BaseChain Whitepaper(Draft)

1. 背景

1.1 围绕比特币和以太坊的区块链世界

不管全世界所有致力于推动区块链技术发展的人们如何宣称——区块链不等于投机，但是大众的认知总是绕不开交易、投机、ICO等词语和概念。理所当然，不管我们如何否认，现在的区块链世界，确实是围绕着比特币和以太坊所发展的基础来运转的。

最初区块链技术事实上要解决的问题并不新鲜，去中心化的概念也不是从比特币之后才产生的。在1985年莱斯利·兰伯特(Leslie Lamport)等人提出拜占庭将军问题(Byzantine Generals Problem)之后，人们进行了大量的研究，这也是分布式系统需要首先解决的问题，即如何在各节点之间产生最终数据一致性。

在1998年，戴伟(Wei Dai)首次提出了通过计算难题来达成共识的匿名分布式的数字货币系统B-money，然而，这个被认为是比特币系统前身的数字货币系统也仅仅是被提出，并没有着手实现，更别提真实应用了。B-money面临的一个最大问题是系统内各节点需要对计算难度达成一致，然而各节点都可以通过隐瞒自己的计算能力来达到优势。

自从1977年RSA算法发明开始，密码学领域的爆发性研究为比特币的产生打下了理论基础。而1999年在肖恩·范宁(Shawn Fanning)与肖恩·帕克(Shaun Parker)的努力下一手打造的Napster则证明了P2P网络的现实可能性。至此，比特币系统产生的一切前提都已具备，只剩下“双花问题”这一难题——因为数据的可复制性，由于错误操作，一笔数字货币可以被多次支付——此后的好几年，不断有人尝试在去中心化数字货币系统中解决这个问题，然而并没有获得大的突破。

事实上回过头来看，这个问题的解决方案近在眼前——1997年亚当·拜克(Adam Back)所发明的哈希现金(Hashcash)算法机制。只是这个机制最初用于解决垃圾邮件的问题，所以并没有人注意到它的可贵。而哈尔·芬尼(Hal Finney)在之后对哈希现金算法进行了改进，终于提出了“可重复的工作量证明”（Reusable Proofs of Work, RPoW）机制。

直到2008年，中本聪将非对称加密、P2P网络以及基于哈希现金产生的RPoW机制结合在一起，他在比特币系统的论文中阐述了如何通过RPoW来解决拜占庭将军问题。然而仅仅如此，这又一篇更加优秀的“哈希现金”，但是中本聪不仅是个密码学大师，他还是个编程高手，他实现了最初的比特币系统，并成功运行了起来，产生了第一个区块，直到现在。

后来，维塔利克·巴特林(Vitalik Buterin)在2013年末提出了以太坊项目。将区块链世界推向了一个新的高度。以太坊采用“智能合约”的方式解决了数字货币个性化和扩展的问题，这导致从2016年初开始基于以太坊ERC20规范产生的各种代币呈井喷式增长。

可以说中本聪创造的比特币打开了人们对数字货币的心智，用事实证明了去中心化数字货币系统的可行性，而以太坊项目则证明了数字货币具备承担复杂业务的能力，使得各类区块链商业落地成为了可能。

1.2 公链技术与商业应用的现状

比特币系统的成功在于，之前的所有类似系统在面对拜占庭容错（Byzantine failures）问题时只能达到类似对于已知身份的N个结点可以容忍N/4的错误这样的结果。他们无法抵抗女巫攻击，即在匿名用户的情况下，女巫们可以通过僵尸网络等手段很轻松地获得N/4的结点控制权。而比特币通过引入工作量证明（Proofs of Work, PoW）使得女巫们获得全网大部分算力的难度比创建全网大部分结点难的多。

可以说从比特币系统中提炼出来的区块链技术，并不是突然出现的，它经过了长足的技术沉淀，才由中本聪整合出一套可行的去中心化方案。尽管这套系统看起来十分粗糙简陋，但是事实证明他已经足够好了。

一个问题是，人们发现比特币系统过于纯粹导致它难以满足丰富多彩的商业世界需求。而最干脆的做法是新做一条区块链。从2008年开始，至少有上百个公链和代币项目直接参考了比特币系统的代码进行开发并发行。

另一种比较简单的方式是以万事达币（Mastercoin）和合约币（Counterparty）为代表的使用元币（metacoin）协议来对比特币系统进行扩展。采用原始链的体系，通过引入一个可信任的结点来提供元数据，并实现更加复杂的业务逻辑。然而，在一个去信任的体系里引入可信结点这种做法无疑十分让人难以接受。

有趣的是，比特币的开发者可能是预见到了这种情况，他们为比特币设计了脚本系统，使得比特币这一最初的区块链实现到现在仍然不见得过时。开发者可以通过脚本来处理特定的UTXO，使得完成一些简单业务逻辑。

然而通过脚本来扩展比特币系统存在很多麻烦，最主要的是不支持循环——这主要是比特币的开发者们担心错误的脚本将使得交易进入死循环。针对这个麻烦，以太坊在智能合约中引入了Gas，合约每执行一步操作都将消耗一定的Gas，即使合约本身代码存在死循环的可能，至少实际执行中不至于真的产生死循环的情况。

以太坊通过实现一个图灵完备的以太坊虚拟机来运行智能合约，从而使得业务逻辑能力大大提升。以太猫等应用的产生足以证明通过智能合约来增加区块链的业务能力是具备可行性的。

以比特币和以太坊为代表的系统的另一个问题是，PoW共识机制为了保证去中心化，牺牲了大量算力和性能，这不仅给了矿工们极大的权力，也使得区块链技术被环保主义者所诟病。以太坊的核心开发者们已经开始尝试推进将以太坊转移到权益证明（Proof of Stake，PoS）的大框架下的进程，试图通过使用这种共识来降低资源浪费并提升性能，但是一定程度上牺牲了去中心化的特征。

开发者们在区块链技术上不断推陈出新，项目方则结合自身实际业务，缓缓推进区块链的落地进程。

1.3 ICO成本扭曲带来的悖论

ICO（Initial Coin Offering）提供了一种新型的且更加轻量匿名的融资方式。催生了许多优质的区块链项目。然而同样出现了金融诈骗的风险，因此世界各地政府官方对于ICO的态度也多半谨慎甚至反对。

对于一个传统的一般体量、功能单纯的互联网创业项目，项目团队也许只需要50万美金的启动资金和三个月的前期开发和运营工作即可上线。而现在的大多数ICO项目，则很有可能动辄需要募集超过10000以太坊（当前约等于600万美金）的资金，却需要超过1年的研发周期。

这里产生了两个悖论：

1. 投资者直观地认为募资越多的项目，越具有投资价值，即便事实是项目本身根本不需要如此大量的资金。
2. 多数ICO项目并不以项目本身的成功来盈利，却以抬升币价来盈利，这也是为何多数项目将研发和上线周期延长的缘故。

1.4 商业尝试和公链项目的价值

对于一个创业项目来说，项目方需要在募得资金后承担项目失败的风险，而ICO的现状导致了许多项目方不得已承担了大资金的风险，因此，在项目募资前进行商业的可行性验证是很有必要的。一方面对于项目方来说，提前验证一部分可行性可以大大规避项目失败的风险，甚至可以对项目成果、预算以及时间排期做一个提前评估。另一方面，对于投资者来说，项目方出具的可行性报告是一个左右投资的重要指标。

然而，当前的区块链项目，尤其是公链或者发布在公链上的项目，其本身的可行性多半停留在一纸白皮书上，这不仅仅是因为ICO导致的项目鱼龙混杂，更是区块链本身特质导致的——一个去中心化的项目，在一个实验室环境中，难以模拟接近真实的业务场景。在当下，任何区块链创新项目都是应当被鼓励的，无法奢望任何一个区块链项目方都能出具模拟数据，但是商业尝试的价值就提现于此——它能使各方都少走弯路。

另一方面，以以太坊智能合约为代表的合约类项目都强烈依赖于平台本身的机制和能力，甚至很多项目都只是使用智能合约发布代币。

以太坊虚拟机实现了图灵完备却增加了安全风险，以太坊网络自从出现到现在不止一次被发现存在漏洞，能力不足的智能合约开发者可能会编写出漏洞百出的合约，从而影响整个智能合约项目的质量。

而即使不出现漏洞，火爆热门的应用会拖垮整个网络的执行性能，以太猫在出现之时受到了大量追捧，一时间以太坊网络拥堵无比。热门的ICO项目在进行限时ICO时，也可能会造成网络的拥堵。

即便并不是所有业务，都需要自己搭建一条公链，因为智能合约项目仍然是很多项目的首选：事实已经证明，一味的关注去中心化并不是一个好的做法，借助区块链完成去中心化部分逻辑，另外的部分可以由项目方中心化处理。但是越来越多的项目方，开始选择自己开发属于自己的公链，因为他们已经发现一个项目方自有的公链是多么具有价值，它能保证区块链的代码完全由业务方控制，又有助于通过公链建立完整和多样的经济生态。

2. 愿景

纵然，实现一部分区块链业务逻辑最优的做法是开发自己的公链，然而对于一个创业团队来说，从零开始实现一个区块链系统未免过于严苛。很不幸的是，当前社区中只有一部分开发者接受并理解区块链的技术和思想，而具备开发完整的公链系统能力的则更加少。总结下来，目前的公链开发领域，存在如下几个问题:

- 公链开发门槛高，其一致性算法在初期得不到有效验证。一个公链的开发周期经常长达一年甚至若干年，比硬件开发周期更长，造成相关领域市场溢价过高。此外，许多公链开发代码质量堪忧，没有形成健康的社区进行开发讨论。
- 公链缺乏非线性系统的讨论与设计。正如我们所知，无论比特币系统还是相当火热的EOS，在形式上都不是绝对正确的共识算法，它们的运行拥有诸多基于社会及组织的假设。因此，我们需要关注如何设计、验证这些假设，并设立环境来检验：基于这些假设下，某个共识、算法是否有效。
- 更多种形式贡献证明的问题。BaseLab团队认为，相比较高 TPS，如何去证明用户其他形式的贡献更为重要，如文件存储、带宽等。比如Filecoin的激励基础在于证明了某个节点贡献了文件存储。兰花网络的激励基础在于证明了流量贡献。

Basechain致力于降低公链项目的开发成本和难度，提高开发速度从而降低项目的投资成本，使得最终降低公链的开发门槛。Basechain将提供公链项目的开发工具链，并尝试建立公链开发、测试乃至部署的流程和基础设施。对于商业想法的验证，Basechain将提供一系列模拟器来进行实际模拟。另外，BaseLab团队希望提升大众对于区块链的认知，而一种新技术往往需要社区开发者首先接受并尝试，故而团队也将同时关注BaseChain社区的发展。

3. 商业

3.1 公链开发框架

与区块链技术同时兴起的分布式商业，以多方参与、共享资源、模式透明等为主要特征，提倡专业分工和价值连接，通过预先设定透明的价值交换或合作规则，使得分工及集群后的新商业模式产生强大力量，与传统单一中心化实体主导的商业模式相比有显著优越性。

在此背景下，区块链技术、分布式账本技术及其相关的分布式一致性算法等成为了前沿科技的核心代表。与基于单一信用背书实体的传统信任机制不同，区块链的信任机制是多个参与方对透明和可信规则的共同信任、对客观信息技术的信任。

目前有许多致力于参与分布式商业的项目方都在开发自己的公链，项目方设计了各种精巧的经济模型和共识机制来为自己的分布式商业规划提供链上技术支持。同时许多机构投资人及个人投资者为这些前景远大的商业规划投入大量的金钱作为前期支持。

区块链项目的特质决定了，绝大多数时候项目方难以对经济模型和共识机制这两个方面的收敛性进行先行验证。同时苦于人力成本高企，合格区块链开发人员匮乏的现实状况，许多项目方在搭建符合他们所设计的经济模型和技术模型的区块链过程中，遇到了公链技术落地上的巨大困难。

BaseChain是BaseLab团队为未来的分布式商业所搭建的一套开发框架。BaseChain能够帮助它的支持者以一种低成本的方式开发区块链。即使是初级程序员也能够通过学习BaseChain开发，快速获得开发区块链或者相关技术的技能。

BaseChain社区以发放BaseCoin做为社区激励的形式，将开发者、公链项目方、链上应用连接起来。BaseChain社区将会给开发者提供教育和培训，让社区的开发者有能力与项目方一起协作开发公链。

3.2 公链节点共享

项目方开发出公链只是一系列艰苦工作的第一步，除此之外，公链的主网上线也是一件非常困难、蕴含高度风险的事情。一般项目方开发的公链，在上线初级很难获得足够的节点算力来支撑整个公链的运行，一旦遇到算力攻击，也几乎没有办法抵御。

BaseChain并不只是一套开发工具，它同时也是区块链运行的基础设施。BaseChain的节点设施，不仅能为BaseChain公链本身提供运行环境，也能为其他基于BaseChain开发的公链提供运行的算力节点。BaseChain设计了一套激励机制，可以对基于BaseChain节点运行的公链进行监测，一旦发现51%攻击的迹象，BaseChain会发布临时激励措施，鼓励有算力冗余的节点接入被攻击的公链，实现对51%攻击的抵御。

3.3 公链性能及去中心化度评测

BaseChain提供的公链测试工具，不仅能为BaseChain用户提供一套完整的开发测试工具，它同时也能够为投资人评判现有公链提供帮忙。

一条公链好不好，是不是值得投资，能不能达到项目方在白皮书里面宣称的目标，一定要有可复现的、客观的评价标准。BaseChain将会为对某些公链有兴趣的投资人提供针对性的专业报告，改变目前投资人投公链全靠感觉和研读白皮书的现状。在去中心化程度上，最近也有知名的公链开发方和投资人发生纠纷，投资人称公链开发方可以修改投资人钱包权限，以限制投资人提充资金。

BaseChain的公链测试工具能够从多个维度对公链的的技术性能进行评测，给出性能的Benchmark和去中心化度，让好的项目方能够在公链的竞争中脱颖而出。BaseChain可以帮助对自己公链性能有信心的项目方，向其他竞品发出挑战，不服就跑个分。

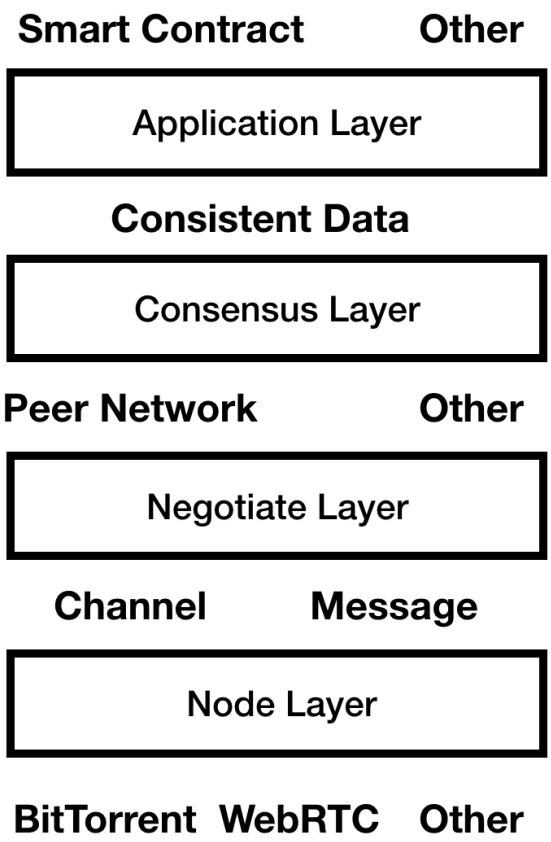
3.4 去中心化交易所

BaseChain提供跨链的价值交换，凡是基于BaseChain开发的公链，都可以通过BaseChain进行信息和价值的兑换。BaseChain上面可以天然形成一个高性能低成本的去中心化交易所。

4. 技术架构

4.1 概念模型

在本质上，区块链是一个拥有写入规则的分布式数据库，并在特定条件下保证了该数据库的一致性。在浏览了市面上绝大多数公链项目后，BaseLab团队提出如下的公链分层:



- 节点层：节点是任何分布式系统的基础，节点与节点之间的通信构成了节点网络。节点层需要实现如下的基本功能：
  - 发现节点。
  - 节点间通讯路由。

  一般情况下，解决“女巫攻击”需要额外机制，即：在对等网络中，单一节点具有多个身份标识，需要通过控制系统大部分节点来削弱冗余备份的作用。为了解决“女巫攻击”问题，Basechain提出“代价函数”概念，即：在经典的 PoW 共识算法中，由于节点并不会有实质性的投票作用，所以分子为0，因此造成女巫攻击的代价无限大。其他网络(如 BFT）中， 女巫攻击也可能存在，所以需 要通过增加 Cost Of Creating New Node 提高攻击代价，比如Dfinity以及采取PoS机制的分布式系统。不过，Basechain提供的框架并不认为PoS没有考虑女巫攻击问题，而是PoS恰好解决了这个问题。
- 协商层：协商层往往是其他公链没有的一个特殊层，它是多样化共识算法的支撑。简言之，节点层通过协商层的抽象来实现不同的共识算法，协商层通常要完成：
  - 随机数协商：如Proof Of Luck或者Dfinity都会要求有一个可被所有节点协商认可的随机数生成机制。
  - 适配协商：用来和其他已经运行的公链进行数据交换，以完成一些特殊的操作。
  - 通讯协商：协商如何进行广播、宣告等操作。
  - 加密协商：协商加密的算法。
- 共识层：共识层是区块链协议的核心部分，定义了共识算法以及块数据的范式。Basechain框架中允许构建链结构和DAG结构。
- 应用层：通常包含一个有限状态机(智能合约的解释器)。

以上就是Basechain公链的分层。此外，公链节点层的节点还运行了一个程序，称为“母节点”。母节点是Basechain节点的子程序。当有人创建一个链合约（Chain Contract）时，母节点会根据链合约的参数和配置，运行一个新的节点程序，而该新节点将会在新链上运行。母节点的运行者除了获得在新链上运行得到的收益外，也可以通过Basechain链合约规定的激励，来获得额外的收益。

通过链合约，公链开发团队可以让自己的公链快速获得可信的节点网络，即共识复制，把Basechain已经形成的共识复制给在Basechain上共生的其他链。与EOS等子链体系不同，Basechain的链合约可以允许开发者开发符合自己特色的新链，而越来越多的新链也将让Basechain的共识更加可靠。

为了让公链的代币融资和换算更加简单，可以把链合约嵌入到智能合约内部。链合约运行时，即自动将智能合约的代币映射为链上的代币。

Basechain将会成为未来分布式系统世界的核心枢纽，成为链的链。

4.2 Basechain Network

4.2.1 共识算法特点

Basecoin Network是一个针对普通用户及开发者的公链，Basecoin Network的特点是具有极强的可扩展性：

- 修改协商层的广播，采用“收集者”机制。不必把消息发送给每个人，而是发送给收集器，由收集器发送给每个人。如果消息采用加密方式签名，将通过阈值签名的方式使得收集器消息大小从线性增长速度减少到常量增长速度。
- 使用阈值签名减少通信的总小。在过去的解决方案中，由于发送ACK消息给对方时，每个节点都需要一个签名验证，所以每次创建交易，每个节点都会收到一条消息。当节点数变多的时候，网络会增加巨大的负担。Basecoin Network的“收集者”会收集所有的阈值签名，再发送消息给每个节点。
- 采用Boneh—Lynn—Shacham签名，在安全性上匹配RSA2048，体积更小，速度更快。
- 采用乐观执行(optimistic executions)，用乐观执行来进行视图更新(View Change)，减少需要传输的历史状态。

4.2.2 共识算法的共识算法

我们假设一个标准的异步BFT系统模型，其中一个对手可以控制多达 f 个拜占庭节点，并且可以延迟任何有限数量的网络中的任何消息。为了展示我们改进的结果，我们还区分了两种特殊情况。我们说系统处于同步模式，当对手可以控制f个拜占庭节点时，但是任何两个非故障节点之间的消息都有一个有界延迟。最后我们说系统处于通用模式，当敌手可以控制多达c ⩽ f个节点，这些节点只能发生崩溃或行为，运行速度慢，并且任何两个无故障节点之间的消息都有一个有限的延迟。

我们广泛使用阈值签名，其中对于阈值参数 k，来自总共n个签名者的k的任何子集可以协作以在任何给定消息上产生有效签名，但是没有小于k的子集可以这样做。阈值签名在以前的BFT算法和系统中证明是有用的。每个签名者都拥有一个不同的私人签名密钥，可用于生成签名份额。对于希腊字母α，我们用αi(d)表示签名者i对摘要d的签名份额。任何k个有效签名份额{αj(d)| j∈J, | J | = k}可以使用公共函数组合成单个签名α(d)，产生数字签名α(d)。验证者可以使用单个公钥验证此签名。

对于我们的区块链，我们使用键值存储。从一个副本中有效地获得客户端确认，我们通过数据认证接口增强了我们的键值存储。正如在公开无许可区块链中一样，我们使用Merkle树接口来验证数据。为了提供数据认证，我们需要实现以下接口：

1. d = digest(D)返回D的Merkle哈希根作为摘要。

2. P = proof(o, val, s, D, l)返回在序列号为s，状态为D的判定块的一系列请求中作为第l个操作执行操作o的证据，该操作的输出是val。对于键值存储，放置操作的证明是Merkle树证明放置操作是在序列号s的请求中作为第l个操作进行的。对于只读查询q，我们写P = proof(q, val, s, D)，并假定所有查询都是针对Ds执行的(状态D在完成序列号s之后)。对于键值存储，获取操作的证明是Merkle树证明，在具有序号s的状态下，所需变量具有期望值。
3. 如果P是一个有效的证据，证明(o, o, val, s, l, P)返回true，那么证明o是作为序号为s的第l个操作执行的，并且在这个判定块执行后得到的状态具有摘要d和val是操作o的返回值（并且当q是查询时类似地验证(d, q, val, s, P)）。对于上面的关键值存储和放置操作，验证是植根于摘要d(Merkle哈希根)的Merkle证明验证。

我们维护n = 3f + 2c + 1副本，其中每个副本在{1, ..., 1}中具有唯一标识符。。。 ,3f + 2c + 1}。该标识符用于确定三个阈值签名中的阈值签名：具有阈值(3f + c + 1)的σ，具有阈值(2f + c + 1)的τ和具有阈值(f + 1)的π。

我们采用副本从一个视图移动到另一个视图更改协议的方法。在一个视图中，一个副本是主要的，其他副本是备份。主要负责就一系列决策发起决策。与某些备份副本不同，它可以具有作为Commit收集器和/或Execution收集器的其他角色。在给定视图和序列号中，将c + 1个非主要副本指定为C收集器（提取收集器），将c + 1个非主要副本指定为电子收集器(执行收集器)。这些复制品负责收集阈值签名，将它们合并并传播所产生的签名。为了生存，只需要一个正确的收集器。我们在共同模式下使用c + 1收集器进行冗余。

粗略地说，该算法在通用模式下工作如下:

1. 客户端向主节点发送操作请求。
2. 主要客户端请求创建一个决策块，并将这一系列请求作为预先准备消息转发给副本。
3. 副本使用它们的σ(3f + c + 1)阈值签名对请求进行签名，并向C收集器发送签名共享消息。
4. 每个C收集器收集签名份额，为决策块创建一个简洁的完全提交证明并将其发回给副本。这个单个消息提交证明具有固定大小的开销，包含单个签名并且足以供副本提交。

步骤2、步骤3和步骤4需要线性消息复杂度（当c是常数时），并替换先前解决方案的二次消息交换。

通过为每个决策块选择一个不同的C收集器组，我们平衡所有副本上的负载。一旦副本接收到提交证明，它就提交决策块。副本然后启动执行协议:

1. 当副本具有连续的已提交决策块序列时，它执行这些操作并使用其π(f + 1)门限签名 签署新状态的摘要，并向E收集器发送符号状态消息。
2. 每个电子收集器收集签名份额，并为决策块创建一个简洁的完全执行证明。然后，它将证书发送回副本，指示状态是持久的，并向客户端发回证明其操作已执行的证书。这个单个消息具有固定大小的开销，包含单个签名并且足以用于确认个别客户端的请求。

步骤1和步骤2为每个客户端提供单消息每请求确认。以前的所有解决方案都需要为每个客户端提供线性数量的每请求确认消息。当客户数量很大时，这是一个显着的优势。

4.3 Basechain Framework

4.3.1 Basechain Consensus Language

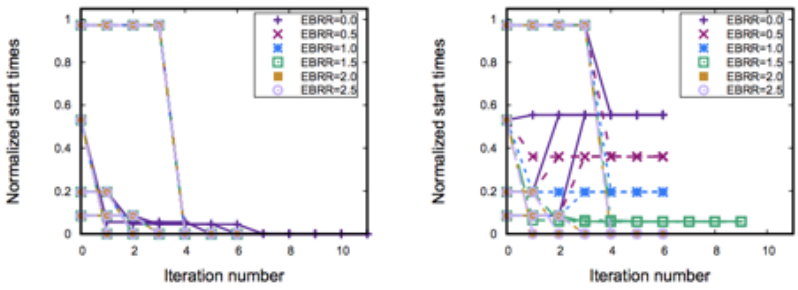
Basechain Consensus Lanugage 提供了一个高度抽象的开发语言，用来开发共识。这是业界第一个对共识算法开发进行抽象的编程语言。将会简化现在PoW 和 PoS 算法 90%。

```
role Proposer:
  def setup(acceptors):
    self.n := undefined
    self.majority := acceptors
  def run():
    send (”prepare”, self) to majority
    await count {a: received (”respond”, =n, _) from a}
       > (count acceptors)/2:
    responded := {a: received (”respond”, =n, _m) from a}
    send (”accept”, n, v) to responded

role acceptor:
  def setup(learners): pass
  def run(): await false

  receive (”prepare”, n) from p:
    if each sent (”respond”, n2, _) has n > n2:
      max_prop := any {(n, v) sent (”accpeted”, n, v)}
    receive(”accept, n, v):
      if not some sent (”respond”, n2, _) has n2 > n:
        send (”accept”, n, v) to learners

role Learner
  def setup(acceptors): pass
  def run():
    await some received(”accept”, n, v) has
          count {a: received (”accepted”, =n, =v) from a}
    output(”learned”, n, v)
```

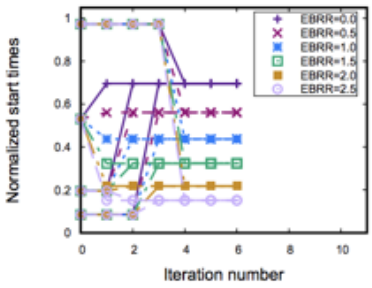
这是一个我们用来编写 PBFT 算法代码片段。我们用了更好的框架和原语来编写。从而减少了开发量

4.3.2 Basechain Test Framework

我们会根据你的区块链的共识算法和激励制度，为你提供在各种网络下的测试框架:



(a) *low_op* (b) *med_op*



(c) *high_op*

1. 公链的运行速度和节点增加的关系
2. 公链的子链和主链安全性是否存在相关性，随着子链数目增多，是否会减少子链的安全性
3. 带宽降低的情况，公链的安全性和稳定性是否能保证
4. 激励成本是否和网络交易调高成正比…

我们提供了更专业的视角来测试区块链平台的稳定性，为区块链研发提供了指路明灯。

4.4 工具

在第一阶段，Basechain将通过三个工具来实现：

- Basechain Net work：Basechain网络，是其他公链项目部署和交换自身区块链项目的核心凭条。
- Base Chainbuilder Tools：用来生成链合约的一套工具链，将根据开发者的需要从节点、协商、共识和应用层进行设计。
- Midgard：Midgard是一个分布式系统模拟工具，提供：
  - 一个分布式系统模拟器，帮开发者度量其算法在不同网络条件下的收敛速度。
  - 代币经济模型模拟器，Midgard 将考虑进所开发代币相关经济模型的实际运转情况。
  - 非线性分析工具，基于真实世界的某些政策和交易所因素将对所开发区块链形成影响，我们设计了几个有效的非线性分析工具：
    - 激励函数分析
    - 纳什均衡分析
    - 分布度分析
  - Midgard志愿者计划，Midgard会和Basecoin Network联通，Basecoin Network的用户将会成为开发者的测试用户，来帮助开发者模拟真实情况下其经济学模型假设是否符合预期。Midgard志愿者社区将会成为去中心化应用和商业最前端的支持者，也将成为Basecoin最有价值的组成部分之一。

我们认为这些工具会极大减轻开发者的工作量，缩短价值代币的投资流程，降低投资门槛。与此同时，Basecoin的用户因为可以参与很多公链或 DAPP 的使用，也将获得极大的回报。

5. 应用

目前，已有两个区块链项目决定基于Basecoin开发。

5.1 Newscoin Network

Newscoin Network是一个基于区块链技术的内容经济网络。Newscoin Network的核心主张是：把中心化内容平台享有的线上流量红利，归还给内容生产者、分发者和消费者。阅读和点击是线上最高频的用户行为。从门户、搜索到社交媒体时代，每位普通用户的阅读和点击，造就了以新浪、百度、微博、今日头条为代表的中心化内容平台。然而过去20年来，内容的生产者、分发者和普通消费者并没有得到应有的回报。Newscoin Network认为，用户的每一次阅读和点击行为，都应获得合理的数字资产回报。

Newscoin Network由中天资讯价值联合会（Midheaven Newscoin Association）发起，总部位于中国香港。任何一个线上内容应用，都可以申请接入Newscoin Network。Newscoin是Newscoin Network的催化剂和燃料，是其唯一流动代币。Newscoin Network将把所有接入节点的用户生产、分发和消费行为资产化进而数字化、流通化，并使用Newscoin（代码NEWS，中文名牛币）作为数字资产奖励。

Newscoin Network提供一个共享平台，在这个共享平台当中有三类角色:

- 内容的生产方
- 内容的消费方
- 内容的分发方

Newscoin Network或采用区块链技术和其他点对点的平台技术，提供:

- 内容确权机制: 内容的原创作者通过发布自己创作的内容到Newscoin Network上，基于区块链技术保护原创作者的所属权不会被篡改。
- 作品版权交易: 通过确权、内容版权及收益权等让作品的交换和使用变得更容易。
- 用户行为激励: 阅读内容和创作内容本身都应该被激励,同时用户在阅读过程中提供的评价也应该被奖励。
- ...

Newscoin Network为内容的生产方、消费方和分发方提供大量的工具和激励，帮助他们通过内容的数字化权力，更方便地构建自己的商业，为内容发展贡献力量。

5.2 巴别塔——Kevin Kelly作为顾问的项目

巴别塔源自圣经《旧约全书》，是人类产生不同语言的起源。在这个故事中，一群只说一种语言的人在“大洪水”之后，决定修建一座城市和一座“能够通天的高塔”。上帝见此情形，就把他们的语言打乱，让他们再也不能明白对方的意思，还把他们分散到了世界各地。

过去几千年来，语言差异是信息传播的最大障碍，也是人类社会任何一个共识达成的必过难关。目前世界上现存的语言超过6900种，不同的语言背后，是不同的文化和价值观。唯有重建巴别塔，才能从不同之处求得大同，从大同之中理解不同。

巴别塔是一个基于区块链技术的应用平台，致力于推动全球跨语言内容的发现、翻译和传播。与其他区块链项目不同，巴别塔将真正通过人工智能和区块链技术提高生产力，也优化生产关系。

目前，中文资料和文化作品的对外输出需求迫切，市场巨大；同时，海外优质内容的输入也存在着无限的潜力。中国、美国以及欧洲也是区块链、人工智能技术和移动互联网发展的主要国家。以网络文学为例：欧美地区可供阅读的网络文学不过50部，翻译人员不到200人。与此同时，还存在着以下三个问题：

- 版权界定模糊
- 翻译效率低下
- 商业落地薄弱

巴别塔团队及其合作方在内容的创作、翻译等领域积累了丰富的经验和技术优势，决定以一种非公司化的平台来更好地提供类似网络文学出海的产品。

巴别塔平台拥有三类角色：

- 发现节点：内容的发现者将内容通过区块链进行分享和确权。
- 翻译节点：根据传播节点的需要,将内容翻译成各种文字。
- 传播节点：投资拥有潜力的内容,并通过传播给消费者创造价值。

巴别塔致力于通过区块链技术来解决版权界定模糊问题，利用人工智能引擎和智能合约来解决翻译效率低下问题，采用代币激励网络解决商业执行薄弱问题。

项目的顾问Kevin Kelly先生是《连线》（Wired）杂志创始主编。创办《连线》之前，Kevin Kelly 是《全球概览》杂志（The Whole Earth Catalog，乔布斯最喜欢的杂志）的编辑和出版人。1984年，K.K发起第一届黑客大会（Hackers Conference），他的文章曾出现在《纽约时报》、《经济学人》、《时代》、《科学》等重量级媒体和杂志上。目前，K.K担任巴别塔项目的核心顾问。

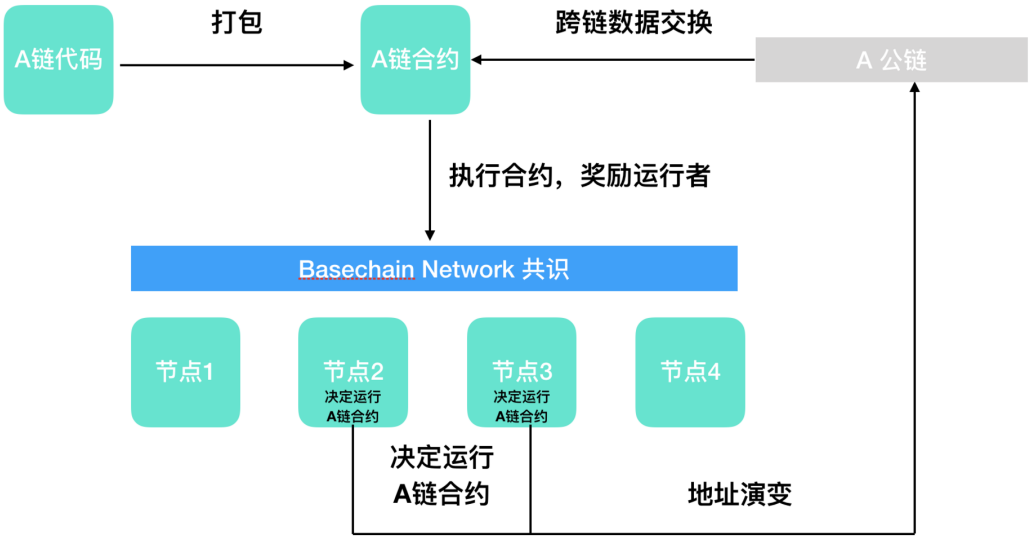
6. 社区

Basecoin是在Basechain流通上的代币，用来维护网络的基本运行，执行智能合约和链合约：

- Basecoin用作给完成Basechain-BFT投票的奖励
- Basecoin用作执行智能合约的奖励
- Basecoin用作执行链合约，即运行一个新链节点的奖励

无论是需要执行智能合约还是运行特定开发的链，Basecoin都将是开发者需要的硬通货。Basechain将通过Proof Of Propasal为开发者提供运行了某个特定链的证明。

代币循环如下：



7. 治理委员会

为了更好的支持社区发展，Basechain将15%的代币交由治理委员会，同时设计了一套机制来选取治理委员会。治理委员会由“众议院”和“参议院”组成，采用“代议制度”：

- 众议院代表“人民”的意志，其投票权由节点和人数决定，其主要决裁链下事务，共设127个席位。
- 参议院代表“持币者“的意志，其投票权有持币量决定，其主要裁决链上事务，共设15个席位。

选举办法：

- 每届治理委员会任期为846720Block。
- 治理委员会选举于每次任期提前120960Block开始。
- 治理委员会选举委员由上一届治理委员会中的众议院随机抽选42人担任，若不满42人的，由项目团队担任选举委员会。
- 为了更好的尊重开发者的利益，每个周期代码贡献度最多的组织和个人可以委托一人直接进入治理委员会的参议院。
- 为了更好的尊重Basechain的社区意愿，治理委员会每次选举发布42个有关去中心化商业、哲学、经济以及技术的问题，用来分成 2^42个小区，并使用最小近邻算法合并为127个虚拟选区。
- 虚拟阵营，治理委员会每次选举发布42个有关去中心化商业、哲学、经济以及技术的问题，用来分成 2^42个小区，并使用最小近邻算法合并为2个虚拟阵营。
- 众议院和参议院分别由虚拟选区和虚拟阵营进行选举。

众议院权力：

- 决定代码的硬分叉。
- 决定出块时间、奖励。
- 讨论制定出块标准和共识算法。

参议院权力：

- 决定运营资金。

- 仲裁链上纠纷。
- 提供雷电网络通道，即提供快速的支付结算服务，并获取佣金

9. 团队成员

李立鸿
李立鸿，人工智能与区块链专家，拥有多年区块链及机器视觉方向的研究经验，擅长图像处理、深度学习、人工智能、区块链技术模型及经济模型搭建，多家互联网公司技术合伙人，上海交通大学人工智能专业博士学历

左开扬
摩根士丹利、高盛系统架构及产品设计副总裁。精通融资融券、股票交易、市场风险管理（VaR、压力测试）、期权和衍生品定价和设计等金融技能，同时精通Scala、Python等开发技能。曾就职于摩根士丹利、高盛等公司，从事风控、衍生品等系统架构设计及开发。擅长区块链技术及经济模型的搭建及设计。

丁舜佳
搜索引擎及技术和分布式数据专家。在亚马逊、ACQUISIO、YELLOW PAGES GROUP等多家互联网公司主导定制开发搜索引擎、数据分析等业务。精通数据分析平台开发，以及数据分析、自然语言处理、机器学习及区块链等多种开发技能。

马晨阳
物联网高级技术专家、上海交通大学工商管理学硕士。曾主导多个物联网云平台的架构设计，javascript 语言解释引擎以及操作系统中间件的研发。Ruff 研发总监，精通物联网mash网络通信模型架构设计、云计算后端开发、区块链等相关技术的底层实现。

邓天源
市场营销专家。2008-2010年新加坡丰隆集团MKT ，2010-2013年香港利星行BD副总监，2013-2016年上海绿地集团西南区风控总监。2016年开始在数字资产投资，DASH、XLM、BNB、OMG、HPB、GXS、LEND早期投资者。曾参与poly、LEND国内宣发，2018年创办鑫禾资本及贵州区块链俱乐部。

9. 代币发行

Basechain将发行42亿枚代币，用来纪念Answer to Life, the Universe, and Everything，以及向2100万枚BTC致敬。

Basechain 分配如下：

- 15%：用于流通和募集。
- 10%：用于核心团队成员奖励。
- 15%：社区激励，由Basechain委员会智能合约托管。
- 60%：用于鼓励 Basechain 节点参与投票和出块。