的信息可以被完全控制并难以保存，但是如果使用 IPFS 等去中心化协议，只要信息被网络中的任何一个用户所拥有的，那么整个网络都可以获取到此信息。

近几年，随着 IPFS 技术的发展，吸引了全世界各地的优秀人才不断涌入这个神奇的开源世界。结合 IPFS 的优点在各个领域不断创新应用，为互联网的新时代开创了无限想象。以下是在 IPFS 生态的应用实例

DAPP 示例

（1）IPFS 电商：OpenBazaar，对标淘宝和亚马逊，去中心化的全球自由买卖市场。Open Bazaar 是一个结合了 eBay 和 BittTorrent 特点的去中心化商品交易市场。这个平台没有一个中心服务器，每个用户要使用 Open Bazaar 平台购物时，都需要下载一个软件，自身也作为一个服务器节点，为整个网络服务。

它形成了一个去中心化的全球自由买卖市场。相信很多用过淘宝、天猫的人都绝对相信阿里集团的第三方仲裁担保，但不同的是，OpenBazaar 运用加密学做担保，信任来自于代码和数学，而不是人，这意味着不需要支付费用，也没有你的档案，你的交易不会被审查。

目前这款软件已经有 30 多个国家在使用，能在上面购买到各个国家的音乐、游戏、食品、饮料、衣服、艺术、珠宝等等。OpenBazaar 利用 IPFS 的强大功能创造了一个完全免费的电子商务！在这里，BTC，ETC，LTC，ZEC，Dash 均可以作为支付货币。OB 有点像小商店的，下线后商铺就成了灰色，很可爱。目前只有桌面版，下载的话，需要适配环境。

（2）PeerPad 是协作的实时编辑器，它不使用第三方，所有参与节点直接对话，不需要中央服务器。同时 Peerpad 开源，展示了开发者如何使用 IPFS 建立自己的无服务器的、实时的、离线优先的多人协作的分布式应用程序，由协议实验室和 IPFS 社区建立。可实现四种功能：1、会议笔记，2、协作或共享代码片段，3、写文章并分享，4、与多个用户同时协作。

（3）IPFS 音乐播放器：比如 Spotify，口号是：Music for everyone，致力于分享数百万首歌曲。使用 Spotify，我们可以轻松地在手机，计算机，平板电脑等设备上随时找到合适的音乐，而且还可以浏览朋友，艺术家和名人的音乐收藏，或者创建一个广播电台，Spotify 将存储放在 IPFS 网络上，极大地降低了音频数据的存储成本。其他的：1）Ujomusic：对标虾米和咪咕音乐的一个 IPFS 上的音乐家的区块链市场；2）DIFFUSE，在线音乐播放器。

（4）IPFS 视频播放器：D.Tube 是第一个加密分布式视频平台，建立在 STEEM 区块链和 IPFS 点对点网络之上，未来会支持 FIlecoin 网络，它旨在成为 YouTube 的替代品，允许用户在 IPFS/FIlecoin 基础上观看或上传视频，并在不可变的 STEEM 区块链上进行分享或评论。

（5）IPFS 社交网络：Orbit，QQ 在 IPFS 上的替代者。Orbit 是在 IPFS 基础上的一个完全分布式、点对点、实时的聊天应用，可以把它当做去中心化的 Slack or IRC。Orbit 通过 IPFS 和 CRDTs 来存储和处理实时通讯：它可以在没有任何中心点的情况下工作，完全点对点。Orbit 通过以太坊和 uport 来注册身份，跟踪用户以及身份信息。这是一个 IPFS 分布式应用与以太坊处理系统强有力结合的展示。

其他 IPFS 社交比如：Akasha，对标 facebook，微信等社交工具；textile，致力于取代 Instagram；magicleap，VR 和 AR 在 IPFS 上的实现；Neocities，开源免费创建个人网页的社交网络。

6.1.2 Fermat：IPFS 生态的激励层网络

目前 IPFS 激励层的应用在全球有多个项目在积极探索，Fermat 是最受关注的项目之一，Fermat 的出现旨在提升 IPFS 协议在一些特定领域内的快速应用和发展。这些领域的普及和推广速度会走在行业的最前沿。Fermat 致力于发展的这些领域包括：医疗健康、身份认证数据存储、高清视频、VR/AR、云游戏、工业互联网、无人驾驶等。

Fermat 自身也形成了一个应用生态，包含存储网络、经济体系、技术构架等。

6.2 Fermat 服务于高清视频数据存储

“信息视频化、视频超高清化”已成为全球信息产业发展的大趋势。高清视频服务的本质就是高质量内容与高速渠道的结合，为广大消费者市场和行业应用市场服务。超高清视频对传输网络大流量、高速率、低时延的需求与 5G 网络特性高度吻合，有望成为未来新媒体行业的基础业务，成为 5G 主要的相关行业。

5G 赋能移动终端实时连接云端获得强大性能后，使用体验大幅提升，应用场景对于移动终端的硬件配置要求不再苛刻，移动终端将深度渗透各行各业。例如，5G 带宽高达 1Gbps，可以支持一个时长 8 分钟、大小 1.3GB、码率约 20.8Mbps 的 5K 全景视频流畅播放。5G 可改善 VR 云游戏的画质，并降低云游戏技术中的网络时延。

运用云端强大的 CPU 和 GPU 来进行 3D 图形运算，以视频流的形式传回本地的 VR/AR 设备，让内置了移动芯片的 VR/AR 设备也能显示出顶级的画质。5G 强大的通信能力可以支持无人机实现云端 AI 计算，处理无人机实时产生的传感器数据和视频数据。5G 网联无人机的应用可以充分扩展到需要实时大数据传输的物流运送、娱乐直播、基础设施巡检、农林植 保、地理测绘、城市规划、应急抢险等场景中。

5G 之下的高清视频将需要超强的数据存储服务能力。Fermat 的分布式云存储生态既能保证超强的、高体验的数据存储需求，又能保证数据安全、隐私保护、数据确权等。

Fermat 基于算力（挖矿）生态，可以在全球范围内快速建立大量的云存储中心及数据中心，Fermat 可以基于超清视频的观看需求分布，就近存储和分享数据，即保证体验及性能，又能降低成本。

6.3 Fermat 服务于云游戏数据存储

基于 5G 云端处理技术，所有手机均可操作云游戏，使游戏终端设备的价格大幅下降。5G 与 4G 的本质区别在于其速度比后者快 10 倍。对普通用户与普通的游戏应用场景而言，画质低于 4K 的视频在 4G 与 5G 条件下没有区别；但对应用场景复杂、游戏元素多元、要求更快速度、更大带宽和超低延迟且支持实时、多人和沉浸式游戏体验的大制作云游，5G 提供了普及的可能。

在 5G 云游戏时代，所有画面渲染带来的资源消耗都在云端完成，通过 5G 大带宽、毫秒级别的低时延优势，手机端更多只要求视频显示功能。

游戏是人的天性，随着社会生产力的发展，在未来人类闲暇的时间只会越来越多，游戏的需求只会越来越大。Fermat 解决了云游戏的数据存储需求，Fermat 的 POC 共识算法下，人人可以参与挖矿的特性使得任何人都可以建立小型的云存储服务中心，在分布式存储技术、IPFS 及 5G 技术共同的作用下，数据检索及传输的速度将会大大提高，延迟可以降低的 10ms 级别，这样为 Fermat 服务于云游戏实现提供了可能。

6.4 Fermat 服务于医疗健康数据存储

中国作为有着 14 亿人口的大国，一直存在医疗资源供给不足、分布不均的问题。5G 发展为远程医疗提供了技术上的支持，可促进医疗资源的线上流动，不同地区不同级别的医院之间实现互联互通，打破医患的空间限制，大幅提升医疗效率，有助于偏远地区获取优质医疗资源，从而改善医疗资源供给不足、分布不均的现状。

大规模物联网涉及医疗物联网（IOMT）生态系统，将包含数以百万计甚至数十亿的低能耗、低比特率的医疗健康监测设备、临床可穿戴设备和远程传感器。医生将依靠这些仪器实施远程监控，全天候采集病人的医疗数据，如生命体征、身体活动等，实现多方交互共享，有助于医生有效地管理或调整治疗方案。

大数据与医疗服务结合的模式在近年来成为关注的热点。优质的数据能有效提高新药研发效率，改善临床治疗手段等。远程医疗在经过一 段时间的运营后，积累和沉淀的数据逐渐形成经济价值。

Fermat 服务于医疗健康数据存储，比如快速存储和共享体细胞癌症数据和相关的临床信息，从全球范围内的医疗数据中提取关键数据，并使研究人员，临床医生和科学家能够在实时，公开和可信的环境中访问数据。进而提高医疗数据流通，有利于医学研究。同时为医疗数据确权，使得数据所有者也得到相应的利益，比如数据买卖的收益，更合理的保险价格等。

6.5 Fermat 服务于工业互联网数据存储

工业互联网是应用于数字时代的先进生产模式，依托 5G 网络、云服务平台，面向工业客户，融合云计算、大数据、人工智能，通过对工业数据深度感知、实时传输、快速计算及高级建模分析，实现生产及运营组织方式 的变革，助力传统工业企业转型。5G 具有增强移动宽带、超可靠低延时、广覆盖大连接的特性，解决工业互联网海量大

数据通信传输的难题，成为工业企业降低成本和提高效益的重要技术支撑。依据 5G 先锋行业识别器，可以判断出 5G 可在电力生产和智能制造业率先应用。

工业互联网的快速发展离不开供应链的不断发展。

Fermat 可以基于每个行业的中心环节实现供应链管理创新。Fermat 数据确权，隐私保护、数据市场等技术实现，可以让每个供应链环节乐于分享数据，保护数据隐私，获得数据的利益，从而促进整个供应链的不断优化。进而促进工业生产模式创新，实现在数据深度感知、实时传输、快速计算及高级建模分析，实现生产及运营组织的变革，助力传统工业企业转型升级。

6.6 Fermat 服务于区块链行业的数据存储

未来区块链发展的主流是多链生态，万链互联互通则是必然。因此，跨链通信、互操作、原子交易等是区块链技术未来十年发展的大势。如同现在的互联网行业生态结构一样，未来的区块链生态将是生态结构化，不同的公链生态在整个行业内提供不同的基础服务。

数据确权、数据交易、数据存储是区块链行业的基础性设施。

Fermat 作为基于 IPFS 的去中心化存储系统，可以为所有的公链系统、基于公链的 DAPP 等提供基础的数据存层服务。

7. Fermat 发展规划

1.项目启动	**2019.Q3**
2.Fermat 测试网发布	**2020.Q3**
3.矿工生态搭建	**2020.Q3**
4.Fermat 主网发布	**2020.Q4**
5.Fermat 全球节点建立	**2020.Q4**
6.Fermat 生态基金一期成立，支持基于 **IPFS** 和 **Fermat** 的生态发展	**2021.Q1**
7.Fermat 二层网络开发，提升网络性能，支持应用搭建	**2021.Q2**
8.Fermat 生态基金二期成立，推动 **Fermat** 在商业领域生态推广	**2021.Q3**

8. Fermat 生态治理

企业治理结构源自于公司制度，是用以约束企业战略、风险管理、运营原则、人力资源以及法律合规的总纲。

区块链技术虽然是以去中心化为出发点，建立高效协同的社区平台，但是企业治理架构的经验必然可以借鉴，以提高区块链社区的协同效率，规范社区的运营活动；我们想要构架的是一个“非传统”社区，除了个人参与者，更有大大小小的商业用户、企业用户，合理的企业治理架构更加能在企业参与者中形成共鸣。

当然也不能完全生搬硬套，需要在社区文化和传统企业管理文化之间寻求一个动态平衡。我们在这里所倡议的这份治理方法，只是根据我们在传统企业的经验结合过去几年里在区块链行业的积累的一个组合，并不代表完美，也需要在后面的发展中，进行不断的优化调整。

8.1 Fermat 基金会

Fermat 基金会为的非营利性实体, 由 Fermat 创始团队发起，技术极客和广大社区爱好者共同支持成立。 基金会将作为 Fermat 区块链的倡导实体，致力于 Fermat 的开发建设和治理透明度倡导及推进工作，促进开源生态社区的安全、和谐发展。

一般的区块链社区以高度自治或去中心化为目标，放任社区参与者进行多样化的议事建议，并通常采用“投票”的方式进行重要事项的决策。然而这样的议事行为，由于参与者意见的 多样化而变得低效或悬而未决，不利于区块链技术的不断迭代和演进。更有甚者，由于意见 的严重分歧，导致区块链的分叉行为。多次采取硬分叉的解决方式更是使得人们对以太坊、乃至区块链的去中心化理念产生质疑。这样的治理方式，与其说是“民主”，倒不如说是“无政府”。

Fermat 团队高度认同区块链“去中心化”建设的实质，同时也吸纳传统公司制治理结构的精华所在，提高 Fermat 开发与推广战略的高效制定与实施，同时也避免可能产生的严重的区块链设计理念的分歧及不可调和情况再次出现。

Fermat 团队将委托具有公信力的第三方机构，协助团队推动基金会实体，并代为维护实体架构的日常运营与报告事务。而基金会设立后，即遴选适当的社区参与成员，加入基金会 职能委员会，共同参与实际的管理与决策。

8.2 Fermat 基金会治理原则

Fermat 基金会治理结构的设计目标主要考虑 Fermat 区块链开放平台的可持续性、战略制定的有效性、管理有效性、风险管控及平台经济的高效运营。

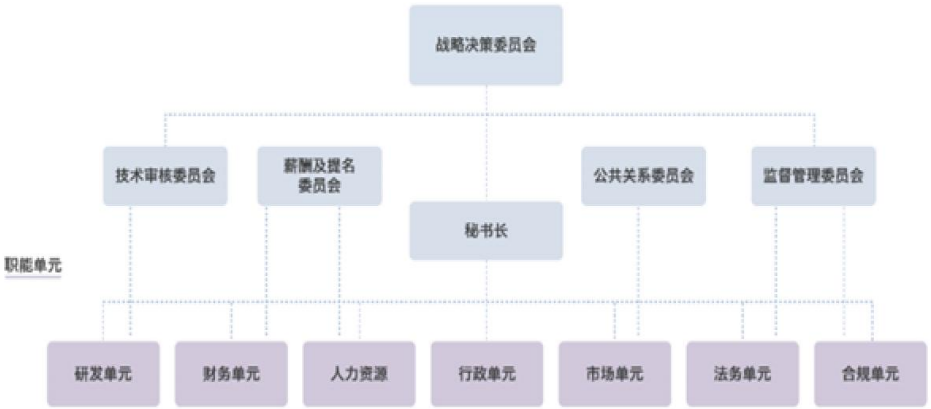
虽然一直有论点提倡区块链就是以“去中心化”或“分布式”为核心的自治社区体系，我们认为完全的去中心化带来的可能是绝对的“公平”也可能是更多的“低效”。因此基金会仍会在管理架构上吸纳一定的中心化治理的核心思想，包括战略决策委员会的最高决策权限以及重大事项的集中议事权力等，以提高整个社区运营的效率。

任何一个技术脱离了商业应用，则其发展往往举步维艰。如果无法证明该技术缺乏实际应用性和意义，甚至会停滞不前乃至胎死腹中。Fermat 团队从创建构想开始，就一贯秉持与商业的紧密结合为宗旨。因此也有了最早的商业 应用落地的案例。Fermat 基金会的设置，同样也遵循这一宗旨。即便基金会以非盈利机构的形式存在，但基金会希望尽最大程度获得商业世界的认可，赢取商业应用的收益， 同时反馈到基金会以及社区，用以进一步推进基金会以及 Fermat 的开发与升级。

于此同时，基金会也通过定期报告以及不定期新闻发布的形式，向社区参与各方披露与报告基金会运行情况和 Fermat 发展进度。同时，基金会主要管理人员的联系方式也将 完全公开，接受各参与方的监督和联络。

8.3 Fermat 基金会组织构架

Fermat 基金会组织结构提出专业委员会与职能部门相结合的方式，对日常工作和特殊事项予以应对。 基金会的设立参考传统实体的运营，将设立各项职能委员会，包括战略决策委员会、技术审 核委员会、薪酬及提名委员会及公共关系委员会等组成。



9. 免责声明

本文件是 Fermat 区块链项目阐述的概念性文件【白皮书】，并非出售或者征集招标相关公司的股份、证券或其他受管制产品。

根据本文件不能作为招股说明书或其他任何形式的标准化合约文件，也并不是构 成任何司法管辖区内的证券或其他任何受管制产品的劝告或征集的投资建议。

本文件不能成为任何销售、订阅或邀请其他人去购买和订阅任何证券，以及基于此基础上形式的联系、合约或承诺。

在本文件中所呈现的任何信息或者分析，都不构成任何参与代币投资决定的建议，并且不会做出任何具有倾向性的具体推荐。

Fermat 基金会不承担任何参与本项目造成的直接或间接的资产损失。

这份文件可能随时会被修改或者置换，然而我们没有任何义务更新此版本白皮书，或者提供读者额外资讯的渠道。