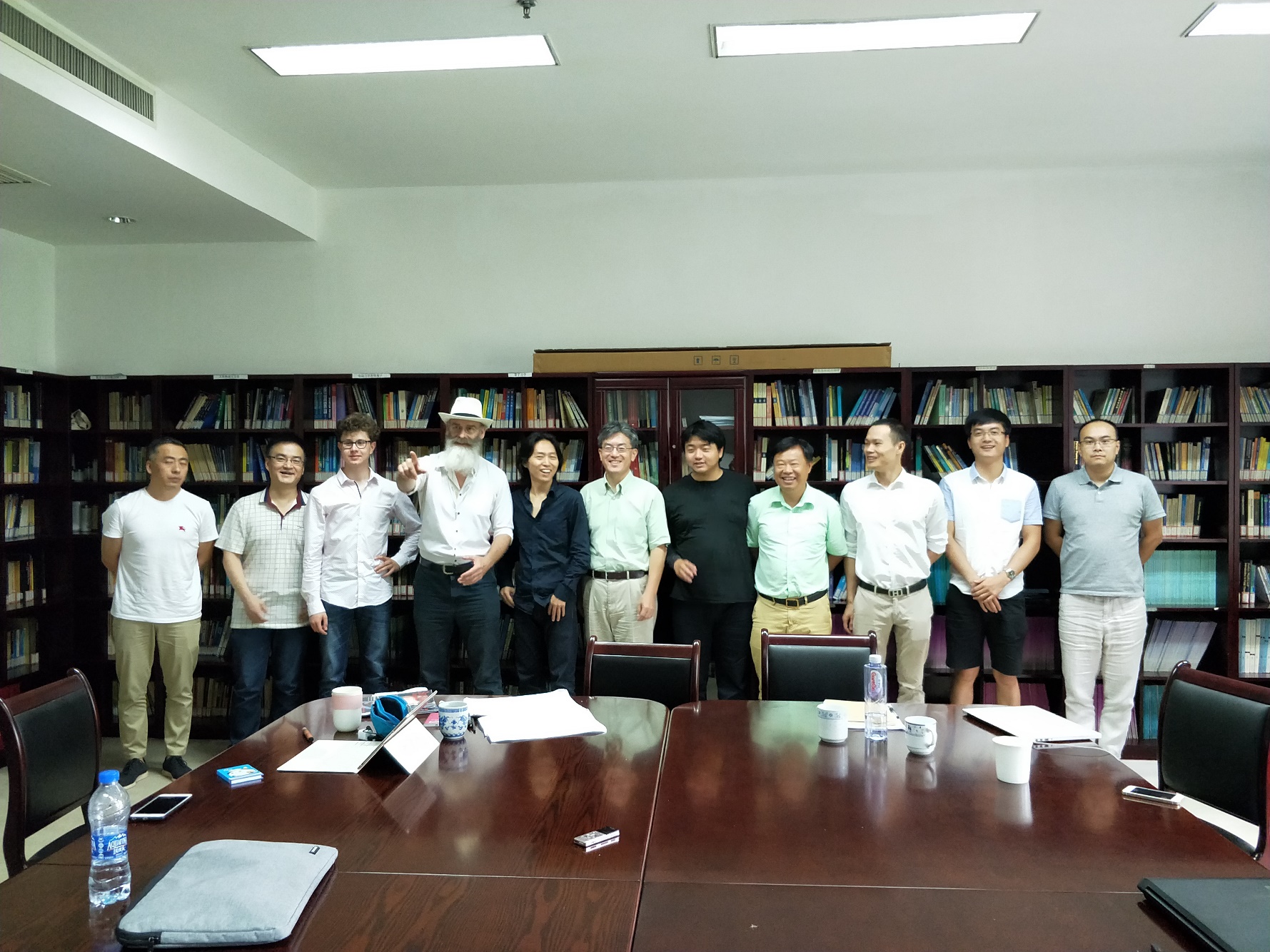
**区块链下一步发展应放弃主链思维**

亦来云清华大学技术研讨会纪要（节选）

参加人：陈榕、辕询、徐继哲、韩锋、叶飞、于班长、李涛涛、大龙、苏翼鹏、胡洪杰等

时间：2017年7月15日

地点：清华大学



首先，亦来币开发团队LEADER辕询（美籍华人、伊利诺伊大学计算机系毕业、Kraken平台核心开发者之一）介绍了亦来币的基本开发设想，四个大方面和四个小方面。

辕询：制定了亦来币一些重要目标的时候，我们会把我们的精力都放在这上面。那些数字货币别的方面，我们越保守越好，做得越简洁越好。每一个数字货币都有三个基础的协议，一个是它的货币格式，我们叫A。一个是它的节点与用户的协议，我们叫B，节点的协议叫C。我们主要会进行比特币的方向，比特币的B协议有30个函数，C协议有105个函数，好些都是重叠的，我们写比特币的时候，是想把最后的函数塞在一个包装里，因为好多人不懂这个概念，不做一个统一的，包括好多混杂东西的系统的话，好多人可能一开始不接受。但是我们估计我们能写一个跟比特币大概一样的系统，它有**proof of work**，工作量证明和一些别的，公钥、私钥、安全性，但是我们的代码，相当于比特币的十分之一，因为我们只是专心在主要的方向上。网络操作和硬盘操作，我们不把那些别的，不直接相关的代码放在一个包装里。

所以四个大的目标是这个，一是联合挖矿，即Equivocation。联合挖矿就是说亦来币能跟比特币同时挖，我们需要调整和沟通，来找矿池，帮他们一个一个布置好联合的代码。第二个继承遗产，即Inheritance。就是说在某一个区块，我们会设定某一个区块处，所有的比特币的区块小于那个数，就是在那个区块数之前，它都会可以取免费亦来币，所以已存的比特币的持有者，都会自动一对一得到亦来币。这个好像没有人做过，这个是类似硬**分叉**，但又不是一种分叉，因为我们的区块链还是会从创世区块开始。第三个，是奖金，即Premium。这个币会有一个一次性的创始人奖金，这个奖金大约设定为1650万，相当于所有已存在的币都会复制一遍，被复制的那个币，会到亦来云这个基金帐户里面。这个有人做过，不同的币有过创始奖金这个概念，但是他们主要是通过两个方式，一个是有一个固定的税，把每一个，挖矿上有的20%的税的金额直接进帐号。

韩锋：你是指ZCASH?

辕询：对。第四个就是通胀，即Gratuity。我们会有膨胀率，在我们系统上。这个通胀率，比如4%，其中70%奖励联合挖矿，30%奖励开发团队和运营。

所以这是四个主要的目标，我们的工程，我们的理想主要围绕这四个。

韩锋：还有四个小目标呢？

辕询：还有四个小的目标，小的目标是过后也能进行的。而且主要我从两三个星期之前的一个会议上，写了一些东西，然后过后又自己单独分析了。第一个是逃避过滤器，比特币是有一个固定的特殊数字，叫魔法数字。如果是两个节点，就是C协议想做交易的话，首先要发魔法数字，对外改易遇到魔法数字的时候，它就知道这是一个交易开始，就开始记。但是问题是这种形式，沟通的形式会很容易被筛选，要是过滤器想要挡上这个协议。所以比特币很容易被一个防火墙挡上，要是某一个防火墙的控制者，决定他想禁止所有比特币交易，一下子就可以。但是一个防火墙，他们都是模糊的禁止，允许任何一些混杂的信息出去，你总是要有方式来藏你的关键信息。所以理论上，除非某一个国家完全封闭他的网络，他总是让任何一个东西出来，加密或者用别的手段。徐刚主张我们把协议调升，或者设计成一个允许对外沟通的模式。穿出过滤器，一个主要的方式，就是你必须得躲避魔法数字是固定数字。你不能有一个固定的号码来表示这是一个亦来云、亦来币，要是有这个号码，他们把号码发到过滤器里面就完了。也需要有一个旋转的号码，或者需要找一个方式来发送信息的时候，里面藏一些比较混杂，不相关的信息，来把关键的信息挡住。或者一些黑客的技巧，但是我们用这个是来保护我们隐私的。

第二个是关于通信，分别是linsten和connect。每一个原则在网上Transmission Control Protocol/Internet Protocol(TCP/IP)都会有两个对访，一个是连接者，一个是监听者。但是根据现在的模式，任何一个预联网计算机都能是一个连接者，但是不是所有都能当监听者。想当监听者的话，必须有特殊的、上层的IP地址，这个IP地址是平常家常用户是不允许的，买不到的，需要开一个商务帐号，再订网络服务，才能得到一个静态、上层的IP地址。但是因为这个游戏技术有害，因为游戏是需要整个玩家能连上的，所以十几年之前，一个技巧被发明了，叫Network Address Translation（NAT），目的就是通过某一些特殊的技巧，可以允许一个正常的、家常的用户，也能连接上。比特币受到这个缺陷一些问题，比特币因为它需要有好多节点，越多节点越安全，但是大多数的节点都是家常用途，不是商务用途，特别是在美国。美国人不是像中国一样这样意外轻闲，但是问题是大多数的节点，只能收信息，不能发信息，因为你要提供给信息，你必须是连接的监听者，不能是一个连接者。所以这就引起了一个问题，你要是想错过这个限制，你必须得改C协议，尤其是把C协议从TCP转到User Datagram Protocol （UDP)。但是美国的群体，没有领导的能力来更改，做这么大的更改，美国不用做太多的更改，不要让所有人马上变换。而且这个IP一部分变化，一部分不变化，也不会引起分叉，因为这只是沟通的协议，不是格式协议。但是这个工作量也是有点大，对于比特币来说。要是只十分之一，二十分之一的节点做代码更改，UDP就能通了。TCP有了网络，UDP有了网络，但是10%或者5%的节点能站在中间，两个都封，就可以扩大这个网络，每一个手机，每一个计算机，都可以有这样一个节点。

所以这个是比特币没有做到的，但是我们想看到，亦来云做到了。而且这个很重要，对于陈榕先生的，为何让家常机器，被动的上云。

陈榕：这件事，我们已经在几年前开始准备了，这么一个智能加机的P2P的网络。

韩锋：这样的节点也会参与挖矿吗？

陈榕：这个简单我翻译一下，因为辕询讲的比较技术。简单讲，我们家里有一个智能路由器的话，比如网上的一些信息，我们上网能拿到。但是我们不能向别人提供服务，比如说随便一个新浪什么，要想对外提供服务，必须有一个静态的IP地址。所以别人想从你家里对等的拿到东西，你家里的路由器是可以拿到网上的东西，你可以上新浪 ，但是你不能提供类似新浪的网站，让别人来访问。这个时候你要是想访问的话，让家里形成一个P2P网，比如说你家里有一个微网站，刚才谈论这个事，新浪就是大网站，每个家庭能不能有一个微网站，因为比如说我们家，让个人拥有数据。比如我自己写个电子书，放在自己的微网站上，给在座十几个人看，我这个微网站站也支持不了什么上百万的用户，但是我家里微网站能支持，美国的家庭可以1G的流量对称，中国现在起码是下行，比如说下行100兆到200兆，在城市已经很普遍了。上行，像我家的上行能够达到8兆，起码支持我们这几个人读本电子书是没有问题。

所以其实中国现在的技术设施也已经相当发达了。那么在这个时候，我们其实几年前启动了这个项目，能让家庭的网站，能做的其实就是辕询在讲的这个事。这个网，反正我们代码全都会启动出来，所以我们想通过这次做亦来币的事，主要是辕询在主导，就是一些币大家讲四大目标，当然像四小目标，逃避过滤器，打洞这个大家跟工程师聊聊就差不多了。

韩锋：那么这个节点跟挖矿没有关系？

陈榕：没关系，所以第二个目标，基本上可以走到大道上。

辕询：挖矿是可以选的，因为挖矿是历史的遗存问题，再一个矿池的话，这个矿池的主人会有1个以上的节点。别的矿池的参与者，只有挖矿程序。挖矿程序必须要遵循这个节点，奖励挖矿的钱都是先通过他们的口袋，才可以发出去。第三个，侧链。比特币现在它现在目前的冲突来源其实是因为侧链，有部分人向增加侧链可运行性的进展，引起政治性质的博弈。但是因为我们是在重造一个币，不是从比特币某个分叉点技术输入，是从1开始输。所以我们有这个能力，在起初把我们的格式划定一个对侧链比较友好的格式。我们觉得长期来讲，侧链是不可避免的，因为一个人，你要全世界共享一个链，是一个公共记忆、记帐的方式，但是有的时候，在 某一些人之间的交易不用功能来记帐，只是需要从主链提一些钱，交换一下，然后再把新的状态给主链汇报一下。侧链，我确实是想请**BLOCKSTREAM**这个公司，这个利益集团的想法，但是他们长期侧链能带来很多好处，侧面要是有一个侧链，我们就不用有矛盾，这是区块的速度。

但是这个问题这是侧链,现在比特币的格式，不允许侧链。比特币的格式，因为**Elliptic Curve Digital Signature Algorithm** (**ECDSA**)有一个小的故障，或者是一个小的缺陷，你签了名字之后，ECDSA的签名，不是一对一的，是一对好多的一个函数。所以每一个签名都有无限的，或者一个相融签名，所以一个节点如果是恶意的话，如果想倒灌的话，把一个签名改成一个通用签名，这个会影响**交易地址**，就不会影响实际的运着，打破侧链变成主链，能接上来的方面。

徐继哲：必须要有一个时间，比特币先要支持它。

韩锋：那要采取硬分叉，才能实现这个吗？

辕询：这个问题是core组， core认为之前比特币协议要是更改的话会投票，比方说投票一个挖矿者一个票。

韩锋：他们想否定这个。

辕询：他们不喜欢中国人的影响，所以他们用这个机会，用这个前提，来想推广一个节点一个票，而不是一个挖矿者一个票。中国的算力比美国多。

韩锋：但是美国的节点更多。

辕询：实际就是这个矛盾的来源。所以这就涉及到第四个问题

徐继哲：它们就是闪电网络，是这个意思吗？

辕询：但是我们的想法就是侧链，我们不一定在主链上运行。

徐继哲：以太网的实践已经说明了大量的智能合约运行在主链上有很多的被动。

辕询：要是一个主链上运行这个合约，要是某一个链上运行智能合约，表示所有有这个链的节点的人，必须得同时运行。

徐继哲：对，这个效率一下子就下来了。

辕询：这个引起了一个很奇怪的现象，以太坊手里有这么大的算力，要是都加在一起。可是它上面跑智能合约的环境，是非常非常弱的。

徐继哲：效率非常低。

辕询：所有的计算节点都是在合作来运行一个，大概10个**普通**的计算机。而且更可怕的是，你为了要用户接触这个智能合约，他们有一个界面程序，这个程序特别慢，需要有一个最最头等的计算机才能用。

辕询：为了避免这个，我们需要对这个界面程序进行改造，造一个侧链。让一些网络的一部分造一个侧链，只是他们运行一些交易，貌似是这样。

韩锋：我明白这个意思了，亦来云的智能合约只在侧链相关的节点运行，或者是授权的节点，比如银行智能合约账户，这是徐刚给我讲的。

辕询：所以这就表示相关的，而且也可以加上几个验证者，或者监督者。

我们的系统，主要是容易安装，**比特币**非常不容易安装，**以太坊**也不太容易安装，我们出了一个题在课上，让不同的学生拿一个新的服务器，特别是一个不适用于**比特币**的服务器，安装**比特币**节点程序。但是我们要是想做一个真正云计算的网络，这是不可执行的。我们的目的，就是希望这个程序越小越好。

韩锋：你提出的技术指标，比如说一个普通的用户，需要多长时间？对它的硬件配置有什么特殊的要求？

辕询：我们主要是说，把所有东西装在一个包装里，直接点这个包装。

韩锋：点击即用，最关键的是要花多少时间。

辕询：我们肯定不用几个星期。

辕询：安装需要多长时间？

辕询：就是下载，就能安装，就像windows一样，大多数windows程序，下载点一下才能安装。

韩锋：那应该是半个小时之内，就能结束。

辕询：半个小时，甚至十分钟就可以。有了这个之后，再加上亦来云。

韩锋：但是有一点疑问，你不需要把那个所有的总帐都下载了吗？那个是很花时间的，你下载程序容易。

辕询：我是说下载程序，但是问题现在下载程序，你要是不用就搬出，原下载程序和安装程序就需要几个小时。

亦来币有一个好的优势，一个非常好的优势，我们一开始我们的交通量不是太多，而且我们是从1开始，所以一开始，我们的储存量是非常小的，我们完全能够让手机开始跑我们这个程序，这个节点。有一个容易安装的模式，中国的节点在亦来云上能马上上位（大大超过比特币节点）。

韩锋：这是好事。但是有一点，建立这样一个节点，对它的好处是什么，如果不想影响挖矿的话。好处是什么？可以建智能合约？

辕询：建智能合约，建侧链。你每次想查一个帐户有多少钱，都需要跟节点。但是这是实际上大多数人会依赖于中心，比如一个钱包网站，就属于中心，一个钱包网站同时支持2000个用户。

徐继哲：只能是在线钱包是这个意思？那我明白你的意思了。

辕询：我们能强烈的减少在线钱包的依赖性，每个人都有自己的钱包。而且这更好了，大多数的钱包就呈现进来，或者网站需要你输入几个IP地址，信任的IP地址，它会跟那些IP地址来交流，这不是我们原来的预想。

韩锋：这不是一个去中心化的想法。

辕询：虽然比特币的总额那么高，但是你想整个世界才有7000多个节点。

韩锋：亦来云至少几十万。

辕询：我们很可能达到几十万的节点。

叶飞：这个问题，用户之所以节点越来越少，最大的限制就是数据量，这一点就已经把普通的人去除。

韩锋：他没有动力。

叶飞：轻节点上，在手机的话，那是不可能的，他永远不能下载。

辕询：轻节点和重节点之间，其实也有一个方式。这个方式就是有一个把节点分成两半，一半是储存的，另一半是计算的。计算的放手机上的，储存的是能放在另一个上。

韩锋：比如说希望用**BLOCKSLACK**解决，比如说分布式存储。

辕询：完全可以。

陈榕：我当时只是调用分布式存储那个，就把两个任务分开，而比特币是合二为一。

辕询：所有的数据还是我控制的，不是一个公开节点控制的。比如我的手机上安装计算的一部分，但是存储那部分是通过**BLOCKSLACK**、阿里云盘、百度云盘，每次他修一个区块的话，会通过加密的网络察看一下云盘。这样做会有点慢，但是会很安全。这是完全可以体验的，其实我的目标是在6-9个月之内，当亦来币上线，我是希望世界上能有100万个节点。

陈榕：我原来的想法是说，其实我们对于用户来讲，是搭一个P2P的网站，一些个人的微网站，包括百度云，对个人来讲是一个微网站，反过来我们要求所有的微网站，都要起码是一个轻节点。你只要是一个微网站，其实在下面已经记了所谓的这些**访问信息**。

陈榕：甚至讲你在腾讯那，在阿里云上，必须是一个，你要是一个家庭微网站，起码是个轻节点，你要真的有**轻节点**，今天的互联网所谓的重网站，那你必须要有节点，这个要求你在这上面弄一个安全的网站，就必须是一个亦来云的节点，你要是160G你也得花。而且我们当时这点事，起自于5年前，我们曾经接一个软银的项目。后来这个项目是LG赢了，这个单想干嘛呢？它希望比如说就是一个接入商，像中国电信是一个SP，这个SP像今天我们看到官方，一般都是电信送你的，这时软银经常做这些奇思妙想的事，我不但送你光猫，这个光猫里还送你500G的个人云存储，你要都用就交财，这么简单，500G我送。其实那个光猫里面放的是1T硬盘，不是500G硬盘。他说我送你500G嘛，因为你也不看，反正给你一个盒子，这个盒子里是一个1T的硬盘。实际上那500G，做了P2P下载和那些电影的种子了，这个东西藏数据于家 。

其实我们做操作系统，你也很容易想象，相当于你做个操作系统，你查你的硬盘有多少USE，多少free，实际上直接把free部分用了，你用了600G的**空间**，那你想这300G干嘛了？作为操作系统，我告诉你600G用了，300G我就用了，你再用我就减少了，不就这么一个简单的道理。反正就这点电，各自都给开了，其实曾经是想做这个事，我也既期望我们做这种对于用户大家很容易想象，中国人不愿意装节点，因为大家不愿意奉献。都愿意占大便宜，不愿意奉献。

叶飞：没有这个驱动，我觉得全程都差不多，必须有一个驱动。

陈榕：就是你要做网站，因为你要发布点东西，那你必须起码是一个轻节点。

叶飞：我估计在中国会有上百万的人想要开节点，要是稍微有一点门户的关系。

陈榕：我们想到几个月几百万，最终有几百万，随着这个网站的多。

辕询：希望至少提出一个愿景来。

陈榕：微网站上，家庭微网站起码是一个轻节点。

韩锋：为了实现这个目标，这就是最大的出发点。

叶飞：从推销的角度，我们需要有一个这样数字，来设置一些节点。

陈榕：起码这是一个目标，为什么要装节点，因为必须装。

韩锋：因为现在任何一个区块链公链，哪怕以太坊，都离这个数据极其遥远。

叶飞：而且你要细分一下，现在区块链的节点，其实有几个功能，一个是钱包的功能，就是收发。现在一个比特币客户端是一个节点，有几个子功能，一个是完整帐本，这个要求很高。再有一个它作为数据的中转站，系统一部分提供的东西，也是它的一个功能，还有Simpilfied Payment Verification(SPV)稍微做一些简单的，我们这个节点，一剔除掉完整的帐本，其实还可以做很多事情，钱包可以做，P2P内部也可以做，所以说是可以的，可行的，快速的达到更多的节点是可行的。

韩锋：关键最重大的驱动，陈榕说的搞一个其他的，有一点商业性质的。

陈榕：必须是网站。

韩锋：好用来发布。

叶飞：本身一个应用就是一个轻节点，对用户来说，也不一定知道节点的硬件。

陈榕：他就不知道。

韩锋：继续。

辕询：所以我就解释，4个大目标，4个次要目标。

叶飞：是这样的，刚才大概听了一下，而且之前业界看过白皮书，这时候比特币区块链，我们研究发展了七八年，现在基本上分代，一代、二代。本质的区别，像刚才我大概总结一下，一代的话，比特币从功能的角度来说，三大模块，央行的部分发行货币，但是也讲到到现在我们有一个自己的发行机制，比特币一点点挖出来，我看了一下比皮书，比特币占一部分。

韩锋：原比特币用户占一部分。

叶飞：就是说这部分的话，技术都没有问题，而且也做了。还有的话，作为一个类似商行部分，支付这块主链是没有问题，侧链也没有问题。还有一点，比特币最重要的就是本身是货币的功能，我们的这套系统里面，亦来币实现了这个功能，我们后来发行的很多资产，可以围绕这个东西去转。一般币里面，其实它的支撑里面，很多的技术基础，也可以分为几大模块。一个是P2P的，这部分的话，比特币之前已经很成熟了，刚才您说的**发行机制**，这几个东西实际上就是在完成这套系统，怎么做防火墙这部分，这部分是可以提升的，但是总体来说有现成的解决方案。还有就是POW，就是共识机制。共识机制的话，我们现在提出来联合挖矿，联合挖矿也是一个很成熟的技术，在这个社区里面。早几年玉米币已经用了，现在狗狗币和莱特也是用，但是我们这个联合挖矿的话，有一个东西要扩张起来，要服务侧链。这部分实际上目前整个技术的社区，应该说研究的比较前沿的是ROOTSTOCK他们，他们快突破了，还有一点点东西，这个东西快能突破，这就解决了主链和侧链的安全问题。

叶飞：他们写了很多论文，提了很多发明，这块的话应该也不是一个盲点，侧链安全问题也不是盲点。然后说**EOS**里面，刚才说的两点以外，还有区块链那部分。那我们肯定的话，第一代都是主链，包括到了现在二代链的话，全部都还是主链。下一步我觉得肯定区块链往前发展，肯定以网络的形式，一条链肯定是不够的，侧链肯定是要有的。侧链和主链的核心问题，一个是安全的问题，一个是侧链和主链之间的交互问题，有多大的交互，交互的附加力度，主链的币能不能留在侧链来，以什么样的形式留过来，侧链能不能回去。

韩锋：是锁定，一般冻结，然后那边等于记帐。

叶飞：包括这个冻结式，真正的链上冻结，还需要第三方都有这样的方案，比如说**ROOTSTOCK**，他们提出有点像借助一个什么基金之类的冻结了。甚至就是说我们搞一个多签字之类的，有一个同意才能解冻。当然，这个在技术上也可以完全做到。

韩锋：我们现在有具体方案吗？比如实现这个，从主链到侧链的那个。

辕询：主链到侧链，有一个我们能实现的，用**ROOTSTOCK**的方案，把特殊的指标放到应用链了，你要一次性的能先转钱。或者把这个钱锁住，然后侧链那些人同意的时候，那个钱再解锁。

韩锋：冻结方案？相当于一个借贷模式？

叶飞：其实在某些使用上，比特币已经允许这个，因为原来造比特币的时候，是想造一个这么的系统的，比特币里面包括力很小的，但是我看到以太坊，把它丰富了。智能合约系统已经能让人造一个微支付渠道。

辕询：不用闪电网络，要是2个人想**反浮**的。甲方向乙方反浮的，或比如说他要付钱10次，每次都是比较小的，它是有一个方式来合并十次，为了只交一次的交易费，这个现在已经能够实现，通过比特币，用它自带的系统。我们稍微把这个延长一点，让它锁住，另一个链上，要是有某个接管的话，钥匙会出完，然后就解锁了。

叶飞：比特币其实有脚本系统，因为我们知道只要**脚本**有完备性的东西，有存储器什么都可以做到。比特币一开始是这么设计的，后来一点一点禁掉了，只留了几个明链。

韩锋：把那个封掉了。

叶飞：后来他觉得不太安全，原本是这样的。

叶飞：后来以太坊相当于，反正全部放开了，重新开发的。

韩锋：但是主链受不了了！我觉得叶飞分析的比较到位，主链从比特币到以太坊都是主链思维，未来的第三个发展阶段，我觉得应该以侧链思维去发展。

叶飞：侧链也是从2015年开始研究，应该说很多东西都突破了，所以我们现在提出来操作系统的层面，肯定思维上要变了。你看我们现在所有的东西，所有的应用，其实我们现在解决的核心问题就是互联网和区块链关系的问题。现在你看多少的应用，全部都是放在操作系统上，操作系统对互联网完全是开放性的，安全各个方面的话就比较全面。我们要做这个东西的时候，互联网变成了我们区块链的资源，本质上要这么去做。就像我这个区块链，这是我现在的操作系统，读内存也好，读硬件也好，读互联网也好，在逻辑上要有这么一个变化。

再一个就是突破主链的侧链，我现在最核心的问题，主链和侧链一个是安全的问题，有一点点东西其实还不是那么清晰。主链和侧链之间的分工，有多大的饱和性和挂钩，这个币能不能流回来，怎么流回去，因为你要知道，如果技术上流可能有流回去的。如果这样的话，意味着主链无论怎么样，区块链这个东西呈现分布式帐单，你只要知道所有的数据，其实就能做所有的判断。所以说当你有这么多侧链的东西，除非你这个主链，你那个节点，拥有侧链所有的数据。

韩锋：那几乎是不可能的。

叶飞：不可能的。

韩锋：所以防止不了很多攻击，我是听到有一些分析，徐刚这个事还是分析过的。

叶飞：确实是这样，我们一定要定义主链要做什么，侧链要做什么，权限跟付出是一模一样，肯定是对等的。所以说核心解决这个问题，智能合约的话，我觉得以太坊的这套东西，也挺成熟的。尤其他们的**智能合约**，是可以移过来用的，很多项目可以自己移过来用，当然肯定会优化。

辕询：我刚才又计算了一下，为了看一个节点的成本。因为我们是想把这个降到越低越好。我在颗粒方面上一直在交互，看到颗粒方面上，我是在去掉所有**函数**，因为这个是增加安全和存储的成本，而且它是用比较动态的连接来把这个程序和**函数，**联结在一起。我们要用静态连接，所以就会减少函数的量。硬件现在变得越来越便宜，硬件的基础PI，是远远超过软件的，在我们世界上。就是说现在的处理器什么东西，非常高级又省电。两年之前有一个很小的机器，socket非常小的，完全都是**图灵**完备的，可以计算东西的机器，就卖一个5英镑，一个5美元好像。但是当时它卖的价格，还是少于实际的市场价格。我们知道这个，因为它一公开的时候，几乎都卖完了。但是现在又过了两年，我们要是有一个手机版本，各种休闲的用户就能开始安装，就能开始连到网上，所以我们有一个免费的手机版本。但是如果我们想出一个节点硬件，我估计也能达到100人民币之下，一年成本，为一个节点。比如陈榕先生说某些公司，要合作大的公司。通过这些，要是在协议中能让他们一些节点，提供一两个机房，机器的房间里面用好多100元的钞票，每个都相当于一个节点，其实一个公司进入这个项目，就能提供1万个、几万个节点，都可以。

徐继哲：NAT穿透的目的是什么？

辕询：穿透的目的是让非商业的用户，能连到节点网上。现在非商业的用户，他们的节点只能下载，不能上传。这是比特币的一个技术缺陷，但是通过陈榕先生和他的团队以前的那些技术，我们是可以修改的。所以一个节点成本少于100块。

陈榕：基本上假设某个小硬件，在35美金。我知道你说的那个，非常简单了。为什么提到**这个硬件呢**，我们现在别假设那么**大的硬件**，一百块。一个**小的硬件**大概现在30-35美金，300块钱以内。我觉得100块钱有点**多**，我最近这几年做过一些智能路由器什么的，因为我们要跑**程序**的话，假设我们的小硬件就已经能跑了。根本不用再大硬件上跑**。**因为五年前启动这个项目的时候，其实提供两个最基本的问题，刚才讲的下面我们会提供P2P，这些NAT的东西。第二我们能够提供的，当时做这个的目的是为了所有智能家居，做智能路由器是希望智能家居这些东西都不能上网。我们把以后的轻节点，就是刚才大家讲的微网站，跟合作伙伴做过智能路由器当小家庭服务器，你插个硬盘，或者插一个**声**卡，就是一个个人云盘。这个东西最主要在说程序，肯定给你一个虚拟机，这叫Virtual Machine（EVM）。这个EVM，我们给你的是C++版的，是一个原生代码，不是一个脚本的。第二这个虚拟机里面，我们会静调你的上外网的能力。这个时候，也就是说你在家庭微网站里面，或者手机这一端，两边都不能直接打开**外网**，你这两边通道的建立，全部是自动生成RTC，这个网络用户是不可能发起50：39，刚才讲到如果说这里面做了去中间人，你本部做一个轻节点，确实你访问多少节点和网站了，这个时候不用找一个Domain Name System（DNS）去解析.COM，你就自己解析IP地址在哪了，P2P就到了我要访问你的电子书，我直接到了你个人的云盘。这两边是没有可能，应用和服务都不允许直接去访问过去，全是通过操作系统间接访问。这样的话，做中间攻击，你只能说我要找免费的网站，你既然说找一个免费的网站，我操作系统帮你找，就像我打你手机似的，找到你的网站。不可能把这个软件包发给元寻的网站，所以我这个机器根本没有东西，不可能把这个包发到元寻的家里去，要不然除非是说我这个要找元寻网站，元寻直接在我手机上放一个白名单，直接放到这个网站，电话不接。所以这个包直接送不导，就是这么简单的道理。

其实这件事，如果我们假设微网站，这个事可以迅速做。如果你假设其他的类型就掰不上去。因为重量、计算能力，辕询能听懂我在讲的这些话吗？中文。所以我觉得我们第一步别那么**少**，说100块钱，我们说300块钱吧。因为300块钱对于一个家庭来说也还好了，做一个微网站。

陈榕：这个东西几乎是没有做的，我们现在只能给你一个非常原始的**虚拟机**跑起来，跑起来就是说有一些服务，C++可以跑，这个时候C++跑，java也可以跑，你也可以跑一些类安卓的**程序**，当时安卓主要由[Andy Rubin](https://baike.baidu.com/item/Andy%20Rubin)发明的，安卓来做**手机**，有人开始做了，在世界上，叫Android操作系统。用安卓做手机，挺幽默的，没投安卓。有人在做一些研发，但是不是很成熟，基本上就是说在这上面能跑到**简单程序**，其实简单就是说你别想今天的新浪网的网站，但是我有三本电子书，能做一个什么东西，让手机导航有一个界面，先从简单说，把这个叫做微网站了，这个不是很难。但是有没有一个特别标准的规范行为，目前还没有。但是能不能比如说这个微网站，我们能够比较快的将程序跑起来，能把这个端到端，现在我的公司实际上就是原来一个很大的大款赞助做开源，后来那个大款后悔了。在智能家居有三大阵营，一个阵营大概是苹果，叫homePad 。还有一大阵营，说起来也挺邪门，高通、微软、因特尔。高通、微软、因特尔三个加起来是一个阵营，叫Cortana，是原来高通的一套协议，但是后来谷歌和微软都加盟了。实际上不是用户找，是我帮你，基本上能做通，还没有走到很顺。

徐继哲：也就是P2P在里面占很大的部分。

陈榕：P2P其实已经基本成熟了，但是还要从虚拟机导到另一个虚拟机，上面还有一些东西。如果整个的工作是这样，如果说是百分百的话，其实大概70%是已经做了。

陈榕：更多的我觉得区块链是做承受我们系统内的一个基础设施，基本上想法是说把区块链，怎么能够创建一个侧链，将来展现给用户，展现给系统程序员的话，这是几个简单的调用，形成一个侧链。其实我开始的想法，甚至主链和侧链的币是不通的，我觉得最简单就是不通。但是让操作系统可以很容易让，比如上面写了一个应用，我们叫德州扑克，德州扑克很容易的几个指令就能发出德州扑克的筹码。我们两德州扑克打完，我们赢一点筹码。

陈榕：不是，有一些里边的一些是联盟链，像我们和比特币联合挖矿，他们的那些寄完的哈希，又寄到我们这个链上，钱并不导，只是说做一个德州扑克，德州扑克发行筹码，我们不是说赌人民币，也不是赌亦来币，我们赌的是德州扑克币，就是拿着筹码玩嘛，你说真见钱，就看社区怎么经营了。我们赌这个，当时我们两发牌也好，币也好，德州扑克币，只是说这个节点记在装我们游戏的这个机器上了，这个东西每一个**交易**哈希，又记在亦来币上，亦来币的每一个节点，又记在比特币的矿机上，只在记录上不可篡改。因为比如说一个德州扑克币节点只有几十个，或者怎么样，看玩多大了。容易攻击性也好，易篡改性也好，是不是要保持十年的记录，没准三年就把前三年的给扔了，这个策略可能截然不同。但是起码在这个三年内，这个链的哈希是不容易被篡改的。只是这个哈希记录了，这个钱中间不导，钱中间不交易。

陈榕：所以我是觉得现在第一期的时候，没有想清楚的时候，这两个链先不要把钱扯上去，先不要把亦来币和德州扑克币，别这边打到那边，那边打到这边，先把不可篡改性避规的做到比特币的那个，所以我挺同意韩锋老师讲的。韩锋说的我们这些矿机，在四川的POW，实际上就是相当于诚信的根，然后大家就是一层一层往下，你的根，比如说德州扑克的**交易**，记在亦来币的**节点上**，亦来币的**交易**，又记在比特币的**账本上**，比特币又通过**吴忌寒**的矿机来保证的，一级级先把这个事了了。其实我们先说，第一句我们做一个亦来云，实际上就面向这种，所有亦来币的网站都是我们的轻节点重节点。这个时候，亦来云呢，实际上想做一个，刚才跟大龙在讨论这个名字。这个互联网上的网站，大家就不像传统互联网的网站，这个网站是真的吗？这个人的用户ID是真的吗？发布的内容是真的吗？起码有可能这个电子书是假的，有可能是网站的，但是起码这个网站就剩下我要发的网站。比如说这个网站挺好的，陈榕你去看看吧，你发我一个SHA256的哈希，我拿着SHA256的哈希上了那个网站，那个网站内容你并不能保证是真的，但是你给我哈希访问的一定是那个网站，不是说有个人直接进入网站，这个网站不是那个网站，这是一个很简单的问题。网站是真的，人是真的，里面的内容是真的，这已经是很大很大的**进步**。先不扯钱怎么着，在中国也敏感。

韩锋：最好是这样，别以后我们动不动硬分杈 。宏观的分析，我特别赞赏叶飞的分析，他基本上梳理得更清楚了，我们的整个思路。为什么一个是操作系统，一个是区块链本身第三阶段的发展，也开始清晰起来。前面因为你已经犯了这么多矛盾，自己没有办法解决，下一代也要设计一个能解决的，要不弄下一代干什么。而且叶飞也明确指出，大的技术基本上已经解决了，小的盲点肯定要自己解决。总的来说，我们要进入第三代，第三代EOS已经挑头了，但是这个头太贪婪了，自己在金融上会有问题。这个我不多说了。

我们准备走一个慢牛的道路，一点一点起来，不求一下子募集几个亿美金，好像要把社区搞得天翻地覆，我们一点一点来，不断展示我们的技术，展示我们做到什么，展示我们的应用。从哪怕私募，一个亦来币也才20多块钱。对标比特币的话，如果未来真可能达到比特币所谓的市值，哪怕10%都将近2000块钱，这个空间是非常巨大的，不用那么着急去炒。哪怕三四年以后，能达到1000倍，这已经是不得了。所以一点不用着急。

徐继哲：我对这个行业的判断，无论我们做到做不到，下一步肯定有一个东西出来，很快就会超越。发布应用也不是现在立马受到瓶颈，以太现在已经立马受到瓶颈了。要达到这个目标的话，侧链肯定会用上，这个思路就是说，这个应用以侧链的形式，这个应用有自己的寿命，有自己的安全方式，就是说不影响主链那么多，本质是这样。

叶飞：这个我同意了。

韩锋：更根本的有一个操作系统，才真正让应用都落地。

陈榕：现在包含了到目前为止，我们提出了所有概念，比如说像刚才说的这些侧链，实际上就是轻节点、全节点，也就是说未来会有很多节点，但不都是全节点，有一些轻节点，重节点，这些节点的应用，就是这样一点点把功能划分出来，以后安全性各个方面定义好了，真正到应用当中去运行，实现它的功能。就差这个东西，下一个阶段就是这样。

（后略）