Thor 白皮书

2020 年 8 月主网上线

1， 生存和价值展现是终极的辩论。10 余年时间足以证明以比特币为代表的数字货币完全超越美元和其他法币。

2， 价格是有价值资产发生交易后的表象。无法虚构也不能鼓吹。

3， 市场的纠偏能力超过任何媒体集体唱空和唱多。回归才是价格走向的终点。

4， 有价值的数字资产发行一定有相应的价值存储和展现逻辑，世界上不存在没有逻辑的结果。

目　录

目录取消，建议本文的阅读者从头到尾认真看清每一个文字。

本篇向数字货币的创造者中本聪团队致敬。

同时致敬让我们学习和借鉴的先行者。

他们包括：

Parker lewis

李启威

Vitalik Buterin

Rob Viglione

Roger Zhang

肖风

Saifedean Ammous

Friedrich August von Hayek

Irving Fisher

T

1 项目背景

全球区块链技术发展极为迅猛，全球上线在运行的公链已经超过 150 条，应用场景也极为广泛，但是至今为止，在数字货币价值存储上仍没有超越和近似比特币的数字货币出现。更多的项目都转而倾向于落地应用,使用区块链的激励机制处理原来互联网业务中的存储、通讯、存证等等。雷神（Thor）是为了优化比特币的价值存储和数字资产发行结构而生。

2 货币

“作为一个思想实验，想象一下，某种金属像黄金一样稀缺但具有以下特性：匿名、不是良好的电导体、不是特别强大、没有任何实际的观赏用途.....它是一种神奇的资产：可以通过通信渠道传输 。”

-Satoshi Nakamoto（August 27, 2010）

2.1 数字货币的机制问题

比特币和任何其他类似的货币一样有价值支撑。货币不是人类的集体幻觉抑或是信仰体系。在人类的整个历史进程中，各种各样的交换媒介都曾以货币的形式出现，但每一次出现都不是偶然。所有以货币形式出现的商品都具有区别于其他市场商品的独特属性。《The Bitcoin Standard》一书中对此提出了更广泛的讨论，商品货币的稀缺性、耐用性、便携性、可分割性、可互换性和可验证性等都导致其特别适合用来作为交易媒介。每当一种新兴货币出现时，货币作为交易媒介的固有属性都会在原有货币形式的基础上得到改进,而原有的货币则会被逐渐抛弃,退出流通市场。货币竞争的本质是一种货币的优势胜过另一种货币。比特币也不例外，比特币是全球货币竞争中的产物，它是黄金和由黄金支撑的法定货币体系的优秀继承者。比特币优秀的货币属性超越了其他货币，比特币极其稀缺，比现有的货币更容易分割和交换，同时

比特币也更加去中心化，作为一种衍生特性比特币更抗审查。世界上比特币的总量只有 2100 万枚，每个比特币可以被分割至 1 亿分之一。通过比特币的区块链网络我们可以在未经许可的基础上转账给世界任何人，并且不依赖任何第三方进行结算。

总的来说，比特币的货币属性远远优于今天仍在使用的任何其他货币。比特币不是空中楼阁，比特币之所以具备这些特性并不是偶然。比特币所涌现出来的货币属性是通过多种技术及加密算法的组合而形成的。

比特币通过去中心化的点对点网络执行共识协议来形成一个算力健壮的网络生态，从而能够保证比特币账本的完整性和不可篡改性。比特币与整个区块链体系绑定在一起形成了货币政策的基石，系统创造了完整的经济激励机制，在保证系统安全的同时能够协同整体发挥作用。同时比特币的货币政策不是专制的，而是由市场参与者来决定的。

你要意识到，每当一美元兑换成比特币之后，世界上就有相同价值的美元和比特币同时存在，这个过程中变化的只有人们对于持有哪种货币的偏好。

随着比特币价值的上升，市场参与者会越来越倾向于持有比特币而非美元。更高的比特币价格意味着必须出售更多的美元才能获得等值的比特币。

总的来说**价格是市场对比特币货币属性相对强度的评估结果。货币属性是输入，价格是交易输出。**随着市场不断对比特币的货币属性进行评估，最后的问题自然演变成了：哪种货币更可信？比特币还是美元？我们需要深思如下几个问题：

（1）比特币和美元哪个更加安全；

（2）暴力机关管理下的美元是否会有一天出现政体变更；

（3）美元发行管理机关（美联储）是否有管理机构风险，管理风格是否持续稳健可预期；

（4）你的个人资产是否可以由一个暴力机关改变或者关停。

2.2 到底是什么支撑了美元

首先是什么支撑着美元（欧元或者日元）的价值？每当讨论这个问题的时候，人们最容易迈入的一个误区是美元的价值是由政府、军队或税收支持的，其实这些都不是美元的价值后盾。

美元的价值后盾不是政府，不是军队，也不是税收。政府会对有价值的东西征税，军队保护的是有价值的东西。**政府不能决定其货币的价值，货币的价值只能由货币的供应支配。**

委内瑞拉、阿根廷和土耳其的法定货币在过去五年里都出现了大幅贬值，这些法币背后都有政府、军队和征税权作为支撑。虽然仅仅这些事实还不能够证明结论，但这每一个例子都与货币的价值源于政府的观点相矛盾。

每一次恶性通胀都证明了法定货币体系内部存在缺陷，不幸的是多数人并不把恶性通胀理解为所有法币体系合乎逻辑的终极游戏，而是简单地认为恶性通胀只是货币管理不善的结果。

这种简化的观点忽视了法币系统下货币需要不断贬值的首要原则，虽然美元在当前货币结构下作为全球储备更加强势，但美元也只不过是众多弱势货币中较强的一种而已。

2.3 美元价值何在

美元的价值并不是自由市场定价的，最初美元的价值是和黄金锚定的。从本质上说，**美元是解决黄金可互换性差、可分割性差和不便携等固有属性限制的一种办法。**美元的诞生依赖于贵金属的货币属性，这不是美元的固有属性。

美元最初也是通过建立一个基于黄金固有的信任体系才得以让更多的国家接受美元，因为这些国家相信美元在未来可以兑换回黄金。黄金由于其局限性最终失败，出现了现在的美元货币体系。如果没有黄金，美元就不会存在于目前的货币体系中。

回顾一下美元与黄金的历史：

• 1900 年，《金本位法》规定黄金是唯一可兑换成美元的金属，黄金可兑换为美元，每盎司 20.67 美元；

• 1913 年，美联储成立，作为 1913 年联邦储备法的一部分；

• 1933 年，罗斯福总统通过"6102 号行政命令"禁止囤积黄金，要求公民以每盎司 20.67 美元的价格将黄金兑换成美元,否则将面临最高 1 万美元的罚款和 5 到 10 年的监禁；

• 1934 年，罗斯福总统签署黄金储备法案，使美元贬值约 40%至每盎司黄金 35 美元；

• 1944 年，布雷顿森林协议正式规定外国政府和其中央银行以 35 美元/盎司的价格将黄金兑换成美元（反之亦然）的能力，同时还规定了美元与其他外币之间的固定汇率；

• 1971 年，尼克松总统正式结束了所有美元与黄金的兑换，布雷顿森林体系宣布结束，美元的价值改为每盎司黄金 38 美元；

• 1973 年，美国政府将黄金重新定价为每盎司 42 美元；

• 1976 年，美国政府将美元与黄金脱钩。

在整个 20 世纪，美元从由黄金储备支持的货币过渡到了由债务支持的货币。但大多数人从未停下来考虑过为什么美元在后黄金时代还具有价值。

最常见的解释是，这是一种集体幻觉（即美元价值，因为我们都相信美元有价值）或是背后由政府、军队和税收支撑。这两种解释都没有基本原理可依，也不是美元具有价值的根本原因。实际美元在通过债务维持其价值（相较于美元计价的债务，美元相对稀缺）。在美元的世界里，一切都是以信贷体系作为基础。名义 GDP 依赖于信贷体系的规模和增长速度，税收则是名义 GDP 的衍生品。政府筹集资金的机制：税收和财政赤字都严重依赖于信贷体系，正是信贷体系让美元在当前结构中发挥作用。美国信贷系统有 73 万亿美元的债务，但只有 1.6 万亿美元的现金，因此必须向系统中注入更多的美元来支撑债务。造成了美元的稀缺性，进而维系了美元的价值体系。

现在美元面临着比特币的竞争，美元体系及其固有的货币属性的缺乏与比特币所显示出的货币属性形成了鲜明的对比。美元稀缺是相对的，比特币的稀缺性是绝对的。

美元体系建立在强制信任的基础上而比特币不是。美元的供应由央行决定而比特币的供应由市场参与者的共识决定。美元的供应总是与信贷体系的规模挂钩而比特币的供应则完全脱离了信贷体系。

创造美元的成本几乎为零，而创造比特币的成本是有形的而且还在不断增加。最终比特币的货币属性是自发性的，越来越不可操控，而美元的货币属性是内在的并且越来越可操控

孰优孰劣，可见一斑。

2.4 是什么支撑了比特币

比特币具有黄金一样的货币属性，同时它也完善了黄金的缺陷。虽然黄金相对稀缺，但比特币更加稀缺，比特币和黄金都极其耐用。

黄金可以进行分割和互换，但是鉴定难度特别大，比特币可以分割和互换且易于鉴定。黄金很难转移，而且存储高度集中。比特币易于转移，且高度分散。

从本质上讲比特币拥有实物黄金和数字美元合二为一的所有可取特征，并且没有两者所存在的关键缺陷。在评估媒介货币时，首要是遵循基本原则即忽略过往的结论来做基础的考量。

如果忽略比特币是数字化的，从比特币的固定供应和稀缺性来讲，比特币是否能成为一种有效的价值衡量手段并最终成为一种价值储存手段呢？我们认为，无论这种稀缺的形式是否是数字化的，稀缺都是一种足以让比特币成为货币的强大属性。

虽然货币可能是一个无形的概念，但只要有贸易和交易，货币就能产生真正的需求和效用。货币是度量消费品和资产相对价值的工具，稀缺性是货币最重要的属性。

如果货币的供应量在不断地、不可预测地变化，那么就很难用货币来衡量商品相对的价值，这就是为什么稀缺性本身是一种非常宝贵的财产。

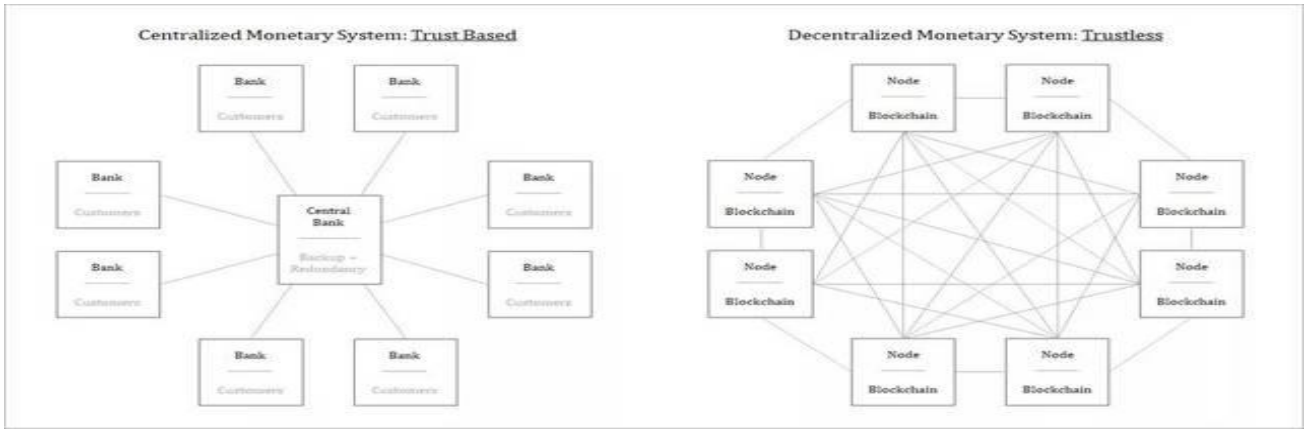
当然，仅仅因为比特币的有限、稀缺特性还是不够的，我们不应该简单地接受这一事实。重要的是，我们要理解这种情况是如何发生的以及为什么会发生？为什么不能创造超过2100万比特币，为什么不能复制比特币？为什么比特币是安全的，为什么它不能被操纵？

虽然比特币区块链网络已经产生了无数的区块，但让比特币能够以可靠的固定供应方式运行。是基于比特币网络中有三个关键的支柱，他们互相促进互相影响，并因比特币本身的经济激励而不断强化。这三个支柱分别是：

（1）网络共识和全节点：执行通用的治理规则集；

（2）挖矿和工作量证明：验证交易历史，在物理世界中确保比特币网络的安全；

（3）私钥：保证资产安全，确保资产所有权独立于验证权



同时，比特币网络中矿工是最为核心的价值主体：

（1）矿工是唯一的数字货币发行组织

比特币链上的每一个矿工节点都是比特币作为货币的发行机关的组成部分。矿工体系高度离散，自由进出，没有统一指挥也没有统一的行动纲领。完全在比特币发行方法的共识机制下生存和博弈。

（2）比特币发行过程中的价值锚定

矿工在发行比特币的过程中对比特币进行了有效的价值锚定。全球所有矿机的能源消耗被量化为定量的比特币数量发行。假设全球有 1000 万台比特币矿机在链上运行。那么相当于 1000 万台矿机十分钟的能耗被表征为 6.25 个比特币增发出来。所以早期伴随着价值锚定效率的提高（半衰期和算力增加）。比特币发行过程中的价值锚定会提高。比特币会提高自己的价值，进而表现为价格的上涨。矿工在自愿选择加入货币体系的前提下，一个由理性的经济行动者组成的全球去中心化网络，不会存在以集体或是压倒性的方式形成的一种共识，他们各自独立、自愿决定是否将用来储存财富的货币贬值。共识机制支撑和强化了比特币的经济激励、技术架构和网络效应。

（3）比特币价值表现为具体交易价格

比特币的矿工群体会自发自由的依据自己的能耗和发行效率，协调比特币的交易价格。当比特币交易价格下跌时，越向发行成本靠近，矿工购买比特币的欲望越强烈，导致买盘上升，比特币的交易价格会提高到正常水平。

这一切的发生都是自主和自发的。任何大算力矿工和意见领袖起到的作用都微乎其微。比特币矿工也是一个去中心化的数字货币发行主体，当交易价格发生变化时，当数字货币的价值存储效率和发行效率出现变化时，会自发行动自主决策。但是一定会形成共识决策，大多数人做一个动作，就会形成强烈的价值维系体系。这种自然形成的体系是极为健康的。不会受到强人指令的影响和破坏。对作弊和作恶具备有效的抵抗能力。


Full nodes:
Enforce consensus rules
Private keys:
Secure ownership of network
Miners:
Order & Clear Transactions
More Miners
More Secure
More Confidence
More Users
Higher Price
CUMULATIVE BTC IN CIRCULATION
Now
Date (approximate)

3 Thor（雷神）

“当比特币还没有在市场上确立价格之前，基于生产成本的估值模型是有意义的，任何商品的价格都趋向于生产成本。但是在几年以后，当新挖出来的比特币只占供应量很小一部分的时候，将会是比特币的价格决定生产成本，而不是反过来。但在未来，市场力量将是决定比特币价格的主要因素。” ----- Satoshi Nakamoto（bitcointalk）

3.1 缺陷弥补

比特币的价值存储和货币发行逻辑可以简单的理解为正向价值存储，线性发行。每隔21万块区块高度，价值存储效率会瞬时提高一倍。在前几个半衰期内，正向存储线性发行的数字货币优势极为明显，交易价格会伴随着发行成本（能源的价值存储效率）的提高而提高。但是当未发行量过少的周期来临的时候，比特币的价值存储效率更倾向于接近交易价格，矿工群体将变得极为脆弱和不可控？交易力量和发行力量会发生反转。

（1）比特币无法完成长周期的价值提升。

当比特币经历4个半衰期后，比特币已发行货币量达到总量的93.75%。流通量将达到1968.75万枚。此时市场交易价格将会反过来影响矿工成本，算力会被市场交易价格左右，当矿工获利丰厚的时候，矿工算力会提高。当矿工获利减弱时，算力会溢出到其他网络。因为未发行货币量过低，会导致矿工群体脆弱。

（2）一个半衰期的周期内，币价波动明显。

比特币在一个半衰期的周期内，由于发行锚定的存储效率无明确明显变化，会导致矿工共识减弱，对交易价格体系无明确方向性指导，会导致币价宽幅波动。由于比特币占整个数字货币总市值比例较高，由此引发熊市行情，引发其他币种出现系统性危机。

（3）基于比特币网络的分叉较多。

现有比特币的分叉网络和低优化区块链网络已经达到甚至超过40个链。矿工一直在各个

链上游离。对各个链形成算力闪击。另外因为矿机厂商的 Asic 芯片算力侵入，导致矿工长期需要更新矿机。导致比特币价值外溢较为严重，无法弥合。

（4）比特币网络交易性能低下

比特币区块链设计时将一个区块的容量设置为 1MB，而后期随着比特币发行量的增加和相关应用类型的增多，比特币区块链网络开始逐渐达到 1MB 的上限，交易大量堆积，经常被迫推迟，扩容成为迫切的需求。比特币每秒处理交易笔数的峰值一般小于 7。由于比特币交易的一次确认时间平均大约是 10 分钟，这也是一个区块的生成时间，6 次确认的情况下，需要等待约 1 小时。与传统的支付系统每秒钟上千笔的交易数相比较，这样的性能是非常低下的。

（5）算力入侵

在形成相同算力的网络里，使用 ASIC 矿机显然要更低成本、更环保，相对于显卡矿机优势非常明显。但 ASIC 挖矿往往带来的是整个网络算力指数级别增长，支撑网络所消耗的能源和制造成本也会比显卡矿机更多。

比特币的 Pow 算力引发了矿机厂商的芯片产业的无序竞争。Asic 芯片成为矿工的主流芯片，这也就导致了比特币网络的矿工价值外溢给矿机厂商，严重影响了比特币本身的价值存储效率和价格管控能力。

3.2 系统概述

尽管区块链技术有一定的瑕疵(Eyal 2015, Eyal and Sirer 2013, Nayak et al. 2016)(AZURE 2016, CACHIN 2016, ROSS and SEWELL 2015)，但区块链技术(Garay, Kiayias, and Leonardos 2015, Nakamoto 2008)(2016)作为创造信任的机器，具有分布式结构、建立信任、公开透明和时序不可篡改等技术优势，吸引了金融界和工业

界的广泛关注，并开始被用于重塑交易系统，在降低交易成本和提高交易效率方面效果显著。

Thor 是一个高性能高效率底层基础区块链。通过使用可信芯片作为共识的保证机制，解决了传统区块链对能源的大量浪费和消耗，并且具有纠缠算法智能合约的高性能处理能力，能极大的提高区块链的处理速度和交易吞吐量，从而构建一个全新的区块链生态环境。

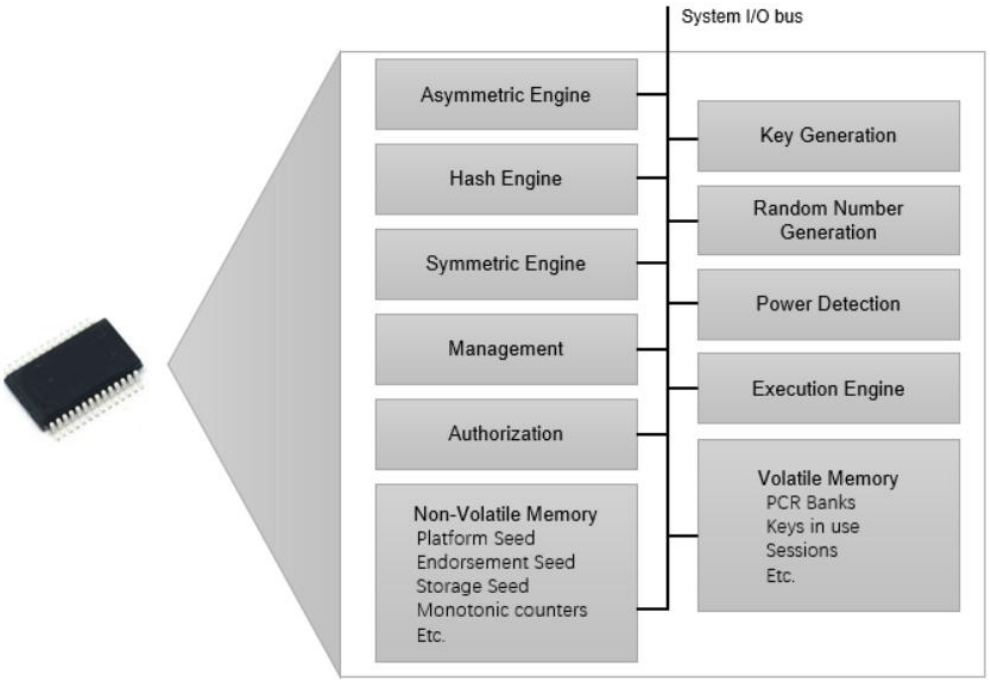
Thor 的出块方式跟其他区块链有根本性不同，它无需耗费大量能源，可信计算芯片的引入会屏蔽掉巨大的 Asic 算力入侵。通过 PoW 证明来达成出块共识，具有高效、节能、安全的特点。

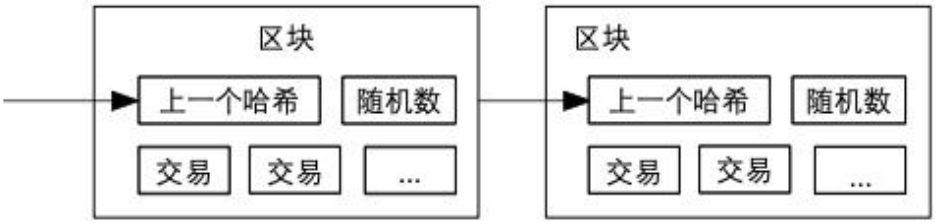
同时，Thor 基础链具有很高的安全等级，保证数据的安全和用户的隐私。使用基于硬件安全模块支持下的可信计算系统将用户的私钥完全保护在可信计算的芯片内，它永远不会以明文的方式出现在系统的任何位置。

可信计算是由可信计算组织 TCG 提出的一套开放的、系统的规范，在平台完整性检查、数字版权管理、磁盘加密、物联网数据保护和关键应用验证等多种场合得到广泛应用。可信计算模块集成了一组加密算法和加密密钥，为平台提供了签名数据和加密敏感信息的工具，可以通过隔离特殊的运行模式并对内存进行分区来创建受保护的执行环境，使可信计算所使用的内存永不被其他进程和处理器访问。

矿机上内置的安全芯片，用以实现矿机的身份识别。在每次出块时矿机的安全芯片都用内部的私钥对区块的哈希进行数字签名，并把签名提交到区块中一起发送给所有节点。这个签名包含了矿机的公钥，用来作为矿机的身份识别，而公钥不可伪造，所以矿机的身份也是不可伪造的。

区块链中的其他节点通过验证区块签名的方式，获得矿机的身份识别信息，并通过判断这个身份来决定是否接收这个区块，只有许可身份的矿机发出的区块才被接受。所以传统的区块链矿机由于没有安全芯片，是无法直接在雷神区块链上使用的。





3.3 Thor 与 Odin 的纠缠机制

1. Thor 在出块的同时和 Odin 网络进行合约交互。通过可信计算芯片的签名来验证出块是否合法，分别验证抵押的 Odin 网络中的 PoC 算力值、和预留燃料费（gas）。其中任何一条不能满足，即被判定为非法区块。

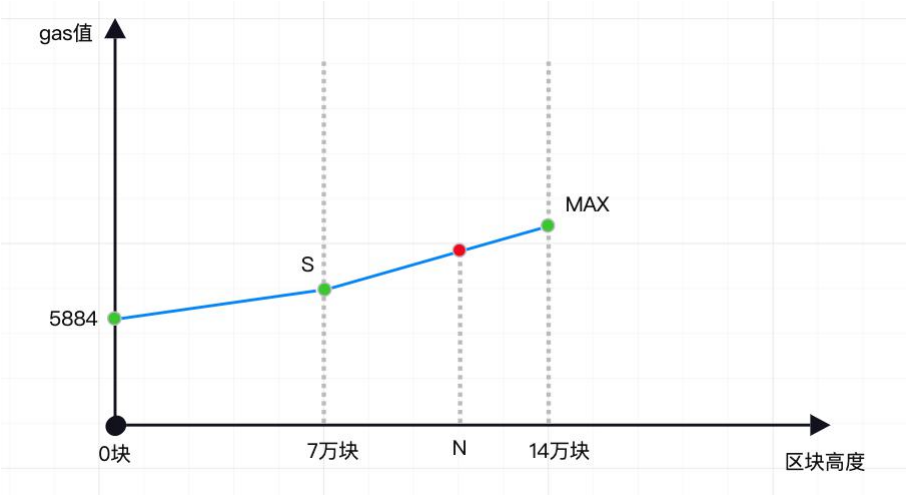
2. 当 Thor 的出块判定为合法后，Thor 的奖励归属给获得出块权的矿机。并且执行 Odin 网络中的黑洞合约。将用于 gas 的 Odin 全额销毁。
3. 矿机验证的 PoC 抵押值，每逢 14 万个区块高度减半一次。起始抵押锚定为 10 万单位 PoC。单个可信芯片矿机仅能抵押一次 PoC 算力。
4. Thor 为每隔 5 分钟出块一次，出块消耗的 gas 起始值为 5884，gas 的起始值每隔区块高度 7 万块调整一次。每个 7 万块消耗的 gas 总量为（Odin 的流通总量*20%）+（odin 日产量*243）。7 万块周期内出块消耗 gas 值线性上涨。

   举例：当前块数为 N；上次结束每个 7 万块的起点 gas 值为 S（如果 N<7 万 则 S=5884）；

   当前 7w 块内对应的 gas 平均值 == (Odin 的流通总量*0.2+odin 日产量 *243)/70000；

   当前 7w 块内对应的 gas 最大值 MAX（第 N*7 万块）== (Odin 的流通总量*0.2+odin 日产量*243)/70000*2-S

   则 第 N 块的 gas 值为： S+(（MAX-S）/6999)*(N-1)



5. Thor 的激励每隔 21 万个区块减半一次，初始激励为 50 个 Thor。每逢 210000 块的整数倍激励减半。
6. 同时，Thor 致力于 Thor 网络的全记账节点更为安全自由，所有预计于 2021 年 10 月前发射一颗使用太赫兹通讯的全记账节点卫星抵达太空。Thor 挖矿节点通过下载整条 Thor 链来进行同步，从创世纪块到当前块，执行其中包含的所有交易。通常，Thor 挖矿节点会存储 Thor 链的全部信息，因为他们在挖矿过程（记账过程）中需要链上的所有信息，也有可能下载一个全节点而不用执行所有的交易。无论如何，一个 Thor 挖矿节点包含了整个 Thor 链。
7. Thor 和 ODIN 的纠缠是通过跨接桥实现的。Thor 链的超级节点上部署并连接了原生的跨接桥，每次 Thor 的出块校验都会通过跨接桥连接到 ODIN 链上查询矿工在 ODIN 链上的抵押情况，只有满足了抵押要求的矿工才能允许被出块。当 Thor 矿工挖出的区块在链上经过 8 个确认之后，超级节点通过跨接桥扣除矿工的抵押，作为 gas 被燃烧掉。

3.4 Thor 挖矿节点

Thor 挖矿节点是构建在可信芯片 SGX/ TPM CPU 之上，该芯片封装了可信的程序块 Enclave，用于构建芯片级共识，保证数据一致性和安全性。可以把 Enclave 理解成可信芯片中的一块“飞地”，它在芯片生产完成后就已被内置到芯片之中，并且不可篡改。为了调用可信芯片中的 Enclave，实现芯片级共识算法，操作系统层需安装 SGX/TPM-Compliant

Progams（即：Enclave 的驱动程序），用于解析来自 Thor 区块链代理程序的信息，并携带未验证的有用贡献和当前区块的难度等信息发送给 Enclave 验证。

为保证 Thor 挖矿节点的权益，保证其能够公平的参与记账权的分配、公平参与区块的产生，所有 Thor 节点产生的有用贡献与 Enclave 产生的随机数一起广播到网络中。Thor 挖矿节点捕获有用贡献的信息后，将根据矿机给的随机数，解析后来判断是否由自己来计算贡献度值。用 RandNum(Useful contribution)表示 Thor 产生的随机数形式如下：

Thor 挖矿节点地址 = hash(RandNum)

只有当随机数的 hash 运算结果与 Thor 挖矿节点地址相同时，有用信息才有自己统计。

同时，为了让贡献度影响节点的挖矿能力，在工作量证明的同时，引入贡献参数。假设用 D(Difficult)表示当前挖矿难度，用 UCs(Useful contributions)表示挖矿节点统计的有用贡献总和。当且仅当当前挖矿节点的 UCs 高于 a%的系统中的其他挖矿节点，将有资格通过 Enclave 的 PoUC 进行工作量证明，即：

ThorProof(UCs, D, hash, a%)

与 PoW 相同，当且仅当其解 hash 值的速度最快，将会获取创建新块、记账的权力。

4 主要技术

4.1 自组织组网

Thor 链是区块链的外延，具有区块链所有的特性，如去中心化 、不可篡改、可信、安全、稳定、透明等。为了满足这些特性，Thor 链系统节点应该具备分布式（分散化/去中心化）、自治性、开放可自由进出等特点。很明显，传统的基于中心服务器的网络拓扑结构或组网方式无法满足 Thor 链系统的要求。比较而言，对等网络 (Peer-to-peer network, P2P) (Qin 2002) (袁勇 and 王飞跃 2016)（如图 5.1） 具有分散化、可扩展性、健壮性、隐私性和高性能等特点（如表 4.1 所示）。

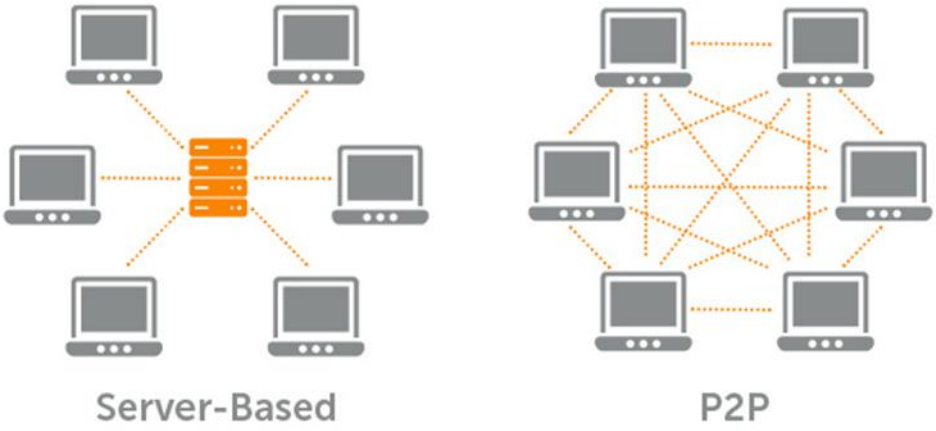


图 4.1 典型的网络拓扑结构

考虑由 k 个 Thor 节点（Z1，Z2，… ， Zk）组成的 Thor 链系统拓扑机构，如上图 4.1 所示。将上图网络中的 Thor 链节点抽象为带权无向图 G=（V，E）。其中，V={ Z1，Z2，… Zi，…，Zk}为顶点集，顶点 Zi 表示 Thor 链节点，k 为 Thor 链节点的个数；E={eZ1，Z2，…，eZi，Zj，…，eZk-1，Zk}为边集，边 eZi，Zj 表示 Thor 链节点 Zi 和 Zj 之间的通

信链路。边上的权重 τ Zi，Zj 表示 Thor 链节点{Zi， Zj}之间的通信时延。该无向图如图 4.2 所示。

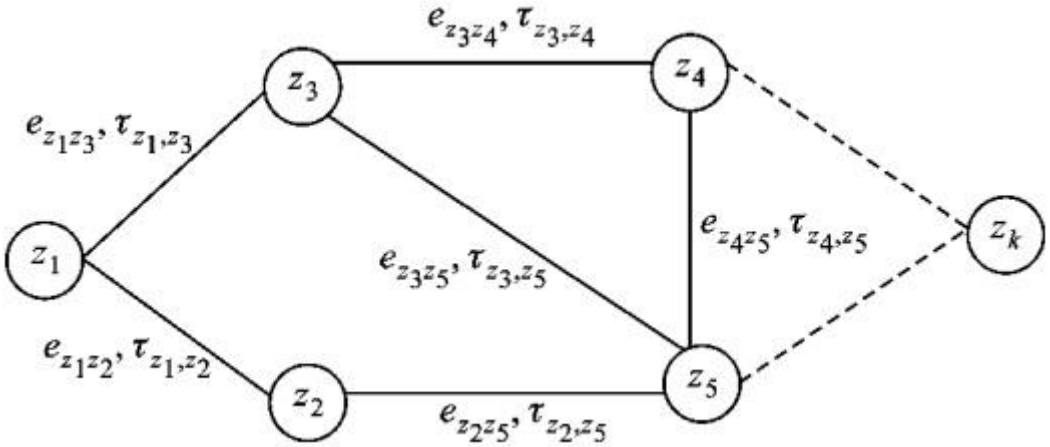


图 4.2 Thor 链的节点之间消息传输示意图

图 4.2 每个 Thor 链节点Z_i的计算能力假设为V_{z_i}。任务执行过程中，用户每次将计算存储任务 D 提交到其连接的 Thor 链节点Z_i，Z_j将存储任务 D 划分为满足$d_i = \delta_i D$的若干子任务，并分配包括自己在内的计算节点进行计算。因此，整个计算存储任务 D 在边缘计算 Odin 链网络中处理的总时间 t 可以表示为

$$t(\delta_i) = \max\left\{\frac{\delta_i D}{\upsilon_{z_i}} + \tau_{z_i,z_j} m_{z_i,z_j}\right\}$$

式中：$\delta_i D / \upsilon_{z_i}$表示 Thor 链节点$Z_i$处理子任务$d_i$的时间；$\tau_{z_i,z_j} m_{z_i,z_j}$表示$\{Z_i,Z_j\}$之间的通信开销，其中$m_{z_i,z_j}$表示$\{Z_i,Z_j\}$之间是否存在子任务分配关系，$m_{z_i,z_j} = 1$表示存在子任务分配关系，$m_{z_i,z_j} = 0$表示不存在子任务分配关系。

由于分布式计算总任务的处理时间等于所有子任务中最大的计算延时，因此为了达到处理时延最小的目标，必须求一组最优的δ_i，使得目标函数 t 最小。综上所述，整个过程可以建模如下：

$$\min\left\{\max\left[\frac{\delta_i D}{\cup_{z_i}}+\tau_{z_i,z_j}m_{z_i,z_j}\right]\right\},\quad i,j=1,2,\cdots,k$$

$$s.t.\ \ m_{z_i,z_j}=\begin{cases}1, & \delta_i\neq 0\\ 0, & \delta_i=0\end{cases},\ \sum_{i=1}^{k}\delta_i=1$$

因此每个 Thor 链节点上应处理的子计算任务为$d_i=\delta_i D$，则 k 个 Thor 链节点上分别处理的计算子任务可构成一个 k 维向量 $d=[d_1,d_2,\cdots,d_k]^T$。考虑到具体情况，计算任务 D 可能来自任意一个节点，假设来自节点Z_1，由上述公式可知，在边缘计算 Thor 链网络中处理计算任务 D 的总时间 t 可以表示为

$$t(d)=\max\left\{\frac{d_1}{\cup_{z_1}}+\tau_{z_1,z_1}m_{z_1,z_1},\cdots,\frac{d_k}{\cup_{z_k}}+\tau_{z_1,z_k}m_{z_1,z_k}\right\}$$

因此，对 Thor 链网络中每个计算节点上应处理的计算任务d_i的求解，即对任务向量 d 的求解，可归结为如下优化问题

$$d=\arg\min_{d\in 1}\{t(d)\}$$

$$s.t.\ d_i\geqslant 0,\ \sum_{i=1}^{k}d_i=D$$

上述优化问题的搜索空间 I 为

$$I\triangleq\prod_{i=1}^{k}[D_{imin},D_{imax}]=\prod_{i=1}^{k}[0,D]$$

对于上述优化问题的求解，目前有很多算法可以参考，例如带约束的粒子群优化负载均衡算法(Venter and Sobieszczanskisobieski 2002, Coello, Pulido, and Lechuga 2007)。

4.2 Proof of Honest(诚实证明)

我们通过在 SGX/TPM 芯片中开辟一个独立安全的程序运行空间——Enclave，把工作量证明的算法、身份认证的密钥，统一封装在该 Enclave 中。创世纪块的产生、记账节点选举和区块验证过程由 Enclave 中的工作量证明和密钥来维护。当 Enclave 中的程序和密钥被

修改时，将破坏硬件和软件的完整性，新区块的参数将与旧区块中 keyRoot 保存的参数不一致，从而不能证明该节点是诚实节点，其创建的新块将不能验证通过，因此我们把该算法称为 Proof of Honest(诚实证明，PoH)。

4.2.1 可信节点双重认证

Thor 链中的记账节点必须是建立在 SGX/TPM 芯片之上的计算机，且在 enclave 中预装 Odin 链的系统密钥 Thor system key (简称 sysKey)，该 key 是系统的唯一标识，它预装在芯片之中，一旦芯片硬件或软件被改写，sysKey 将销毁。

Enclave 中会包含自己私有的 Thor node key(简称 nodeKey) 该 key 是 Thor 记账节点的唯一标识。同理，nodeKey 也预装在芯片之中，一旦芯片硬件或软件被改写，nodeKey 将销毁。

4.2.2 创世纪区块和新矿工

Thor 链的创世区块由 Thor 矿工挖矿产生，当第一位矿工在系统中未发现其他节点存在时，将触发 enclave 中内置的程序，该程序将创建包含 Enclave 系统密钥 sysKey 和自身密钥的区。一旦创世纪区块产生，区块链的 sysKey 将永久存储在区块链的块头中，记为 Block sysKey。

当第二个 Thor 节点和第三个 Thor 节点到来时，其它节点提供的 sysKey (记为: Thor sysKey)必须和创世块中的 sysKey 一致且参数完整，它将成为 Thor 链中的矿工。即：

Block sysKey = hash(Thor sysKey)

当节点的 Thor sysKey 的 hash 散列必须与 Block sysKey 相等，这时才能加入到区块链中。同时，节点还必须要上报自己的 nodeKey，并记录到区块链系统中。

4.3 SGX/TPM 安全硬件基础

SGX 全称 Intel Software Guard Extensions，顾名思义，其是对因特尔体系（IA）的一个扩展，用于增强软件的安全性。这种方式并不是识别和隔离平台上的所有恶意软件，而是将合法软件的安全操作封装在一个 enclave 中，保护其不受恶意软件的攻击，特权或者非特权的软件都无法访问 enclave，也就是说，一旦软件和数据位于 enclave 中，即便操作系统或者和 VMM（Hypervisor）也无法影响 enclave 里面的代码和数据。Enclave 的安全边界只包含 CPU 和它自身。SGX 创建的 enclave 也可以理解为一个可信执行环境 TEE（Trusted Execution Environment）。不过其与 ARM TrustZone（TZ）还是有一点小区别的，TZ 中通过 CPU 划分为两个隔离环境（安全世界和正常世界），两者之间通过 SMC 指令通信；而 SGX 中一个 CPU 可以运行多个安全 enclaves，并发执行亦可。当然，在 TZ 的安全世界内部实现多个相互隔离的安全服务亦可达到同样的效果。

受信任的平台模块 (TPM) 技术旨在提供基于硬件安全相关的功能。TPM 芯片是安全加密处理器，旨在执行加密操作。该芯片包含多个物理安全机制以使其防篡改，并且恶意软件无法篡改 TPM 的安全功能。

整个启动序列中都遵循“先度量，再执行”的原则，当前阶段的代码负责度量下一阶段即将要执行的代码，然后再将度量值扩展到 PCR 寄存器中，这样循环往复，这就构成了信任链。

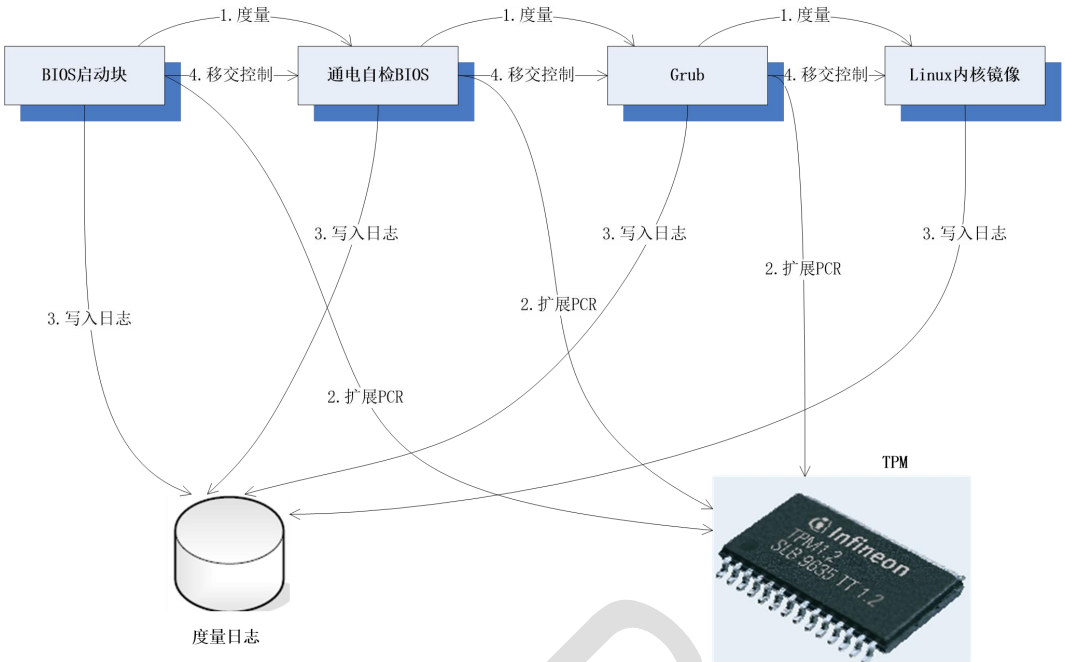


图 4.9 信任链与完整性度量过程

5 Thor 链经济模型

5.1 Thor Token 价值基础

Thor Token 是 Odin 链上的原生资产，Thor Token 的价值起源是其能够方便的表征和度量 Thor 链上的数字化经济活动。Thor Token 代表 Thor 链的所有权又代表使用权。

5.2 激励机制

Thor 网络包含其内建的 Thor Token,在网络内包含一种 Thor Token 的原因是多重的。首先,Thor Token 被奖励给矿工以促进网络安全；其次，用它来支付 Gas 费用，这也是是一种反欺诈机制。

由于独特的发行机制和价值存储机制，Thor 的节点矿工对 Thor token 的价值存储效率每 5 分钟提高一次。以此来锚定 Thor 更好的经济价值。形成更为广泛的价值强共识。

5.3 挖矿难度

每个周期 Thor 系统自动设定一个贡献度阈值，工作量超过阈值的节点获得记账授权。为了使每个周期获得记账授权的节点比例维持在一定水平上，系统将根据上个周期拥有记账授权的节点比例来调整当前周期的工作量阈值。定义工作量阈值为挖矿难度。

Thor 的区块平均每 5 分钟生成一个，这是 Thor Token 发行速率和交易确认速度的基础。不仅是在短期内,而是在几十年内它都必须要保持恒定。在此期间,计算机性能将飞速提升。此外,参与挖矿的人和计算机也会不断变化。为了能让新区块的保持 t 分钟一个的产生速率,挖矿的难度必须根据这些变化进行调整。事实上,难度是一个动态的参数,会定期调整以达到每 5 分钟一个新区块的目标。简单地说,无论挖矿能力如何,新区块产生速率都保持在 5 分钟一个。