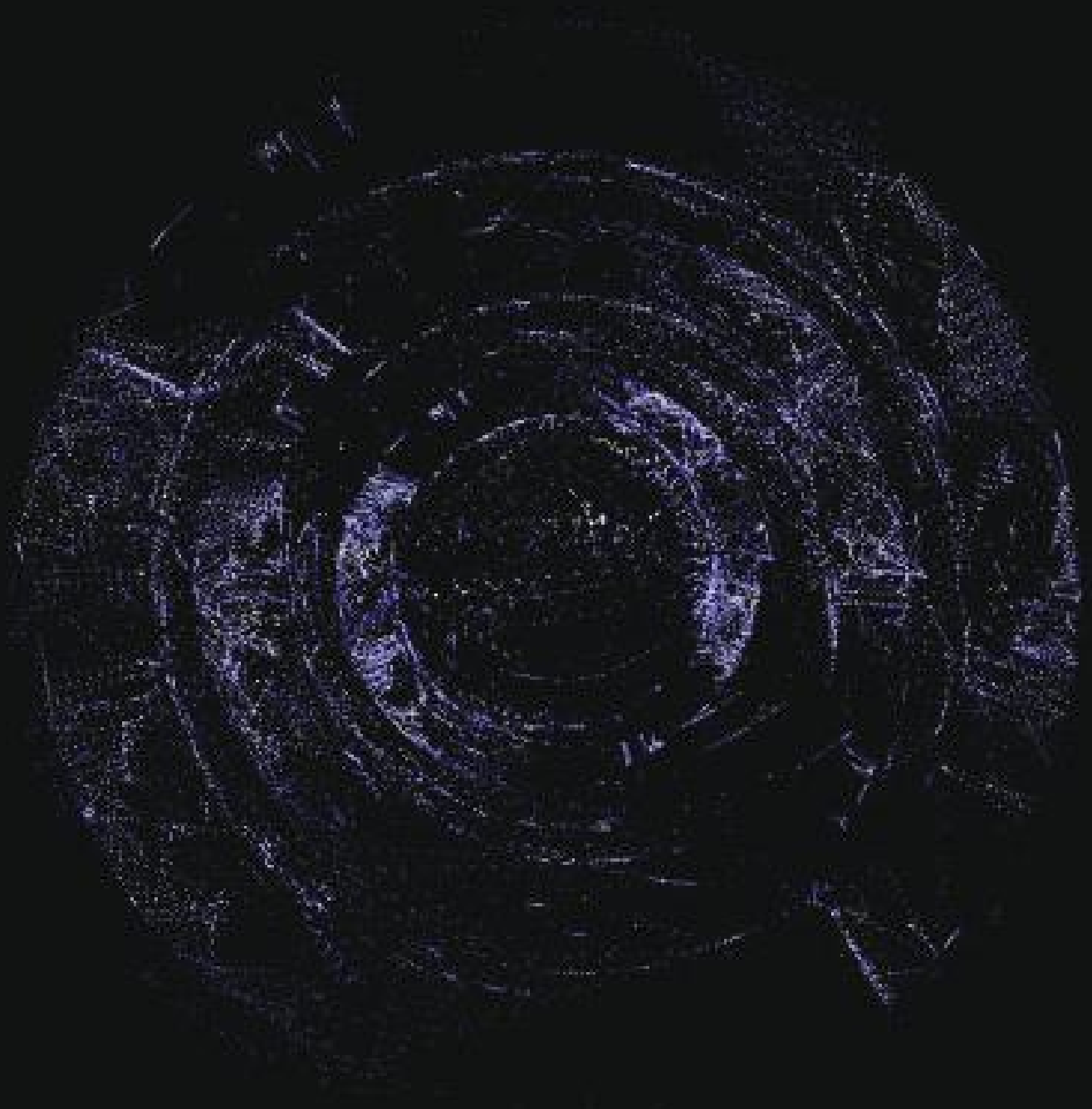
FANTOM

I BEYOND BLOCKCHAIN

白皮书

v1.6 | 2018年8月28日



https://Fantom.foundation

目 录

免责申明

本文件作为一份技术类白皮书，介绍了Fantom平台和Fantom基金有限公司（Fantom）生态系统的发展现状和未来规划。本文件旨在提供信息而非对未来规划进行精准描述。除非明确说明，本文件中所提到的产品和创新技术仍处于开发状态，有待合并。针对此文件中提到的此类技术，创新成果以及相关活动，Fantom并未为其成功开发和试验提供质量保证以及书面承诺。此外，在法律允许的范围内，Fantom拒绝承担任何技术运用和其他方法使用过程中所带来的质量责任。任何人都无权信任本文件中的任何内容及其相关推论，此理同样适用于本文件所概述的Fantom技术交互之间的相互交流。本文件存在一定的纰漏和疏忽之处，但是Fantom对与本文相关的任何个人与团体因错误，疏忽以及其他行为带来的损失概不承担法律责任。

本刊物所涉及到的信息的数据来源于Fantom认为是值得信任的数据，但Fantom并未对此类信息的准确性，完整性以及合适性撰写过任何质量保证，质量确认以及承诺声明。您不得随意授权本文信息，为自己，员工，债权人，抵押权人，其他股东或是其他人提供解决方案。本文所涉及的观点仅能反映本文作者的现行评估，并不一定代表Fantom的观点。本文所涉及的观点可能会更改，恕不另行通知。而且这些观点并不一定和Fantom的观点相保持一致。Fantom没有修订，完善以及更新本文件的义务。而且，倘若未来本文件中的一些观点，预测和假设出现改变或是产生错误，Fantom没有通知订阅者和接收者的义务。

针对任何人（包括该刊接收者在内）因为本刊直接或是间接表达出来的相关陈述，观点或是信息的不实描述而造成的损失，Fantom及其职员，承包商和代理商等对此概不负责。上述陈述，观点或是信息无论是本文直接包含，间接衍生还是无意忽略的，均适用上一条规定。Fantom及其顾问均未对该文件所囊括的如预测，展望以及计划等信息进行独立验证。

针对本报告的重点问题以及与进一步调查相关的任何信息，所有的收件人只能依靠自己的知识和调查对其作出判断和评估，来保证此类事项的精确性和完整性，从而让自己满意。

尽管已尽一切努力确保本文中所做的事实陈述都是准确的，确保所有的估计预测，前景展望，观点表达以及主观判断都是基于一项预测--在撰写本文件时，上述信息均是合理的，然而，不得将本文件理解为：里面所涉及的一切内容都将发生。鉴于现实中存在多重风险因素，诸如技术发展中的局限与不足，法律法规的制定与执行，市场及行业波动，公司行为以及无法获得完整准确的信息等，本文件中所涉及到的所有计划和预测可能无法实现。

Fantom可能会提供本文中提到的实体网站的超链接，但这并不代表Fantom认可，推荐或是支持链接页面上的任何内容或通过页面链接进一步获取的信息，访问此类链接网站的风险完全由您自己承担。对于此类材料及其后续使用所造成的一切后果，Fantom概不承担任何责任。

本文件的受众定位不包括以下个人或是实体，即其所在的州，国家或是其他司法管辖区内有相关的法律法规禁止分发，出版或是使用此类文件。

本文件仅可在网站www.Fantom.foundation上获取，且事先未经Fantom书面同意，不得处于任何目的将该文件部分或全部进行重新分发，复制或是传送给其他人。一些国家或地区的法律法规可能还会限制分发该文件的方式。持有本文件的相关人员必须了解和遵守此类限制。访问该文档即默认该收件人同意上述限制的约束。

本白皮书作为一份信息文件，在接受最终审查之前还有待更新。本文件并不构成合约。任何此类合约必须接受最终监管审查，并受修订文件和销售条件文件的约束。倘若本文件与下述即将提到的文件不一致，前述修订文件和销售条件文件会发挥效力。因此，只能在收到了最终文件之后才能做出购买Fantom代币的决定，并且只有在所有最终监管条件都得到满足之后，最终文件才会发行，代币才能顺利买到。

该文件并不是企业招股书，产品发布声明或任何其他规定的报价文件。它尚未得到任何政府机构或是监管部门的认可和登记注册。在某些司法管辖区，本文件的分发和使用，诸如相关广告营销材料以及代币的最终销售等，会受到法律的制约。因此，代币购买者必须充分了解这些法律并遵守相关约束条件。倘若您持有该份文件，请务必寻求当地司法部分的建议以及遵守相关约束条件，这些约束条件包括但不局限于国际证券委员会组织（IOSCO）网站上“关于初始货币的监管申明”中所罗列的适用限制。IOSCO的网址为：https：//www.iosco.org / publications /？subsection = ico-statements。上述约束条件随时可能发生变化。若您未能遵守此类约束条件，其结果是违反相关适用法律。访问本文件即表示您同意遵守此要求。

1.0 Fantom

区块链技术提供了一种在没有中央权限的情况下仍能保持所有节点共识的方法。然而，这一技术面临着一些基本问题，例如缺乏实时交易结算和扩展性。尽管区块链的共识算法得到了改进，但一些区块链（如比特币和以太坊）目前还处于一次同步一个块的阶段。由此造成的确认时间缓慢,这一问题也是阻碍区块链技术应用于更多产业的最大因素之一。尽管Cardano和EOS这样的智能合约平台开始出现，公共分布式账本仍未得到广泛应用。

为了解决这些存在已久的问题，开发了一种基于有向无环图（DAG）的新模型。Fantom就是在DAG基础上发展起来的一种新型智能合约平台，旨在解决现存的公共分布式账本技术中的可扩展性问题。该平台计划通过使用现有的基于DAG协议改进版本将自己与传统的基于块的分布式账本存储基础架构区分开来。Fantom平台采用一种名为“lachesis协议”的新协议来维持共识。该协议将被整合到Fantom OPERA链中。其目的是允许在Fantom OPERA链之上建立一批程序，让所有的用户能够享受成本几乎为零的即时交易。

Fantom的目标是让世界上所有的交易机构能够相互兼容，并且创建一个能够以低成本实现实时交易和数据共享的生态系统。

2.0 我们为什么要创建Fantom?

Fantom的愿景是确保全球所有交易机构之间的兼容性，这些机构使用的是可在现实世界中进行大规模部署的快速DAG技术。与此同时，Fantom还想要创建具有高可靠性的新基础架构，从而实现实时交易和数据共享。

FANTOM的愿景是使用可在现实世界中大规模部署的快速DAG技术来授予全球所有交易机构之间的兼容性，并创建具有高可靠性的新基础架构，以实现实时交易和数据共享。

FANTOM希望能够在各种垂直行业中得到大规模应用，例如电信，金融，物流，电动汽车供应等等。FANTOM基金会计划创建FANTOM平台以及基于智能合约的新生态系统，供全球所有当前与未来的合作伙伴公司使用。

Fantom基金会还将引领下一代分布式账本技术的发展，从而促进精确性，可靠性以及连续性更高的全球交易。

该平台将开放其源代码供社区使用和更改，而且提供可用于创建分散应用程序（DApps）的各种应用程序支持工具。

2.1 区块链存在的一些问题?

区块链作为一种软件创新形式，在用户之间建立数字信任，从而促进价值通过网络从一个实体转移至另一个实体。其目的是在不需要传统公共机构或中间人的情况下实现资本的安全保存和汇款结算。Fantom认为，区块链技术要实现在现实生活中的广泛应用，必须做到易于转让，不可撤销以及交易费用极低甚至为零。然而，现有的区块链技术由于确认时间较慢以及交易费用偏高仍存在很多局限性。

可扩展性问题

在现有的区块链中，所有的节点一次验证并存储单个块，导致创建块的时间更长，块的大小也受到限制。因此，无论连接了多少个节点，区块链的运行会受到每个节点速度的限制。需要处理的事务越多，网络本身存在的瓶颈问题会让区块链的性能更差。因此，Fantom认为需要使用并行方法。

费用

使用区块链进行价值交换的时候会产生各种费用。主要费用包括支付给矿工的交易确认成本，以及支付给块本身的奖励

[1] www.mdpi.com/2071-1050/9/12/2214/pdf

这些费用能够激励区块链的共识参与者，确保网络免受DDOS及其他风险系统的攻击。但是，Fantom认为，对于具有众多用户以及应用，且还处于扩展和蓬勃发展状态的区块链而言，这些费用确实相当高。

历史数据

区块链无法从外部获取信息来验证优先交易，只能使用存储于块中的信息。而现有区块链中存储的信息作用有限。

Fantom认为，要想区块链技术在现实世界中得到充分运用，管理区块内交易的历史信息这一功能至关重要。

2.2 FANTOM提供的解决方案

区块链作为一种软件创新形式，在用户之间建立数字信任，从而促进价值通过网络从一个实体转移至另一个实体。其目的是在不需要传统公共机构或中间人的情况下实现资本的安全保存和汇款结算。Fantom认为，区块链技术要实现在现实生活中的广泛应用，必须做到易于转让，不可撤销以及交易费用极低甚至为零。然而，现有的区块链技术由于确认时间较慢以及交易费用偏高仍存在很多局限性。

[2] https://bitcoin.org/bitcoin.pdf

[3] https://eprint.iacr.org/2016/168.pdf

3.0 技术概要

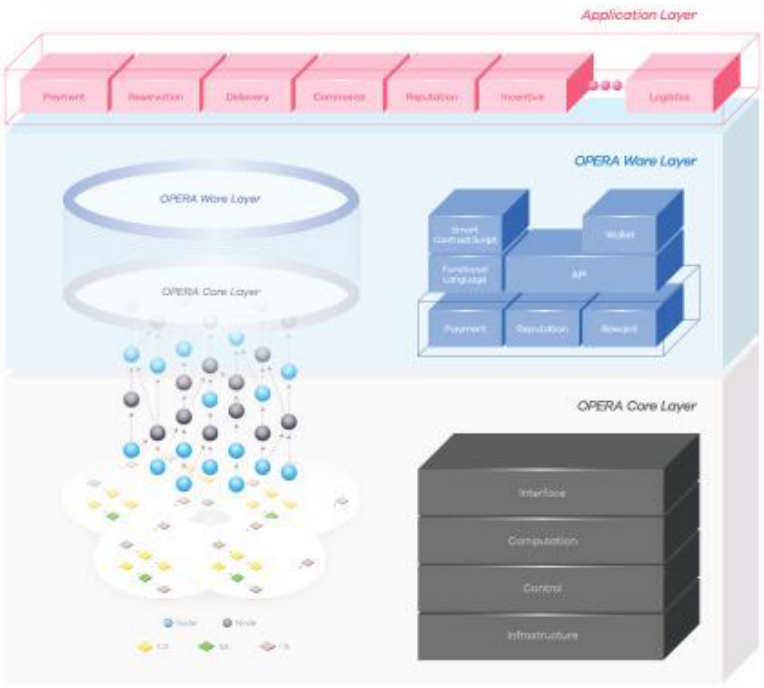
3.1 绪论

Fantom平台拥有一项名为OPERA的独特技术。OPERA链作为一种新型分布式基础架构，旨在通过大规模快速处理块来解决现存区块链的扩展性问题。同时，OPERA链试图在分布式环境中实时处理交易信息以及“Story Data”。

“Story root”存储于事件数据中以记录详细的历史信息。其结构和一般交易结构相似，但是“Storyroot”在某些属性的继承方面意义更加广泛。“Story root”的运行原理将在接下来的科技论文中加以介绍和解释。

Fantom OPERA链将使用基于Scala的高级函数编程语言，这种语言遵循Fantom网络上的智能合约字节码。

Fantom OPERA链由三层组成：核心层（Core Layer）负责大规模处理交易，OPERA软件层（OPERA Ware Layer）负责支持智能合约以及其他功能，OPERA应用层（OPERA Application Layer）为第三方应用程序提供支持。OPERA核心层（the OPERA Core Layer）的目标是在Fantom生态系统中运行可靠的交易，以及在信息交换中运用核心链技术。OPERA核心层（OPERA’s Core Layer）作为一种链技术，理论上每秒可处理的交易多达300,000份。



<图3.1> Fantom结构

3.2 OPERA链

3.2.1 Lachesis共识算法

3.2.1.1 介绍

OPERA链将使用名为Lachesis Consensus Algorithm（LCA）的新型共识算法，该算法旨在使用基于DAG的分布式账本技术来提高性能和安全度。LCA期望成为一种拜占庭容错（BFT）技术，这种技术能够保证与现有区块链类似的共识水平。它不仅可以防止特定节点故障导致的攻击，还能做到每秒处理300,00多份交易。OPERA链计划使用加密技术来增强节点之间通信的安全性，并使用函数编程语言以获取完整的智能合约支持。

LCA打算在Lachesis协议的基础上形成“Lachesis DAG”。事件块之间的一连串链接形成DAG，DAG作为一个分布式系统，可存储不可更改的任意数据。事件块包括以下信息：交易，智能合约，历史信息以及之前交易的价值等。

中央权限操纵整个结构将一个事件块与之前的事件块连接起来。后期事件块的添加使得前几轮的事件块得到更加充分的验证。<图3.2.1-1>展示的是先前提到的Lachesis DAG的结构。

LCA打算完全异步运行，需要两份相同交易时（即双重支出问题），只有最早的交易会得到验证。交易之间的顺序由主链表辅助安排。

<图3.2.1-1> Lachesis DAG

3.2.1.2 组件

LCA在Lachesis图上运行，它包括事件（Events），Clothos，Atro-pos和主链（Main Chain）。

事件块

事件块数据结构包括以下内容：

•存储数据：单个事件块可包含多个数据包，数据包的类型多样，具体包含哪种数据包取决于交易，智能合约，历史信息，声誉管理以及补偿等。
•签名：即创建事件块的用户的签名，用户可通过账户或是地址进行识别。
•前一个事件块的一个或多个哈希值：包含此值以提供事件块之间的链接。同其他的区块链技术一样，只要新的事件块验证了之前全部事件块（包括其中的交易），所有新的事件块将只能验证其父事件块。新事件块将通过哈希（Hash）连接到其父事件块，并且所有的哈希（Hash）由父事件块衍生而来，因此，先前的事件块无法修改或删除。一个事件块连接成功之后，另一个节点将在这个已连接的事件块之上构建新的事件块。

标识表（Flag Table）

Flag Table作为一种数据结构，可以储存某一事件块（Clothos）的连接数据。这种数据结构包括以下内容：
•Clotho指数：包括每个Clotho的索引信息
•连接：包含与其他Clotho连接的信息

Clotho

Clotho是一个包含Flag Table的事件块，可以看到大部分之前事件块路径中创造的块。能够连接大多数事件块的事件块会被指定为“Clotho”，并被用于Atropos的任命与其他事件块的共识。

Atropos

Atropos作为主链（Main Chain）的一部分，是在Clothos信息的基础上指定的一组特殊的事件块。可用Atropos来验证特定阶段的事件块。

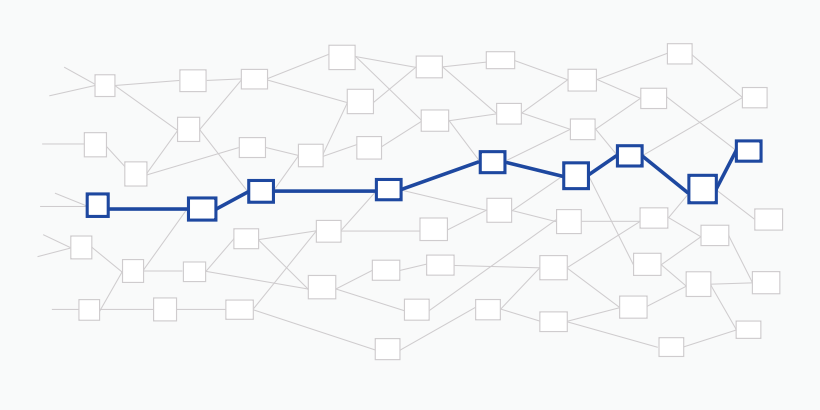
主链（Main Chain）

主链包括Atropos及相关事件块，主要用于事件块的验证以及整个系统结构的维护。

3.2.1.3 工作原理

Lachesis技术旨在实现高性能和安全的数据存储。所有的事件块都可从节点起进行异步创建，每个事件块都包含一组业务（如支付，汇款，智能合约，story，声誉以及奖励）。新的事件块会被连接到父事件块（之前事件块中最近的一个），而且该节点将通过Lachesis协议高速生成块。

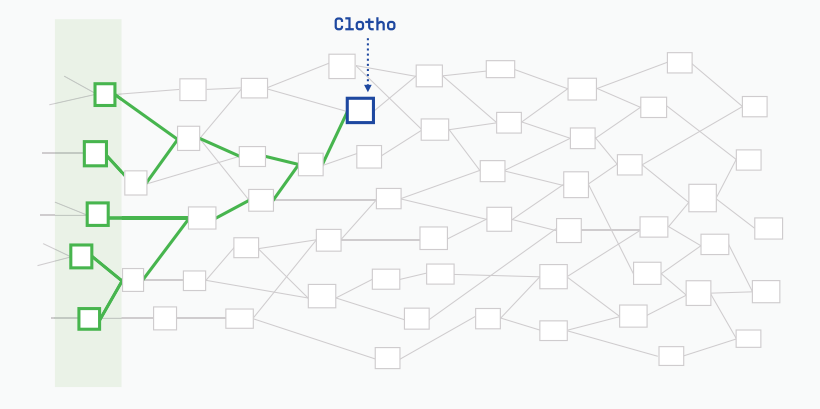
Lachesis协议内容如下图，里面的所有事件块都得以连接。还有一种通过集合块进行连接的链，我们称其为主链。图3.2.1-2展示的是所有Lachesis DAG上存在主链的假设。



<图3.2.1-2> Lachesis DAG主链

主链作为一组事件块，可以验证一段时间内创建的事件块。LCA可以在维护主链的同时有目的性地生成错误事件块，从而有效解决诸如双重支付或恶意攻击等问题。主链还对异步产生的事件块之间的排序有影响，它会让先产生的事件块在序列中具有优先级。主链的核心是Atropos

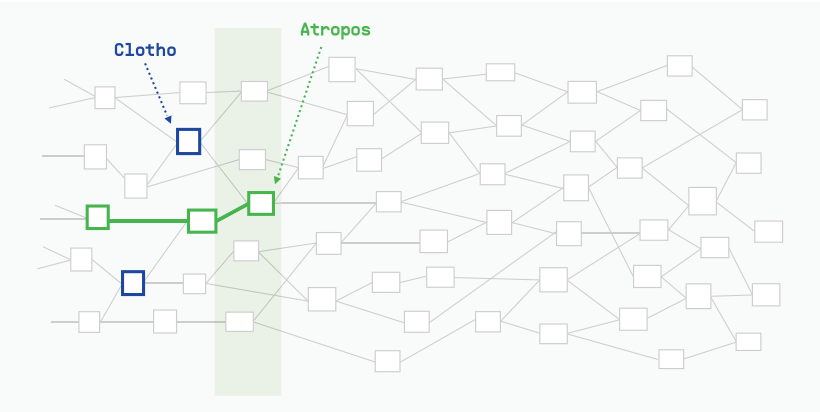
<图3.2.1-4>展示的是Clotho存在于某一Lachesis DAG中的例子



<图3.2.1-3> Lachesis DAG的Clotho

Lachesis DAG中存在一个Clotho，它与一组事件块中近七成的块具有联系。在事件块的随机分布中，Clotho所处的位置与大多数事件块位置的偏差最小。每个Clotho都有一个Flag Table，用于存储同另一个Clotho集的连接信息。

使用Flag Table（Clotho之间的连接信息）也就指定了Atropos。利用Flag Table的信息进行Atropos指定的过程中，事件块与Clotho组之间达成共识，这种共识将促成一个BFT（拜占庭容错）。



<图3.2.1-4> Lachesis DAG的Atropos

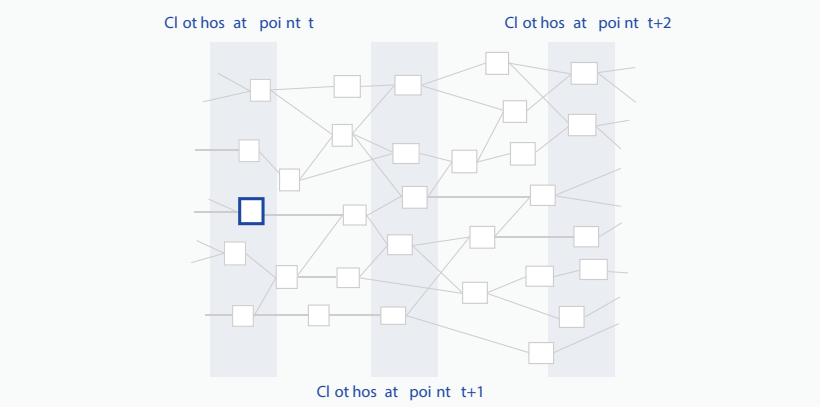
Atropos事件块是Cloth事件块的子集，它们为现存主链事件块的连接生成信息，并能完成新的主链。Clotho作为所有事件块的中间块，位于路径中的重要位置。 单个Atropos事件块可以检查某一轮（所有的父块都在这一轮中）的有效性。指定Atropos和Clothos的算法是在事件块本身及其所有祖先快的基础上确定的。LCA异步完成主链。

父块的子块不能连接到另一个父块，这就意味着已经生成的块无法修改或删除。

$$Clotho(i) = \sum_{j=0}^{n-1} \frac{(N-1)}{d_G(i,j)} \ , i \neq j$$

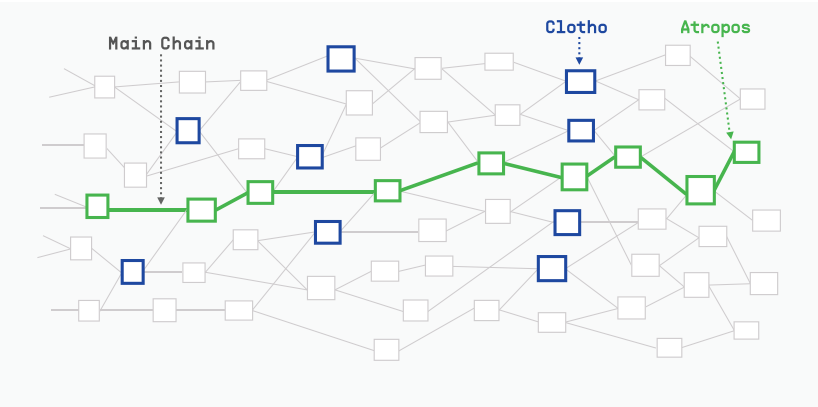
Clothos是特定时刻从顶点i到n-1的最短路径的总和。

Clothos会选择同一组中具有最大中心性的事件块。



<图3.2.1-5> 在Lachesis DAG中寻找 Atropos

<图3.2.1-5>为在某个Lanchesis DAG中选择Atropos事件块的示意流程图。假设1,2,3,4,5事件块为t点处的Clotho，13,14,15,16,17事件块为点t+1处的Clotho，27,28,29.30,31事件块为点t+2处的Clotho。所有的Clotho都有一个Flag表，这些表包含用于查找Atropos的连接信息。 Lachesis DAG包含快速查找Atropos的算法。要想让整个算法工作起来，Clotho需要找到Atropos，而且Atropos需要连接至主链。



<图3.2.1-6> 主链和Lachesis DAG中的Atropos

Atropos 被确定以及主链创建成功之后，就可以确定无序事件块的顺序。可以根据Atropos的事件块连接信息来确定每个事件块精确的共识时间。

倘若两个事件块的共识时间相同，那这两个事件块就会利用Atropos时间戳来确定视点（viewpoint）。特定事件块的时间点值会决定交易顺序。

3.2.1.4 程序

```
Lachesis Consensus Algorithm
         loop
         parallel procedure 1
                   create a new block on each Node
         parallel procedure 2
                   Find_Atropos(all_block, atropos, clotho)
                   Main_Chain(MC, atropos, clotho)
         end loop
```

<图3.2.1-7> Lachesis**共识算法**

<图3.2.1-7>展示的是Lachesis算法中的主要部分，简单易懂，一目了然。每个节点都可以同时异步自由创建新事件。这使得Lachesis与其他需要每个节点都参与共识的区块链技术不同。Lachesis算法旨在让每个节点能够平行创建块。每个节点都会通过向对方发送消息的方式来异步创建新的事件块。这些信息之间的交流将创建一个新的实体链。

这种简单的信息传递协议足以实现拜占庭容错（BFT）。每个节点收发信息的时候，都会通过在前一个事件块之后连接新的事件块来维持事件块的顺序。节点快速创建新的事件块之时，Lachesis算法会使用两种程序来创建主链并快速确定事件块的顺序。这两大程序无需每个节点参与通信。

```
procedure Find_Atropos (all_block, atropos, clotho)
         atropos[]
         heap clotho
         heap lookup
         for each clotho c
                   traverse flagtable c
                   if find atropos_path then
                             atropos[c]++
end procedure
```

<图3.2.1-8> 查找Atropos的过程

<图3.2.1-8>是查找Atropos事件块以创建主链的算法。Atropos将被包含于主链中，查找它主要是通过“Find_Atropos”这一程序来完成。使用某一特定时间的Clotho就可以找到Atropos事件块。

```
procedure Main_Chain (MC, atropos, clotho)
         heap MC
         heap clotho
         heap MC.last_block
         traverse lookup
         // optimistic MC_path between former and atropos
                   if find MC_path then
                             MC append set of list
end procedure
```

<图3.2.1-9>创建主链的过程

<图3.2.1-9>展示了创建主链的过程。Lachesis算法的关键因素是维护好主链，其对保持块的整齐很重要。在Lachesis算法中寻找Atropos和Clotho主要是为了提高主链的速度。完备的主链应该能保证OPERA链的安全，且能在BFT的创建过程中发挥重要作用。

3.2.1.5 椭圆曲线加密技术

Fantom的技术特点之一就是安全性。Fantom希望用安全性很高的椭圆曲线密码系统（ECC）技术来增强签名和节点之间传输数据时的安全性。椭圆曲线加密的优点体现在它能够用较短的密钥长度确保较高的安全性，并允许在签名时进行高速计算。椭圆曲线密码系统（ECC）运用最有效的算法来解决离散对数问题，从而很轻松地设计出一个安全的密码系统。这一密码系统的效率更高，因为安全性相同的情况下，它的密钥长度较其他的加密系统更短，

RSA1024位密钥才相当于ECC160位密钥。此外，无论是在硬件还是软件中，椭圆曲线操作都易于实现。Fantom还打算通过使用ECC增加对硬件钱包和软件钱包的支持，并增强这些钱包的安全性。此外，Fantom对使用ECC的secp256k1参数也很感兴趣。

3.2.1.6 对攻击的响应

Lachesis协议可能会受到恶意团体的攻击，这些团体的目的是获取经济利益或损害系统。在此，我们会解释一些可能存在的攻击场景，以及Lachesis协议会如何采取预防措施。

西比尔（Sybil）攻击

攻击者可以在一台计算机上制作成百上千个OPERA链节点。但是，鉴于OPERA链的节点操作方法和委任权益证明（DPOS）所用方法类似，投票系统产生的结果将用于准确地识别错误节点。攻击者不用获取额外投票来在网络中添加新的节点。此外，鉴于单台计算机只能创建单个节点，OPERA链中出现的西比尔攻击的可能性不大。

寄生虫链攻击

在基于DAG的协议中，寄生虫链背后往往会有一些恶意目的，例如，通过让此链看起来像合法的事件块来尝试连接。Atropos和Clotho在Lachesis协议支持下创建好主链，每个事件块的验证也就完成了。验证过程中，任何未连接到主链的块都视为无效而被忽略，双重支出就体现了这一点。

交易泛滥

恶意参与者可能会在其控制的账户中开展大量有效交易，其目的是让网络超负荷运行。因此，OPERA链计划征收最低交易费来防止类似情况。交易费用的存在让恶意用户无法继续实施此类攻击。而节点参与者会获得奖励，那些通过开展交易等方式为这个生态系统做出贡献的人也会不断获得奖励。这些奖励足以用于目的适当的交易。

但是，鉴于执行异常攻击需要巨大成本，恶意攻击者很难让交易泛滥。

3.2.2 功能语言

Fantom打算设计一个虚拟机来用现有的语言编写合同，以此来吸引大量开发人员。众所周知，Scala是一门支持式函数式编程语言，很可能成为源语言。Scala的优点如下：
Scala的开发是为了消除Java带来的不便，它让开发人员能够写出组织顺畅，条理清晰的代码。Scala的强类型功能可以促进开发，提高性能。例如，函数，宏和元组只是Scala提供的众多高级函数中的一部分。Scala作为一门精心设计的语言，集合了功能和面向对象的编程。字符串模式或Mixins包含类定义中的函数，让编写代码成为一件享受的事情。Fantom相信，Scala这样一种拥有全面文档的语言，是处于不同经验水平的开发人员的最佳选择。闭合器和函数是这门语言的一部分。Scala的最大优点是它能够同时提供面向对象和功能的编码模型。开发人员可以利用这两种方法的优势轻松编写简洁而且功能强大的程序。

测试和开发也很方便。和Java一样，Scala也能用短行代码写程序。尽管Java也有一些缩小代码长度的方法，但这些方法与标准编码风格有所不同，使得代码的可读性和效率有所降低。Scala本身具备的特点让写代码变得更加简洁，测试和分布变得更快。Scala拥有一个非扩展的API库，简洁但具备所有必需的功能。用Scala编写可扩展的软件可以让代码编写，测试，调试以及分配变得更加容易。该语言功能多样，可用于所有领域，包括桌面软件，游戏，网页应用程序，移动解决方案以及软件服务等。该语言也很适合编写智能合约。

Scala是一门使用非常广泛的函数式编程语言。一个名为“Play”的网页应用程序就是用Scala写的。这款应用程序已经成功登陆亚马逊和Coursera等众多IT平台。其优势已经通过产业中的实际应用得到了证明。Haskell作为广受数学家们支持的一种函数式编程语言，本身十分优秀，但其用户数量不及Scala。相对来说，Scala学习起来更容易，也更受欢迎，拥有的用户数量也更加庞大。而且Scala还支持面向对象的编程，这就进一步促进了其发展。此外，它具备所有精心设计的函数式编程语言的优点。运用删除“Side Effects”这一功能，许多编码错误以及任何可变的地方都可以提前进行识别，将代码传送到分布式环境中也变得更加容易。

Scala可以引进严格的编码技术进行编译和正式验证。正式验证作为一种数学方法可用来验证计算机程序的准确性。这一方法已用于维护军事系统，传输基础设施，加密和微处理器的软件和硬件。职能合约代码的正式验证如今也得到了认可，这一点在以太坊区块链上尤为突出。

下面就是Scala代码的一个例子，汇率一定的条件下，可用这个代码进行一定数量钱币的换算。

```
package FTM.example

import fantom._

object SendMoneyExample extends SmartContract {
        def Send100100(): Unit = {
                implicit val converter = Converter() LatestCurrencyRate

                val sum = 100.0 (USD) + 100.0 (EUR) To FTM

                Approve If (Sender.Balance >=sum){
                        Transaction {
                                () => Sender Balance Send (amount) To
                                (Recipient)
                        }
                }
        }
}
```

<图3.2.2> 使用Scala Fantom的步骤示例

4 http://antoine.delignat-lavaud.fr/doc/plas16.pdf

3.2.3 Fantom虚拟机

3.2.3.1 基于虚拟机的寄存器

现有加密货币平台使用的虚拟机（VM）大多以堆栈为基础，例如以太坊的以太坊虚拟机（EVM）。基于堆栈的虚拟机可以使用堆栈数据结构轻松执行指令。但是，如下所述，同基于寄存器的机器相比，基于堆栈的机器通常代码长度更长，执行速度更慢。DAG事件块中的存储价格十分高。代码会使用这种存储方式，因此很多指令十分昂贵。Fantom虚拟机旨在大幅减少容量并提升处理速度。基于寄存器的虚拟机可以将OPCODE的执行成本降低50%以上，并将性能容量提高近一倍。

3.2.3.2 基于堆栈的模型

堆栈是一种基本的数据结构。基于堆栈的虚拟机使用堆栈执行操作。假设我们正在执行一个简单的添加，则需要使用PUSH和POP操作来让四个命令行执行其他操作。基于堆栈的模型的优点是运算对象由堆栈指针进行隐式处理，即调用堆栈指针提供下一个运算对象（POP），并且不需要显式声明操作数地址。在基于堆栈的虚拟机中，所有算术和逻辑操作都是按下面这种方式完成的：首先弹出并计算堆积在堆栈上的值，然后将计算结果放在堆栈里。例如：

- 加载A：将本地变量A存储到堆栈
- 加载 B：将本地变量B存储到堆栈
- 添加：添加两个值
- 储存C：将操作结果存储到本地变量 C

3.2.3.3 基于寄存器的模型

基于寄存器的虚拟机在存储操作数时，会对CPU寄存器建模。即使没有PUSH或POP指令，命令也必须包括指针名称，而且命令操作数必须加以明确说明。例如，在基于寄存器的虚拟系统上执行“添加”时，该命令如下。您会发现此代码比之前基于堆栈的版本要短：

- **添加** AX，BX，CX; **添加**AX**与**BX**并存储到**CX.

如前所述，此处并没有POP或PUSH指令，因此只有一行代码。但是，与堆栈不同的是，此处操作数（如AX，BX和CX）的地址必须加以明确说明。此处没有使用堆栈推送和弹出的开销，因此，基于寄存器的虚拟机的命令更快。

基于寄存器的模型的另一个优点是，无法用基于堆栈的方法进行的优化可由基于寄存器的模型完成。例如，执行两次相同的计算的时候，可将寄存器模型代码加以优化，使其仅能够进行单次计算，并将该值储存至计算机以备再次使用，从而提高代码的执行速度。

基于寄存器的模型的缺点是需要明确声明操作数地址，与基于堆栈的模型相比，这就增加了命令的平均大小。基于堆栈的虚拟机非常短，因为它不无需明确说明堆栈地址，而基于寄存器的虚拟机必须包含OPCODE里操作数的位置，这就增加了单个指令的大小。但是，正如Dalvik将其与Java虚拟机对比以后所证实的那样，整个代码库的规模可以大大缩减。

5 Yunhe Shi, David Gregg, Andrew Beatty. Virtual Machine Showdown: Stack Versus Registers. 2005.

3.2.3.4 具备图灵完整性的虚拟机安全且强大

鉴于我们无法知道未来需要哪些类型的操作，提供图灵完整性对于建立DApp生态系统至关重要。然而，提供图灵完整性不可避免导致不可能达到决策的问题。为了解决这一问题，以太坊引入了“GAS”这一概念来避免停机问题。

但是在以太坊代码中，气体消耗量是硬编码的，没有硬叉就不可能灵活地改变这种情况。此外，尽管一些操作很关键，因为是执行器决定是否执行合同，但是低级程序可能会也可能不会执行这些操作。2016年9月发生的DDOS攻击以太坊虚拟机实际上就减慢了网络速度，几乎让其停机，因为攻击者能够利用低油价来攻击网络。

Fantom计划以理想中灵活的执行成本来设计出Fantom虚拟机，与此同时，该虚拟机操作节点的权限也要受到限制。Fantom认为，使用LCA即意味着无需执行所有节点的相同指令集。即使攻击可能发生，其灵活性也会将攻击对网络的影响限制在一定的范围内。

不仅以太坊虚拟机存在安全性和可行性问题，许多分布式账本项目也存在上述问题。一些项目（如比特币）通过删除图灵完整性来减轻这些限制，以太坊则通过提供大量智能合约模板来支持正式验证。但是，缺少结果功能使得实现合适的DApp变得困难。

Fantom虚拟机希望提高安全性能和图灵完整性。此外，它还提供正确建立DApp生态系统的核心功能，例如外部代码链接，库和导入，以及可以网格超级计算机一起运行的强大可扩展性。基于Fantom的智能合约不仅可以独立工作，还能作为DApp框架的一个组成部分，与其他协约协同工作。

6 David Ehringer. The Dalvik Virtuoal Machine Architecture. p5, 2010.

7 https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/

3.2.4 OPERA链的结构

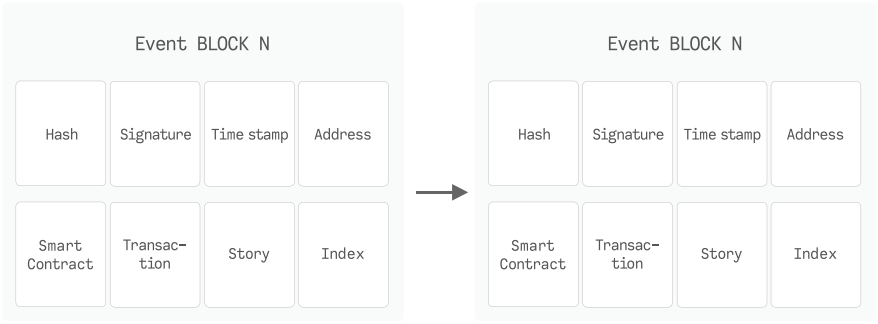
与现有的区块链结构类似，Fantom的OPERA区块链结构有其独特特征。旨在囊括哈希（hash），签名，时间戳，地址，交易，智能合约，Story以及索引信息的新型数据结构里添加了“Story”的概念，详细讲解如下。

在OPERA链的事件块数据结构中，哈希（hash）是指前一个块的值。

交易是按块的交易列表中每份交易填充的值 。

智能合约包含账户创建的智能合约的信息 。

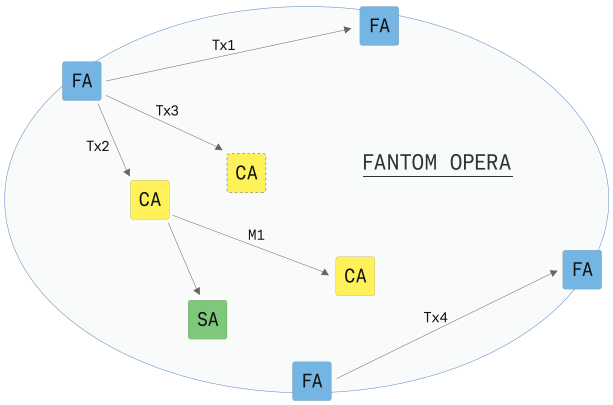
Story旨在记录不断变化的详细信息，例如有点分布历史的信息。即事件块中的交易里填充的Story的交易值。Story的结构与交易结构类似，但其结构已经扩展到拥有继承属性的信息。此外，它还添加了阻止将存储复制到事件块中的算法。



<图3.2.4-1>事件块的数据结构

OPERA链包括一个外部持有账户和一个合约账户，前者由私钥控制，后者由控制代码控制。它还拥有一个Story帐户，该帐户由合同代码创建，以便管理Story信息。账户拥有可供Fantom使用的地址和Fantom代币。外部持有账户持有由私钥控制的地址，并且可将已获准交易的代币交给其他账户。外部账户可以创建新的合约账户。而且条件满足的前提下，预编程订单会执行合约账户。若有必要，一个合约账户可以调用另一个合约账户。但是，在未经外部账户调用的情况下，上述行为不成立。

OPERA链中智能合约功能应设计为根据预编程模式自动运行，即一旦满足某些条件，它就会运行。 智能合约的一些条件得到满足以后，一旦自动运行完成，OPERA链的Story也就得以创建。其功能是为智能合约储存交易以及一些Story数据。



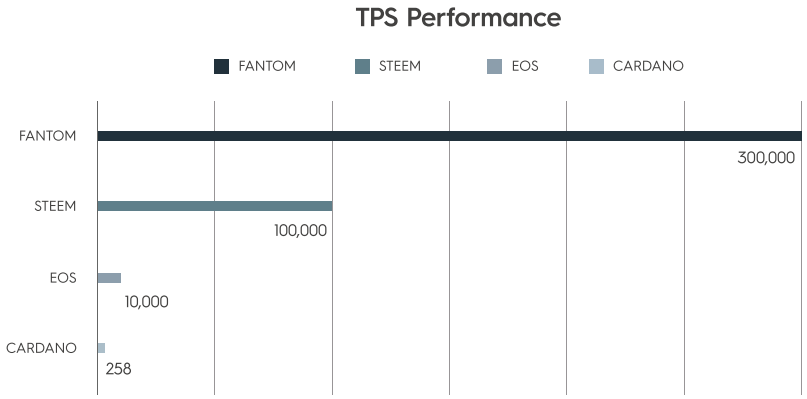
<图3.2.4-2> OPERA链内不同账户的交互

分布式应用是一种能在OPERA链的分布式环境中运行的应用程序。分布式应用程序可利用Fantom网络的资源提供可靠性与安全性，还能帮助运行合约代码，这些代码存储在用户浏览器中的Fantom中。Fantom支持免费的网页生态系统，对创建新的基础架构做出了贡献，还能有效地用于超链接网络。此外，它可通过担任代理人或中央控制机构推动业务流程的变革，还能提供跨国境服务。

倘若创建了新的块，或者账户状态发生发生改变，OPERA链会存储这些数据。块头会使用Merkle树的哈西树结构来保存每个状态值。 在Fantom中，OPERA提供了实施智能合约的环境，对Story信息进行交易，并在每次创建块之后将块头信息保存至Story的根目录中

3.2.5 OPERA链的性能

OPERA使用独一无二的Lachesis协议算法，旨在解决快速处理块时出现的延展性问题。与之前的区块链技术相比，第三代区块链的技术的性能有所改进，但创建块的速度依然很慢。OPERA链的目的是确保每秒高达300,000笔交易的快速创建和处理性能。凭借高可靠性和强扩展性，Fantom相信自己能够促进第三代区块链技术，这一技术可跨多重领域和产业得以大规模利用。OPERA链不仅要规模化处理大量交易，还要处理能够确保交易可靠性的Story和历史信息



<图3.2.5-1> Fantom TPS功能

OPERA是基于Fantom的 Lachesis协议算法，旨在同步通过多次验证，同时测试交易的方向性和合法性。每个节点在处理分布于Fantom网络上的所有交易时，都应该提供最好的交易处理速度。过去，所有的参与者都按顺序验证每个块。但是，Lachesis协议算法将被设计为用分布式并行方法异步验证和处理事件块。

LCA处理的每个事件块的大小最多可扩展至100KB，鉴于块的传输速度更快了，Fantom认为事件块这一大小是足够的。例如，假设每个交易为260字节，那么单个事件块包含的交易将多达440个。如果每个节点创建一个事件块所需的时间为0.1s，则每个节点每秒将创建7到10个事件块。假设要求的交易数量是无限的，并且有100个节点参与，那么，每个节点每秒将异步同时创建7到10个事件块。一旦事件块的数量达到参与的所有节点的2/3时，Lachesis协议就会添加并验证另一个主链。如果可用的节点为100个，每秒就会创建700~1000个事件块，并同时得到验证。鉴于每个阶段都验证和处理大约700到1000个事件块，超3000,000TPS的性能可以实现。但是网络延迟等因素可能会降低tps

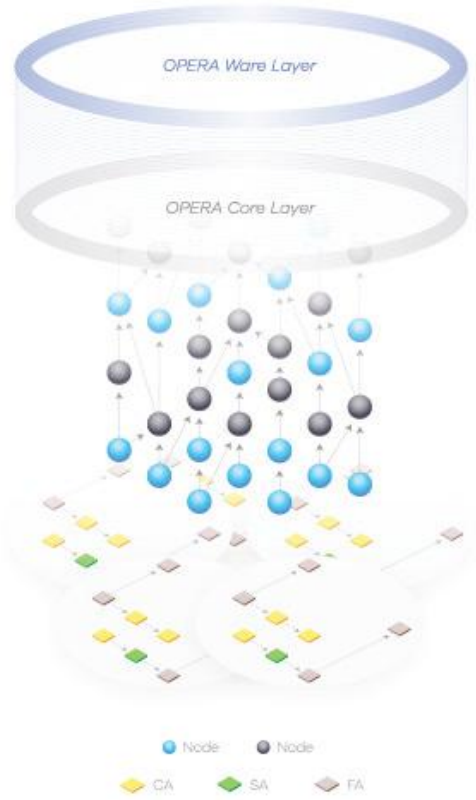
Fantom认为，Lachesis算法的时间复杂度意味着使用O（N Log（N））可以实现更快的运行速度。

由时间复杂度O（N2）和O（N Log（N））（n指节点数）来计算运行速度的方式如下。

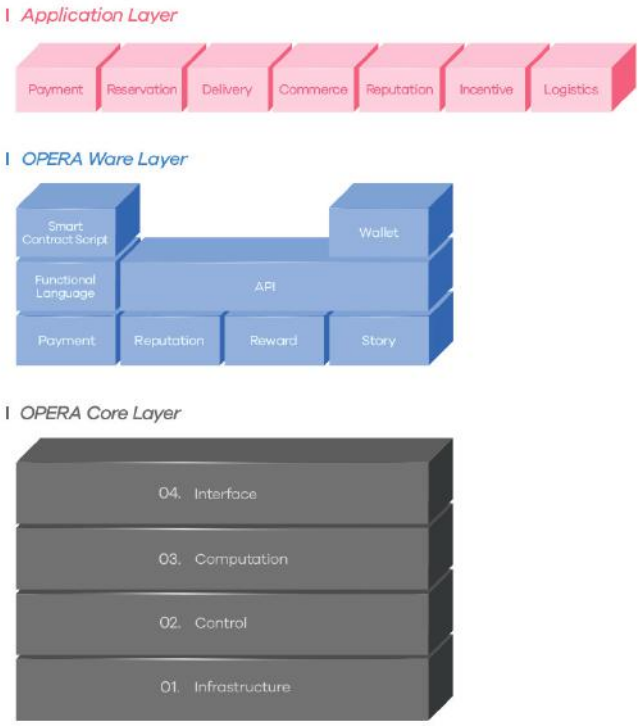
n^2= n * n
n Log N = n * log（n）n * n vs n * log（n）
n vs log（n）

如果n = 10，则nlog（n）~2.3
如果n = 100，则nlog（n）~4.6
如果n = 1,000，则nlog（n）~6.9
如果n = 10,000，则nlog（n）~9.21
如果n = 100,000，则nlog（n）~11.5
如果n = 1,000,000，则nlog（n）~13.8

4.0 OPERA的多层组织



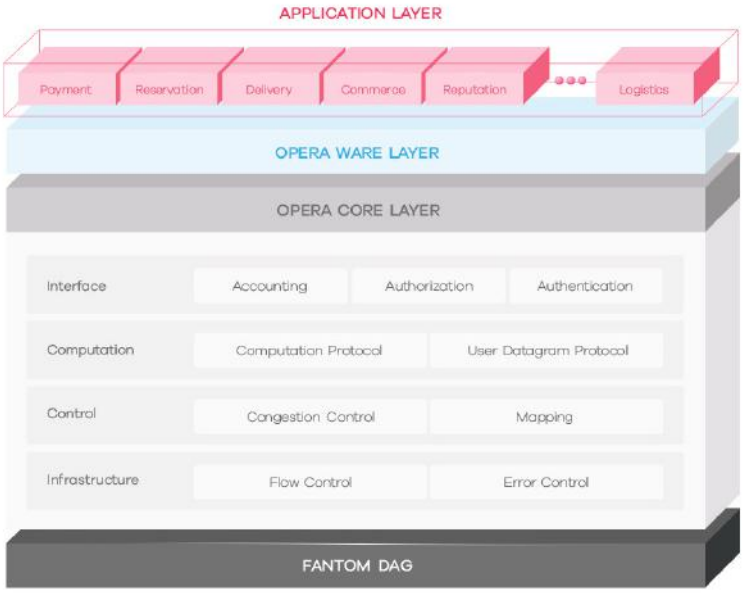
<图4.0-1> OPERA链的多层组织



<图4.0-2> OPERA链多层组织的结构

Fantom的OPERA链是双层结构，由可支持各种应用程序的OPERA软件层组成，如通过付款，收款，保存，交付，商业和信誉数据处理事件块的OPERA核心层。与此同时，在OPERA核心层中，用于确保交易可靠性的核心链技术以及Fantom生态系统中的交换信息可以运行。

4.1 核心层



<图4.1> Fantom OPERA核心层的结构

4.1.1基础结构

OPERA基础结构是Fantom生态系统的核心。Fantom会使用Fantom OPERA基础结构。在分布式环境中收集和处理区块链数据时，与其他的区块链相比，OPERA链会提供更多功能。

OPERA基础结构层中，有关交易、智能合约、和Story（历史信息）等信息都被映射并储存至控制层中，这些信息来源多样，有些来自付款，预定，交付，商业和信誉等领域的各种应用程序，有些来自操作计算层中当前与先前事件块数据的结果，有些数据则能反映前一个事件块的价值。

每个应用程序里事件块的主链会创建起来，而直接或间接连接到主链的事件块的索引都会被存储起来。

结构层要确保实体网络之上的对象能够平稳可靠地传输数据。它提供了传输事件块数据或发现和修复错误所需的功能或程序手段。它还提供了修复错误的功能，来验证那些识别和传输物理设备的数据未经伪造。它也通过将事件块数据分组并传输到帧，然后重新计算并比较每个帧的校验和，从而来检查和修订错误。此外，它还通过验证和调节数据传输速度这样一种流量控制的方式来防止帧丢失，通过检查是否所有的帧都有序传输至目的地这样一种错误控制的方式来处理错误。而且，它还能应对可能出现的一些冲突。

对于一些由现有主机运行应用程序的平台服务，Fantom在保持Fantom OEPRA链系统的优势的同时，应确保其能转换为免佣金网络。

4.1.2 控制

控制层能控制基础结构层。而且，它能将计算层中处理的结果映射到基础结构层。

控制层可评估指定交易，智能合约，Story（历史信息），信誉管理以及奖励等某些操作是否经过准确计算并且是否可靠。它还能记录编写智能合约所需的所有详细信息。此外，它还能验证计算层执行的操作，并将每个事件块的数据物理性映射至基础结构层。

控制层可评估指定交易，智能合约，Story（历史信息），信誉管理以及奖励等某些操作是否经过准确计算并且是否可靠。它还能记录编写智能合约所需的所有详细信息。此外，它还能验证计算层执行的操作，并将每个事件块的数据物理性映射至基础结构层。 控制层具备拥塞控制功能，用于控制数据传输时产生的拥塞，还具备在系统与高级系统之间，建立，维护和终止数据传输线上的网络连接的功能。

此外，事件块数据被分成数据包并在传输后重新统一。为了确定数据通信的最佳路径，会使用路径算法来分配逻辑地址，而且数据包会由发送器传输到接收器。

4.1.3 计算

Fantom的计算层运行并操作应用程序里的交易，智能合约和Story（历史)数据。计算层会分析从控制层中接受的流量，并对服务类型进行分类。计算层使用TCP/UDP协议与接口层和控制层通信，以在事件块中发送和接受诸如交易，智能合约，历史数据，管理数据以及奖励数据之类的数据。

计算层还会检查错误以确保数据发送中的准确性，并安排事件数据的顺序。此外，计算层会提供区分可信传输和不可信传输的多种通信，确保操作处理的公正性，整个网络的优化性以及系统的扩展性。

4.1.4 接口

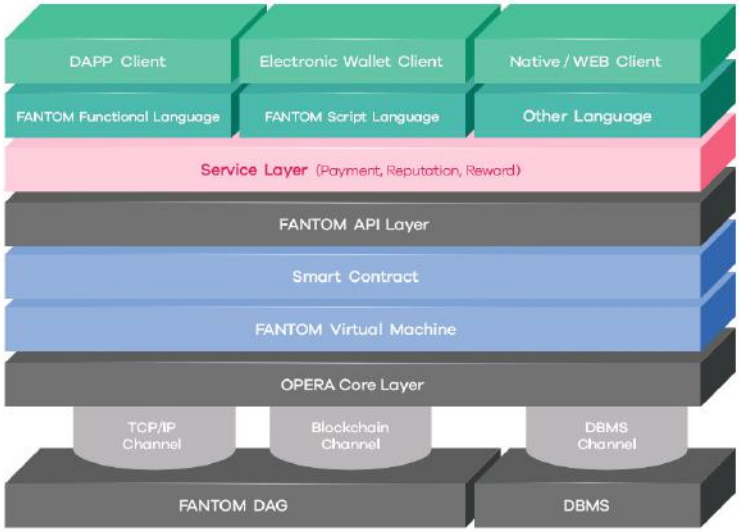
接口层创建的环境里，每个应用程序都能访问Fantom OPERA链。它会管理和监督参与网络的每个账户，限制和验证节点的权限。它还会验证Fantom钱包地址和交易签名等数据，以检查某个账户是否已获得合适的授权。

Fantom OPERA链中的OPERA核心层和OPERA软件层通过Linux内核环境中的TCP / IP通道和DBMS通道等接口进行通信，发送和接收交易数据。接口层验证和管理每个应用的全部交易，映射和发送验证完成的数据至OPERA核心层的计算层以执行操作。

接口层为每个层提供控制结构，并维护和同步账户设置。管理和调整传输数据至软件层（由不同的节点控制）所需的对话。提供按序组合和同步每个事件块数据所需的方法，以及建立、调整和终止应用层单元之间的对话通道所需的方法。

4.2 OPERA软件层

OPERA Ware层提供各类dApp所需的开源API、智能合约脚本、函数式编程语言、钱包以及中间件（如支付，信誉，奖励）。Fantom代币是OPERA软件层中交易的基本组成部 分。OPERA软件除了具备Fantom代币这一核心功能外，还支持与交易相关的适当奖励。根据每个参与者（消费者，公司和生产者）的信誉评分和交易记录，使用Fantom代币进行支付。



<图4.2>Fantom OPERA软件的平台结构

4.2.1 中间件

Fantom的OPERA链的中间件统称为链接Dapps的协议和API。中间件包括API，Scala功能语言，智能合约，电子钱包和协议（支付，声誉，奖励和Story），它将应用程序和OPERA核心层连接起来发送和接收数据。

<图4.2>展示的是Fantom中间件平台的体系结构。该结构包括Fantom开发环境和虚拟机。如上面的体系结构所示，Fantom中间件平台由主服务的模块层组成。这种模块化架构实现了在开发智能合约时，可以很轻松地对智能合约的相关服务进行修改，扩展和整合。此外，为了集成现有的支付服务（如PG服务）以便于使用Fantom服务，提供了类似于现有类型的Native / Web客户端SDK，从而确保其能整合至现有的服务环境中。

Fantom中间平台不仅提供支付服务，还集成了奖励和信誉服务，给使用OPERA链的应用服务进行交易的客户提供各种各样的奖励服务。这样的奖励服务创建的环境可与其他服务协同提供额外的综合奖励服务。

Fantom通用框架层管理账户，认证和消息传输，这些都是访问使用DApp，电子钱包和Native-Web客户端的平台所必需的。账户管理的设计从一开始就是用于多语言支持，以确保服务扩展至国外以后，该功能依然易于使用。

此外，加密方法也用于账户信息（包括敏感信息），并且采用严格的安全设计，即使是内部管理人员也无法访问此类信息。安全服务的主要流程如下图所示。认证管理基于OAuth 2.0，它简单直观且允许使用各种加密方法。

OAuth 2.0还支持扩展到大型应用程序。此外，在考虑到监管环境的基础上，可使用IOS和Android设备支持的标准Push方法来处理消息：提供支付服务（如短信和邮件通知）时，可使用法律要求的信息处理协议。

客户层由DApp客户端，电子钱包客户端和本地网页客户端组成。关于DApp客户端，集成开发服务环境（如Fantom虚拟机和开发语言）将在下一阶段的开发中的得以运用。此外，当前这一阶段还会开发和提供电子钱包客户端以及本地网页客户端。电子钱包中的服务致力于Fantom币的交换，而且，如有必要，这种功能将扩展至与其他币的交换。奖励服务和声誉服务作为OPERA软件的主要特色，也会得到运用。最终，Native / Web客户端会提供支付，奖励以及声誉服务，在现有的环境中，这些主要由OPERA软件服务以集成方式提供。

开发语言层由Fantom高级函数编程语言，Fantom脚本语言和其他语言组成，可使用上述几种语言轻松开发和利用智能合同服务。后续开发阶段计划还会使用开发语言层，此外，还将提供开发语言所需的集成开发环境。

服务层包括包括支付，声誉以及奖励服务。在第一个开发阶段，其他服务可使用对外公开的IOS或Android客户端SDK和电子钱包客户端。服务层应允许其服务扩展为智能合约，这些合约可通过下一阶段的Fantom开发语言和Fantom虚拟机实现。

Fantom API层提供基础架构，允许在Fantom服务环境中开发的服务应用程序运行。这一独立层还允许与其他币的连接或扩展，并帮助其扩展至其他服务领域。Fantom API层还包含处理智能合约，区块链和交易的模块。由Fantom API层所处理的交易能够检测和预测由国内PG公司或卡公司运营的Fantom币支付的任何可疑记录，从而系统化地防止非法交易。

Fantom虚拟机层作为主要组件，能够在不同服务环境中公开Fantom服务生态系统，它还为Fantom服务环境提供通用基础架构并促进各种DApp的开发。

Fantom通信层旨在实现与区块链，TCP/IP，同步信息，异步信息以及DBMS之间的通信。将用于通信的抽象层与物理层分开，从而允许该通信层与TCP / IP，同步信息，异步信息，以及DBMS进行直接通信，还允许开发人员用其进行编程而无需使用复杂的通信编码。

4.2.2 智能合约生产工具

Fantom OPERA链提供智能合约脚本编辑器。它允许输入符合DApp特征的各种交易条件来辅助编写智能合约。

OPERA链的智能合约脚本处理的交易类型适用于每个行业的参与者，例如通信，财务，物流和电动车车辆供应。

智能合约在Scalaz中进行编码，并通过Fantom虚拟机使其符合字节码，因此智能合约具备图灵完整性。

4.2.3 OPERA钱包

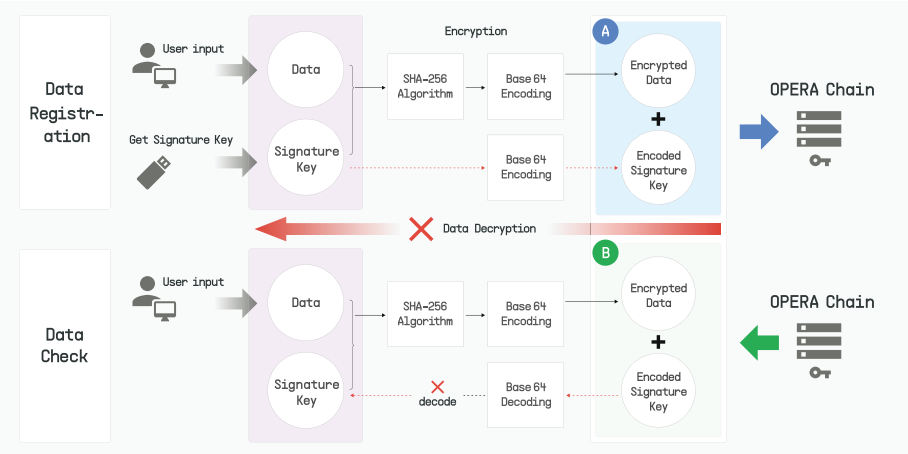
用于Fantom交易的电子钱包Native/ Web客户端旨在提供分布式服务，这些服务包括钱包管理，多地址管理（主帐户，提款帐户，存款帐户），地址验证，加密处理，解密处理以及交易货币组件兑换。 Fantom使用微服务架构为Fantom币交换服务领域的扩展做准备。每个组件的细节如下。

钱包管理组件通过扫描二维码，快速识别服务用户的电子钱包地址一次提供相关服务，并在输入数量后立即进行交易。此外，它还可以使用IOS/ Android Native和网页的方法，用电子钱包服务在不同的环境中部署Dapp以及操作系统，从而实现外部交易。

多地址管理组件通过将账户划分为主账户、提取账户和存款账户的方式来管理电子钱包的地址。这可以防止电子钱包服务在使用服务期间（如付款，存款等）被暴露，并最大限度地减少因电子钱包地址的暴露而引起的损失。例如，一个商人在销售产品时，只向顾客提供商家的存款账户地址。即使使用这种交易服务的电子钱包的地址被暴露，它也可以最小化损害，因为地址仅提供接受存款的功能。

地址验证组件通过连接公钥，私钥以及电子钱包所有者的信息来验证电子钱包的地址。这一过程使电子钱包地址的伪造变得困难，还允许根据环境中的变化对验证逻辑加以修改。标准的加密/解密方法提供电子钱包地址上使用的加密和解密服务。

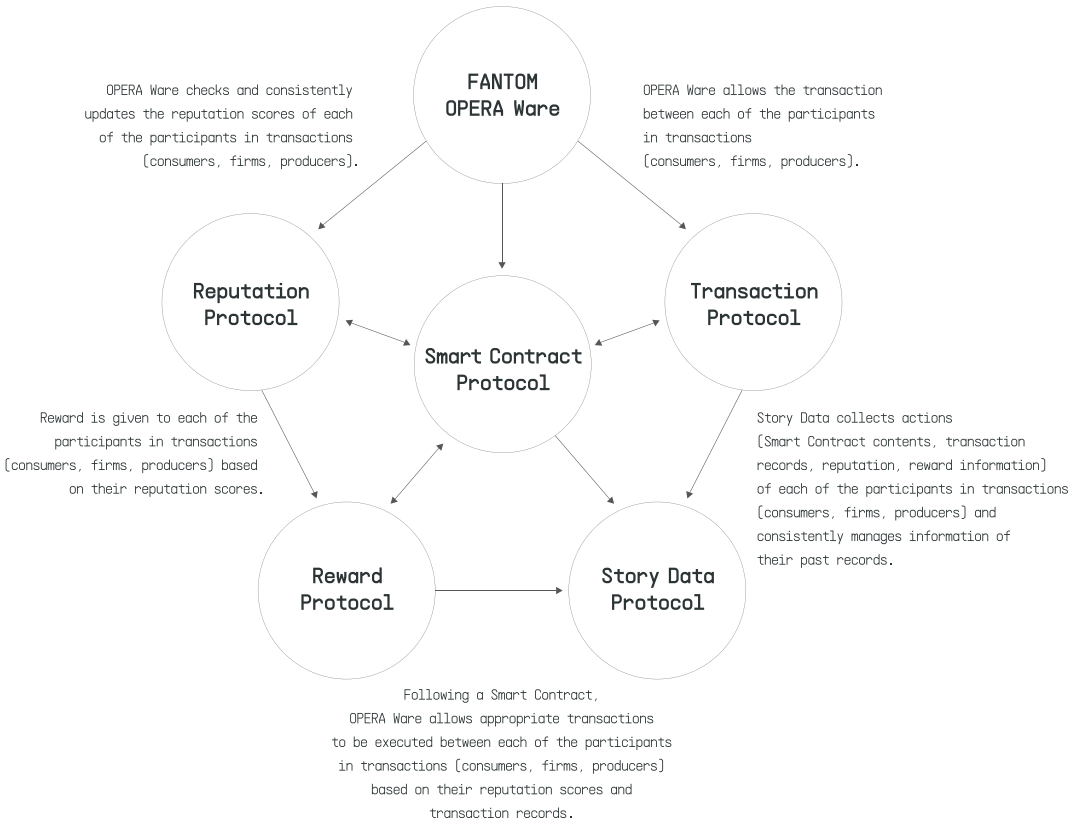
交易组件允许用户将Fantom币从一个账户转移至另一个账户，或转移至在Fantom网络之上运行的其他代币。



<图4.2.3> Fantom钱包的运行平台

4.3 Fantom OPERA软件协议

OPERA软件使用交易，智能合约，Story，声誉以及奖励协议。



<图 4.3> Fantom OPERA软件协议

4.3.1交易协议

根据交易协议，OPERA生态系统的参与者（从事电信，金融，物流，电动汽车，销售，餐饮，生产等的企业）像消费者提供合适的商品或服务。例如，Fantom的OPERA链的交易协议可用于食品配送行业，如下所述。

应用示例：食品配送

这些应用程序由在OPERA链上运行的智能合约编写而成，能够允许消费者在线下单食品和接收食品之后（这一时间可以是预定的时间，也可以是支付时间）支付费用。消费者使用食品配送应用程序主机下单食品，并发送代币。食品配送完成后，消费者支付的代币将根据预定义的智能合约转移至餐馆。

倘若食物配送不成功，消费者可要求更换食物或退还费用。智能合约的设计将允许餐馆或送货员退款给消费者，这将由OPERA支付协议执行。

餐厅和送货员还将使用应用程序主机，根据智能合约的相关条件批准退款。一旦获得批准，将根据预定义的智能合约进行退款，将相应的交易代币按一定比率由基础算法得出结果后转移给消费者。餐馆还可以向应用程序主机付款以进行广告宣传。

4.3.2 智能合约协议

智能合约作为一段代码，可在没有合同文件或是第三方的情况下在线支持，验证和执行合同要求，它还能再现合同条款的逻辑。

在分布式账本上运行的智能合约允许以透明的方式交换货币，资产，股票或任何其他贵重物品，而无需经纪人或第三方。“传统”合约在收到货物和服务前，需要经纪人，政府机构，银行，律师或公证人的第三方参与，以及一定的处理时间。但是，智能合约技术的使用将使上述大部分内容实现自动化。

这种智能合约技术与自动售货机原理类似。自动售货机可根据预编程规则运行，相关条件满足就能够确定输出的货物。使用自动售货机时，用户将钱存入机器并输入具体的商品数量，之后就可以拿到想要的产品。上述存入的钱按照智能合约的规定会在OPERA链中进行托管和保存，一旦满足相关条件，将立即转移至相关交易人员手中。

Fantom的OPERA链的智能合约协议根据每个行业的条件和要求处理参与者之间的交易。

智能合约中的一些条件得以满足，并且合同成功履行之后，OPERA的Story就得以创建，并将消息信息存储至Story数据段中以用于交易和智能合约。

4.3.3 Story协议

Story协议用于记录和管理变量值，例如从产品生产到分发的全部历史数据。它使用交易链中STORY段所捕获的数据。虽然其结构与交易段类似，但STORY段的结构具有附加域以获取更多信息，还具备从父交易中继承属性的能力。此外，防止空间浪费和信息冗余的算法也得到了应用。

Fantom的OPERA链提供创建智能合约的环境，能用STORY数据处理交易，并在每次块成功创建时将头节点信息存储至STORY根目录。

4.3.4 信誉协议

信誉协议里所有的Fantom生态系统参与者可以相互评估，这些参与者包括生产者，消费者，销售人员，交付机构，快递员等，当然这要取决于具体的行业。每一方参与者的信誉会根据其数据和反应进行确定，然后对应相关标准算出合适的奖励。

$$\sum_{i=1}^{n}(A_i\alpha_i) = \frac{A_1\alpha_1 + A_2\alpha_2 + A_3\alpha_3 + \cdots + A_n\alpha_n}{n} \ (n \geq 1, \text{Integer})$$

<公式4.3.4>计算信誉分数的公式

- A被定义为每个行业的参与者的评估标准，其中A是0到100之间的实数。
- α是由A值计算出的每个评估标准的加权值。
- n是评估标准的总数。

每种产品对应的评估标准与其加权值的总和，除以n得到的是平均值，即信誉得分。

如上所示，Fantom的OPERA链的信誉协议可以不断更新每位参与者的信誉分数，并在必要时将分数调用出来加以利用。信誉得分是0到100之间的实数（四舍五入到小数点后十位），它适用于参与Fantom生态系统的所有方。

信誉分数又可分为A-D四个等级，反映的是不同层次的可靠性。评估标准确认以后，评估分数将根据加权值和重要性计算出的值进行更新。例如，与其值被认为相对较低的标准相比，将以更高的权重来计算被认为是有价值的评估标准。

4.3.5 奖励协议

Fantom的代币经济会用FNATOM代币奖励公正的评估者。激励所有参与者为这个平台做出有价值的努力，从而建立可靠的生态系统。奖励协议将根据交易数量在信誉协议的基础上建立智能合约，并在满足相关条件之后奖励每笔交易。

例如，接下来这个案例就是Fantom的OPERA链奖励协议在食品交付中的应用。OPERA链根据供应商所采用的策略和激励模型来奖励消费者，餐馆以及送货员。

若使用奖励协议的智能合约的相关条件得以满足，收件人将获得代币。奖励可能包括经验值，或优先考虑搜索排名。例如，那些在Fantom生态系统中拥有大量订单和评论的用户，将予以交易代币或经验值奖励。接下来还是以食品交易案例为例，对于那些信誉分数高的餐馆，协议将在用户搜索中提升其曝光率和优先级，以此作为奖励。餐馆可以使用交易代币向应用程序主机支付广告费用。

承接上述案例，按照奖励协议的规定，如果消费者撰写了大量质量高的评论，或拥有大量的订单，亦或是其支出达到了某个阈值，其将按智能奖励协议的规定收到一批交易代币。

5.0 路径图

5.1 里程碑

5.1.1 Intermezzo阶段（~6月15日 ICO）

- 验证Lachesis协议
- 验证Fantom体系结构
- Fantom代币预售
- Fantom代币抢售
- Fantom钱包开发和发行
- 开放中间件测试版
- 开始OPERA Ware Layer Beta网络

5.1.2 Seria阶段（~3Q，2018）

- 打开主要中间件/发布API
- 启动OPERA Ware主网
- 打开OPERA Core Layer beta
- 完成交易处理管理
- 完成Story数据管理
- 完成声誉管理
- 完成激励管理
- 完成付款管理
- 启动餐厅服务应用

5.1.3 Buffa阶段（~1Q，2019）

- 启动主OPERA核心层
- 完成基础架构层开发
- 完成接口层开发
- 完成计算层开发
- 完成控制层开发
- 开放功能语言测试版
- 打开虚拟机测试版
- 打开智能合约生产工具
- 管理智能合约
- 加强安全签名
- 加强客户支持
- 启动Beta网主网的设计策略
- 启动交付服务申请

5.1.4 Operetta阶段（~3Q，2019）

- 开启OPERA链主网
- 完成共识模型和费用模型
- 完成分散网络组合
- 运用投票中心和投票功能
- 打开主要功能语言
- 打开主虚拟机
- 分发智能合约模板并与之互动
- 运用事务处理主网
- 运用Story数据主网
- 运用声誉主网
- 运用奖励主网
- 运用付款主网
- 扩展到食品技术行业
- 扩展到其他行业
- 开放POS应用服务
- 开放商务应用服务

5.1.5 Grand OPERA阶段（~2Q，2020）

- 支持Fantom源代码开发
- 进行全球扩张
- 组建Fantom技术开发委员会
- 组建Fantom研究支持机构
- 提高性能并加强安全性
- 增强系统模型
- 加强可靠性/保证
- 开放物流应用服务
- 开放金融服务应用程序

5.2 Fantom (FTM) 代币分配

目前有31.75亿Fantom（FTM）代币。Fantom平台采用通胀模型来扩展生态系统。Fantom预测，随着越来越多的用户加入网络，最初的年通货膨胀率将会下降5%。总通货膨胀的20%将用于奖励节点，其余的将用于为Fantom平台用户提供奖励，如近乎为零的交易费用，并奖励那些为该生态系统的良好运行做出贡献的用户 good flow of the ecosystem.

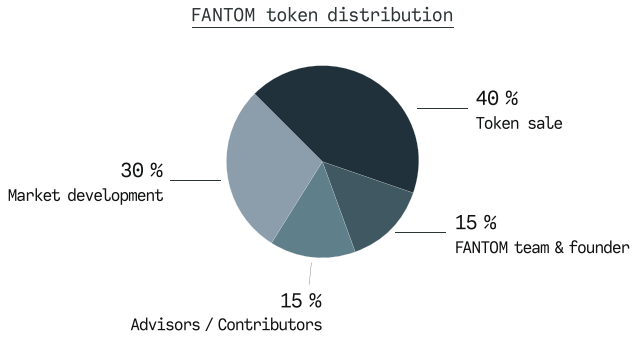
Fantom**代币的分配方式如下**:

- 40%用于销售
- 30%用于市场开发
- 15%用于顾问/贡献者
- 15%用于Fantom团队和创始人

有关代币的法律法规正在不断发展。对于那些居住地时常限制购买代币的公民，居民和个人，代币不予分发。这些地区可能包括中华人民共和国，美利坚合众国或其他司法管辖地区。

与此同时，有关网络基础设施运营商的法律法规也在不断发展。Fantom基金会的运营可能经常会受到许可限制的约束。因此，在确定主机代币发布活动的条件和时间等相关事情时，应考虑到这些限制。

用于推广Fantom生态系统的代币旨在激励新项目，营销活动，招聘新员工以及未来五年的增长。



<图5.2> Fantom**代币的分配**

给Fantom团队和创始人分配的代币具有24个月的特别保护权，这些代币每月发布，给顾问和贡献者分配的代币具有三个月的锁定期。

5.3 Fantom资本的用处

据估计，Fantom的资金将用于以下领域：

- 营销费用：30%
- 运营费用：20%
- 生态系统的研发/开发和应用：50%

营销费用包括以下内容。

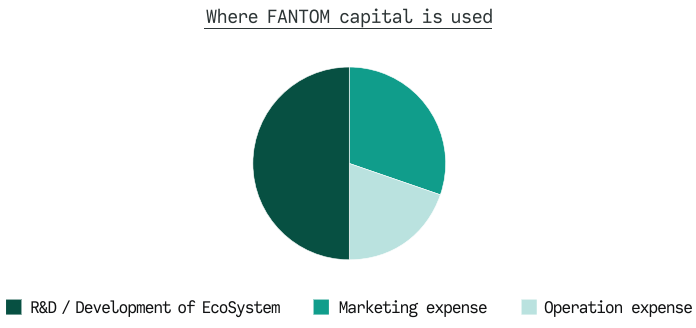
- 获取Fantom服务的直接营销
- Fantom的公关营销
- 通过SNS（例如相关文章和视频）进行Fantom的内容营销
- 社区发展活动

生态系统的研发/开发和应用包括以下内容。

- 销售/运营
- 法律
- 海外扩张
- 应急准备

R&D / Development and application of ecosystem include the following.

- OPERA平台的研发
- 开发和扩展OPERA Ware
- 开发和扩展OPERA钱包



<图5.3> Fantom资本的流向

6.0 团队和合作伙伴

6.1 董事会和团队成员

经过数月的研究和归化，Fantom Pty Ltd（FAN-TOM）于2018年1月正式建立，旨在创建一个全球Fantom生态系统。

<创立成员>

Byung Ik Ahn
CEO
LinkedIn

Joseph Jang
COO / CSO
LinkedIn

Bob Tucker
Treasury
LinkedIn

Fred Pucci
Legal Counsel
LinkedIn

Jake Choi
CMO
LinkedIn

Michael Kong
CIO
LinkedIn

Seung Mun Lee
CFO
LinkedIn

Sung Yun
CBO
LinkedIn

Woong Jae Hyun
Eco Architect
LinkedIn

Yeweon Park
Marketing Director
LinkedIn

Gyumin Kim
Marketing Manager
LinkedIn

Yongwon Seo
Marketing Manager
LinkedIn

Sin Chul Kim
Business Development
LinkedIn

Jung Taek Lee
Business Development
LinkedIn

<평台发展>

Yo Seob Han
Ph.D
LinkedIn
GitHub

Sang Min Choi
Ph.D
LinkedIn
GitHub

Ji Ho Park
Ph.D
LinkedIn
GitHub

Ki Young Jang
Ph.D
LinkedIn
GitHub

Hyun Joon Cheon
Ph.D Candidate
LinkedIn

Choi Hae Lim
Development
LinkedIn

Park Gyo Seok
Development
LinkedIn

Park Jong Chul
Development
LinkedIn

Kim Kang Ho
Development
LinkedIn

Ye Jung Hwa
Development
LinkedIn

Jo Chan Yeul
Development
LinkedIn

Yang Sang Ha
Development
LinkedIn

Lee Eun Jeong
Ph.D Candidate
LinkedIn

Kim Sung Hwan
Development
LinkedIn

Choi Im Chung
Development
LinkedIn

6.2 顾问团队

<顾问>

Steve Bellotti
Executive Advisor
LinkedIn

Matthew Hur
Executive Advisor
LinkedIn

Ashton Hettiarachi
Technical Advisor
LinkedIn

Quan Nguyen
Technical Advisor
LinkedIn

Alex Kampa
Technical Advisor
LinkedIn

Eddy Travia
Advisor
LinkedIn

Ran Neu Ner
Advisor
LinkedIn

Francisco Jo
Advisor
LinkedIn

Issac Lee
Advisor
LinkedIn

Hak Kyoon Kim
Advisor
LinkedIn

Min Sik Jo
Advisor
LinkedIn

Hyeong Joo Kim
Advisor
LinkedIn

6.3 合作伙伴公司

韩国食品技术协会

食品技术（FoodTech）产业是传统食品行业与信息通信技术以改变所有价值链（包括生产，加工，分销和服务）的新产业，也是第四次工业革命的主要领域。未来十年里，食品技术行业在交付，智能农场，数据，食品安全和教育领域预计会创造30万个新的工作岗位。

韩国食品基础产业（FoodTech Industry）是由主要的FoodTech首席执行官，执行工作者，政府，学者和风险投资家联合开发的创业公司和专家协会。

旨在促进食品技术行业的信息共享与人际互动，食品技术行业的市场价值将达200万亿元韩元。这一产业大约有80家公司，企业经营类型多样，包括FoodTech平台，信息服务，交付服务，食品相关基础设施，在线食品配料分销，内容和共享特许经营论坛

甲骨文公司

甲骨文公司总部位于美国加利福尼亚州，就销售额而言，是世界上第二大软件公司。它是一家为企业开发和运营硬件和软件的通用IT公司，在全世界约175个国家拥有约430,000客户公司。其主要产品包括Oracle DBMS，做为一种数据库产品，它在世界市场上所占份额最大。

Quantum Equity Partners

Quantum Equity Partners 作为一家新型风险投资公司，主要投资私募股权。Hak-gyun Kim是韩华公司风险投资部负责人，而且Central Investment Partners作为这家公司的合作伙伴，正引领其发展。核心业务人员包括Neoplux的合伙人Dong-woo Lee和Aju IB Investment的合伙人Tae-suk Choi。Quantum Equity Partners与众多优秀企业一起探索，一起投资，一起成长。


ORACLE

SB CK
SoftBank Group

coinsilium

FoodTech Association
한국푸드테크협회

SikSin

Blockchain
Partners

Quantum
EQUITY PARTNERS

Coinhills

KBIPA
한국블록체인산업진흥협회

SFA
SINGAPORE
FINTECH
ASSOCIATION

6.4 投资公司

Blockwater Capital

Blockwater Capital是一家创于2018年，位于韩国的加密货币基金。Francisco Jo是Coinhills的创始人，Issac Lee是其普通合伙人，Erica Kang是KryptoSeoul的首席执行官，也是一位颇受欢迎的行动派，王万林是Bibox这一全球交易所的联合创始人。

TCM

TCM专注于资产管理和区块链咨询业务。

6.5 法律顾问

KING&WOOD MALLESONS

金杜律师事务所（KWM）作为一家总部设在香港的跨国律师事务所，是第一家也是唯一一家总部设在亚洲的全球律师事务所，是总部设在美国或欧洲以外地区的最大律师事务所。 2015年，它在律师人数和销售额方面排名前30位，是全球第六大律师事务所。