安全共享网络及
基于信用认证的共识网络

2020.09.30

Version 2.0.2

执行摘要

这篇白皮书陈述了 Deeper 项目的产品应用场景，技术框架及其实现细节。Deeper 项目分为安全的网络资源共享平台，真正去中心化的共识网络和可信互联网开发平台三大阶段。目前安全的网络资源共享平台已经开发完毕，经过一段时间的公测后，我们将于 2019 年初正式发布一款名为 Deeper Connect 的智能安全硬件。它对于用户来说既是一款网络安全设备又是一款能盈利的网络资源共享设备。在不久的将来，所有用户的 Deeper Connect 可以通过 Deeper 独创的 PoC (Proof of Credit) 共识机制，组成一个真正的去中心化共识网络，而该网络可以进一步作为可信互联网的开发平台。Deeper Connect 是第一个结合了网络安全技术，网络共享经济，以及区块链技术的新物种。

Deeper Connect 的设计理念是即插即用以及零配置，让用户无门槛的享受网络安全技术所带来的保护。用户不需要任何专业知识或使用说明，而只需要用网线将设备连接在调制解调器和路由器之间就可以使用。而这个简单的操作能够为用户实现突破网络干扰，防御网络攻击，流量控制，家长控制，分享网络带宽盈利和区块链挖矿等功能。

从网络安全技术角度看，Deeper Connect 能够提供一体化的网络安全解决方案。网络安全功能的核心是 Deeper 自主研发的 AtomOS 网络操作系统。AtomOS 是世界上第一个无锁的网络操作系统，它先进的无锁设计是保障整个系统具有高可靠，高性能，高可扩展性的关键。另外，Deeper 独创了三叉戟协议，自适应隧道，智能路由，链路层隧道，以及隧道层拥塞控制等创新技术，来向用户提供更深层次的安全保障和更好的用户体验。

从区块链技术角度看，Deeper 通过智能合约在区块链上实现网络资源共享平台。它主要包括了代币合约，节点合约和微支付合约。我们未来会推出一个全新的智能合约区块链平台 — deeper 链。deeper 链使用 Deeper 独创的基于信用证明 (PoC) 的共识机制来实现真正的去中心化公链平台。同时 deeper 链具备高效率，低能耗，安全性的特点，是新一代的公链平台。在 deeper 链主网上线后，用户所拥有的 Deeper

Connect 在满 deeper 链所要求的最低信用值之后，即可自动参与 deeper 链挖矿。DApp 开发者也可以在 deeper 链上开发诸如数字货币交易平台，社交平台和电商平台之类的去中心化分布式应用程序。这些基于 deeper 链的新型应用程序，除了能满足用户的基本需求之外，还能更好的保护用户的隐私和数据，从而打造个人数据主权得以保障的可信互联网。

目录

1 愿景介绍

随着互联网技术的飞速发展，我们所处的世界正在被一个东西深刻改变 — 信息。早在 1948 年，香农博士就用数学方法量化了信息从而开创了信息论 [62]。互联网出现后，信息得到了前所未有的流通，人们所能获取的信息数量呈爆炸式增长。互联网也革命性地将知识信息平民化，使得高质量的知识信息不再成为少数阶级所拥有。自 2009 年起，区块链技术发展迅猛，更是开启了去中心化的信息自由时代。但是，在技术浪潮的推动下，人们往往只注重技术发展所带来的便利与利益，而忽视了这些技术的应用场景是否被恶意操控，以及这些技术的内在缺陷所带来的严重后果。

1.1 网络犯罪

网络病毒的传播可以说是层出不穷，屡屡给社会造成严重的危害和损失 [68]。在 2017 年，被网络病毒成功劫持并被迫从事数字货币挖矿的计算机达到 165 万台 [51]。而随着物联网 (IoT) 发展起来的物联网病毒，不但能够劫持个人计算机，还可以劫持摄像头，智能家电，智能门锁，路由器等一切联网设备。从 Mirai 病毒 [47] 开始发动攻击到 2018 年中，已经将超过 60 万台联网设备变为肉机 [65]。另一方面，恶意网站发动的钓鱼式攻击通过伪装成可信的法人媒体来获得如用户名、密码和信用卡明细等个人敏感信息 [54]。在 2017 年，卡巴斯基反钓鱼系统触发了 2.46 亿余次，15.9% 的用户成了为钓鱼网站目标 [25]。从钓鱼网站造成的损失来看，在 2013 年 12 月至 2016 年 12 月期间，FBI 在美国境内调查了 22,000 件钓鱼网站诈骗事件，总金额高达 16 亿美金 [45]。2015 年，网络犯罪所造成的损失总计高达 3 万亿美金，而 2021 年将达到每年 6 亿万美金 [48]。

1.2 信息抑制与网络审查

信息抑制与网络审查包括了剥夺用户在互联网上的某些权利 [6]。世界上许多国家出于各种原因封锁了大量的网站 [39][40][72]。除了信息封锁，审查和监视也在互联网普遍存在。这些问题是如此普遍，以至于人们不得不放弃某种程度的隐私，以换取互联网的便利 [75]，并常常在不知不觉中丧失数据隐私权 [31] (个人数据往往被服务提供商控制，甚至出售给第三方牟利 [35][38])。

注：由于不同地区和国家的政策不同，Deeper Network 将对不同地区销售的版本的无障碍特性进行调整和限制，并针对不同国家推出不同版本，以确保 Deeper Network 产品能够适应其法律法规。

1.3 网络信任危机

数据泄露是指私有或保密数据被有意或无意地释放到了不被信任的环境 [13]。从 2005 年 1 月至 2008 年 5 月，有大约 2 亿多条个人敏感记录涉嫌泄露 [14]。医疗机构在 2014 和 2015 年为此损失达 62 亿美金 [55]。在 2018 年，Facebook 和剑桥分析数据泄露事件 [64] 再一次引起了全社会的关注。实际上，全球发生的严重数据泄露事件可谓比比皆是 [41]。高度中心化的互联网带来的信息泄露甚至信息买卖副作用已经让人们产生了恐慌 [66]。基于以上种种问题不难看出，当今互联网并不是一个让人充分信任与依赖的基础设施。相反，它是一个充斥着封锁与干扰、欺骗与攻击的不可信环境。

从 2009 年开始，以比特币为代表的区块链技术迅猛发展。区块链技术的初衷是建立去中心化的信任网络，但是最终因为技术上没有做好充足的准备再次成为中心化控制的网络 [3][29]，沦为少数人牟利的工具。数字货币在利益分配上的严重失衡 [27] 导致了多起人们之前认为只有在理论上才可行的 51% 攻击 [28]，这让很多人开始逐渐丧失对数字货币的信任 [73]。

虽然区块链技术燃起了人们解决网络信任危机的希望，但是由于技术上的不成熟

而又举步维艰。鉴于当今严峻的形势，Deeper 决心尝试利用多年来在硬件设计，操作系统，网络安全以及区块链等领域所累计的技术和经验来改变这一现状。

在深入阐述 Deeper 项目的细节之前，首先请大家和我们一起先来了解一下 Deeper 所秉持的理念。Deeper 产品中的所有技术都是围绕着这些理念而打造：

1. 我们认为，有必要让信息的流转不受到技术干扰导致无法自由访问互联网，让全人类实现真正的信息共享。

2. 我们认为，区块链技术的价值是为普通人赋能，而不是用来作为少数人牟利的工具。一个真正去中心化的共识网络必须是每个人都能够参与且能从中获益的平台，它应该是为整个社会而不是中心化的组织或者个人服务。

3. 我们认为，如同房屋，土地，存款一样，个人数据是属于公民的私有财产。私有财产神圣不可侵犯，Deeper 的终极使命是结合安全技术和区块链技术打造个人数据主权得以保障的可信互联网。

2 项目综述

2.1 Deeper Connect 应用场景

Deeper Connect (图 1) 是世界上第一个集成了安全、共享经济和区块链技术的一体化解决方案。Deeper Connect 硬件设备的设计理念是零配置和即插即用，这样用户就可以轻松地享受 Deeper Connect 所带来的网络安全保护，而不需要专门的技术知识或者复杂的用户手册。用户只需将设备插入调制解调器和路由器之间，接通电源，即可使用。

(a) Deeper Connect 设备　　(b) 即插即用

图 1: Deeper 的安全、共享经济、区块链解决方案

Deeper Connect 通过搭载 Deeper 自研的网络操作系统 AtomOS 来实现对外的各种服务。除了这套硬件解决方案以外，我们还提供了一套基于虚拟化技术的软件解决方案 *DVM* (Deeper Virtual Machine)。DVM 在 Virtualbox [70] 提供的一组虚拟硬件上运行 AtomOS，并提供与 Deeper Connect 完全相同的服务。任何支持 Virtualbox 的操作系统都可以运行 DVM，这其中包括 Windows、MacOS 和 Linux 等主流操作系统。使用 DVM 解决方案时，用户的网络流量可以通过 DVM 助手重定向到 DVM，再由 DVM 转发至互联网。

接下来，我们将详细阐述 Deeper Connect/Deeper Virtual Machine 的一些典型应用场景。

2.1.1 规避网络审查

网络审查是指由监管机构或者个人制定的对在互联网上访问或发布内容进行审查和控制 [32]。成功规避网络审查需要复杂的操作和专业知识，普通用户往往无法自己实现。Deeper Connect 通过自动对网络数据进行加密，并寻找 Deeper Connect 组建的区块链网络中存在的隧道传递数据来实现规避网络审查，自由无障碍浏览任何想访问的网络数据并避免被追踪和网络干扰。

图 2: 突破网络干扰，无障碍访问

2.1.2 防御网络攻击

网络攻击是指针对计算机网络或个人计算机设备的任何类型的进攻动作 [12]。诸如网络病毒和钓鱼网站之类的网络攻击可以通过互联网迅速传播，对于用户来说是防不胜防。Deeper Connect 不但拥有全套的防火墙功能，还独创了三叉戟协议、智能路由等网络技术，使得用户可以安全、自由地访问互联网。

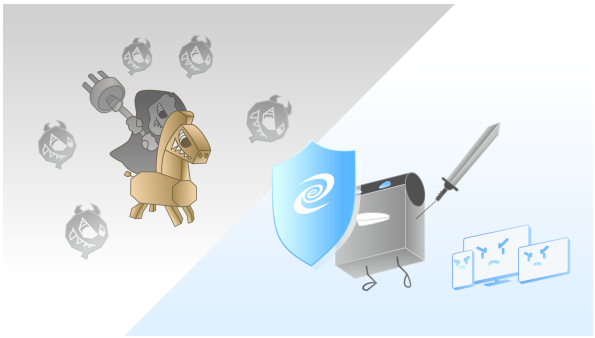

图 3: 隔离网络攻击

2.1.3 家长控制

家长控制是指允许家长监控整个家庭的网络记录或对某些互联网内容实施屏蔽的功能。Deeper Connect 根据网站内容可以将网站划分为不同的级别，以此来适应各个年龄段的未成年儿童。网站级别数据库可以定期的自动更新。如果孩子访问的网站超出了家长要求的级别，Deeper Connect 会根据内嵌的网站级别数据库进行判断并自动切断网页下载，以此保证孩子不会接触到任何不良信息。

图 4: 家长控制家庭网络

2.1.4 漫游访问

漫游访问是指当用户设备不在家庭网络覆盖范围内时，用户只要在设备上设置漫游隧道 [21] 来连通家中的 Deeper Connect，该设备也可以同样得到 Deeper Connect 的保护从而安全，自由的访问互联网。

图 5: 漫游访问

2.1.5 分享网络带宽盈利

用户可以通过 Deeper Connect 将家庭网络带宽分享出一部分作为公共带宽以此来换取数字货币 DPR — 分享即挖矿。网络带宽共享其实就是一个 Deeper Connect 节点做其他 Deeper Connect 节点的远程网络代理的过程。如果分享的家庭网络节点带宽被他人使用，使用者需要按流量和网速向提供者支付数字货币 DPR。同时，Deeper Connect 的网络隔离以及网络过滤功能将杜绝各种由于分享所带来的安全隐患。此外，用户可以灵活地调配共享宽带的网速和时段以保证带宽共享不影响自己的正常网络使用体验。

图 6: 分享网络带宽来盈利

2.1.6 区块链挖矿

用户可以把 Deeper Connect 作为矿机在区块链上挖掘数字货币 DPR。未来我们将推出基于信用证明 PoC 的区块链共识网络 deeper 链，而矿工基础将是所有 Deeper Connect 用户。全球所有 Deeper Connect 会根据我们定制的安全网络协议自动匹配成一个 P2P 网络，进而升级为一个区块链共识网络 — deeper 链。拥有 Deeper Connect 的用户都可以在 deeper 链上挖掘数字货币。

图 7: 区块链挖矿

2.1.7 分布式应用商店

在 Deeper 项目的第二阶段，我们将推出图灵完备的区块链公链 — deeper 链。我们将在 deeper 链上开发 DApp 并且加入 Deeper 的分布式应用程序商店。DApp 开发者可以在 deeper 链上开发诸如数字货币交易平台，社交平台和电商平台之类的分布式应用程序。全球所有 Deeper Connect 都是这些应用的算力和存储基础。同时，普通用户也可以通过 Deeper Connect 方便的获取和使用各种 DApp。

图 8: 分布式应用商店

2.2 Deeper Connect 网络

Deeper 的价值不仅仅在于其推出的硬件设备，更在于这些设备之间互相连接所组建的网络平台。其具体表现形式为：

- 安全的网络资源共享平台
- 真正去中心化的区块链共识网络

- 可信互联网的开发平台

梅特卡夫定律 [63] 指出网络的价值是与该网络中节点数量的平方成正比的。因此，随着 Deeper 硬件设备布署数量的增长，设备之间所构成网络的价值将会成指数增长。

2.2.1 安全的网络资源共享平台

共享经济在这几年尤为火爆，使得像 Uber[61] 和 Airbnb[67] 这样的独角兽迅速都超过了百亿的市场估值。不过令人震惊的是，虽然 Uber 成为了全球知名的打车平台，但是它没有拥有任何一辆汽车；虽然 Airbnb 成为了全球知名的民宿平台，但是它并没有拥有任何一个房间 [22]。同样，Deeper 既不拥有一根网线也不拥有一台服务器，但是用户之间可以通过 Deeper Connect 来搭建全球互联的网络资源共享平台从而获取自己所需要的网络资源。

在项目初期，网络资源共享平台的各种功能是通过以太坊 [18] 上的智能合约来实现的。未来，它将被迁移到 Deeper 自己的区块链 deeper 链上以保证项目的持久发展。通过智能合约，使用共享服务和提供共享资源的交易双方可以根据各自需求迅速匹配并建立端到端的加密连接。双方在对服务质量和服务价格达成一致后，便可以正式开启网络共享交易。一方通过支付 DPR 来获取网络资源，而另一方则提供网络资源来获取 DPR。DPR 在交易过程中充当了一般等价物的角色。

为了维护一个能够持续健康发展的网络共享经济体，我们也采取了一系列可靠措施来保障共享经济平台正常运作。交易双方采用概率微支付以抵御双花攻击，用户赖账和服务器不作为等违约现象。我们也通过智能合约代码实现了一系列共享平台维护措施，从而屏蔽恶意服务器和恶意用户，防御女巫攻击以及保障服务质量。

2.2.2 区块链共识网络

区块链技术这几年发展极为迅速，造就了多个像比特币 [5] 和以太坊 [19] 这样动辄市值百亿甚至千亿美金的数字货币。然而很多人并不看好数字货币的未来，认为这只是

市场疯狂炒作的结果 [24]。难道数字货币真的一文不值吗？这个想法显然忽略了区块链技术带给我们的核心价值 — 解决信任问题的去中心化共识机制。

Deeper 项目的价值之一在于其独创的信用证明 PoC 的共识机制，我们将运行该机制的区块链命名为 deeper 链。在 deeper 链主网上线后，全球所有 Deeper 硬件设备会根据我们制定的安全网络协议自动映射成一个 P2P 网络，进而升级为 deeper 链。Deeper 硬件设备的所有用户将转化为 deeper 链的矿工。从公平性的角度来看，虽然共识网络的初衷是去中心化 [49], 但是采用算力证明 PoW[34] 和权益证明 PoS[37] 的数字货币最终往往还是被少数人主导 [69]。而 deeper 链将采用去中心化的随机算法 [9] 和信用证明 PoC 从根本上解决用户的公平性问题，从而建立一个真正的去中心化共识网络。从运算效率上看，因为不需要浪费算力去竞争挖矿而且采用分片技术 (Sharding) 和随机任务分配技术，所以全体网络节点可以高效的并行运算数据，这大大提高了整体网络效率。从能耗角度来看，deeper 链矿机 (即 Deeper Connect) 的最大功率为 15 瓦远低于传统 ASIC/GPU 矿机的功率，这又大大减轻了用户运行成本。不仅如此，通过我们制定的信用积分算法，deeper 链可以抵御女巫攻击，日食攻击，预防 51% 攻击等常见的攻击手段。

2.2.3 可信互联网开发平台

如前文中所提，互联网用户数据泄露事件频频发生。全球用户在享受互联网便利的时候，也产生了大量的用户数据，而这其中很大一部分数据是属于用户的隐私信息。目前用户大多依赖于互联网公司对其隐私数据的保护承诺 [2][23]。然而互联网公司实际上也往往默认或仅仅告知一个简单的用户隐私协议 (用户如果要使用其服务，也别无选择)，却可以拥有一定程度上浏览甚至出售用户数据的权限 [35]。难道用户对自己的数据就不能拥有主权吗？

Deeper 项目的终极愿景是打造一个用户拥有个人数据主权的可信互联网。它是基于我们前文所提的 deeper 链实现的，因为其本质上是一个去中心化的不可篡改的分

布式数据库。这个由所有 Deeper 硬件设备组成的可信互联网具有数据保密属性，用户匿名属性和网络安全属性。社交网站，电商平台等各种互联网应用都可以在可信互联网中得以重新实现。就数据保密性而言，用户再也不需要寄希望于互联网公司的数据保护承诺，而是将个人数据用非对称加密技术 [57] 加密后保存在可信互联网。用户可以自主选择拥有浏览其数据权限的用户，而没有权限的用户由于无法解密而无法偷窥数据，这保护了用户的个人数据主权不容侵犯。就数据完整性而言，用户再也不用担心数据篡改或丢失。可信互联网的数据存储采用哈希树 [46] 来实现，哈希树的每一支都将被无数节点同时保存。即使仅想篡改某一个用户信息的一个比特，都需要改变哈希树某一支上的所有哈希值，而这对于任何攻击者来说都需要付出难以承受的代价。

3 硬件设备

Deeper 旨在用即插即用的安全硬件来解决安全、共享以及区块链领域的复杂技术问题，为用户提供一体化解决方案。下面我们将带您领略 Deeper Connect 安全硬件设计的一些特色。

3.1 跨平台

Deeper Connect 旨在兼容不同的硬件平台。AtomOS 已经成功地在 Intel 和 ARM64 处理器上运行，这使得 Deeper 能够充分利用这两种平台的优势 — Intel 处理器的强大功能足以处理各种高负载网络情况，这使得 Deeper 不仅能够满足家庭网络的复杂使用情形，同时也可以满足企业级的应用需求。另一方面，ARM 平台以低能耗、低成本著称，足以满足日常家庭网络需求以及各种移动应用场合。在未来，Deeper 还计划推出基于 ARM32 的产品，这将进一步降低硬件成本。

3.2 低功耗

根据 digiconomist 的评估 [4]，全球比特币挖矿耗电 1.88 亿千瓦时，相当于年耗电 688.1 亿千瓦时，是 2017 年 5 月耗电水平 (115.7 亿千瓦时) 的 6 倍。全球比特币挖矿总耗电量相当于捷克一个国家的耗电量，占全球电力消费的 0.31%。平均每笔比特币交易耗电 968 千瓦时，相当于美国 32 个家庭一天的用电量。目前比特币全年碳排放为 3,385 万吨，平均每块比特币需要排放 1,300 公斤的二氧化碳 [44]。

由 Deeper 独创的 PoC 共识算法可以从根本上解决这个问题，PoC 共识算法可以让设备以极低的运算量参与网络共识。Deeper Connect 选取低功耗的嵌入式处理器来打造我们的共享和共识网络。我们已经设计完毕的 Deeper Connect 的最大功耗是 15W，下一代便携式产品 Deeper Connect Mini 最大功耗仅 5W。搭载 AtomOS 的 Deeper 硬件是市面上性能功耗比最高的安全产品 (与普通的 ASIC/GPU 挖矿设备相

比，能耗降低了大约三个数量级)，未来 Deeper Connect 也有可能成为收益功耗比最高的区块链矿机。

硬件类型	功耗
Deeper Connect	5∼15W
ASIC 矿机	2,000∼3,000W
GPU 矿机	1,000∼2,000W

表 1: 不同类型矿机的功耗对比

3.3 加密货币的硬件钱包

Deeper 的安全硬件集成了加密货币钱包功能，旨在为没有任何区块链以及安全相关知识背景的用户提供最高级别的加密货币安全保障。

Deeper Connect 通过 AtomOS 提供的多重安全保障，使得黑客和恶意组织无法远程获取对硬件的控制权限，从而无法更进一步获取存储在设备上的密钥信息。同时恶意攻击将被识别和记录，为今后进一步破获网络犯罪以及抓捕黑客做好准备。

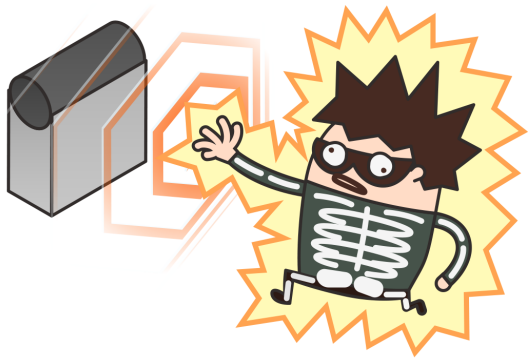

图 9: 黑客对 Deeper Connect 的恶意访问将被阻止并记录

Deeper Connect 采用了三重加密技术来保证其存储设备的安全。即使用户的硬件

设备被盗取，他人依然无法破解设备上存储的密钥信息。所以，Deeper 的存储设备将具备极高强度的保密性。接下来分别阐述 Deeper 的三重加密技术。

3.3.1 块设备加密

当用户的存储设备被盗取后，黑客可以通过分析块设备上的数据来获得重要的文件。Deeper Connect 通过对每个磁盘块进行 AES-CBC [20] (图 10) 加密使得黑客只能得到加密后的数据，从而极大增大了其破解难度。

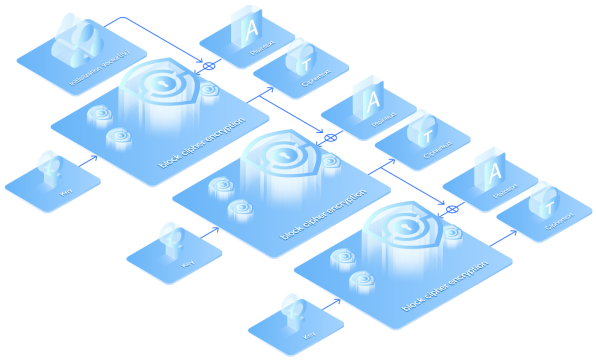

图 10: Deeper Connect 对磁盘数据块进行 AES-CBC 加密

3.3.2 文件系统加密

单纯使用块设备加密技术并不是万无一失的。为了进一步保护我们的存储介质，Deeper 对通用文件的关键元数据以及普通数据的组织方式进行了重新组织，从而实现了 Deeper 自有格式的文件系统 — DeeperFS。由于 DeeperFS 的数据结构严格保密，使得黑客无法从块设备中获取文件系统的结构信息，从而无法更进一步获得存放在文件系统中的关键文件 (图 11)。

图 11: 加密的文件系统将保护磁盘文件不被提取

3.3.3 文件加密

Deeper Connect 设备上的所有重要文件都是经过 AES-CBC 加密后存储在文件系统上的。所有文件的秘钥是固化在 Deeper 的应用程序的内部，只有 Deeper 的应用程序才能够打开获取到这些数据的明文信息。

图 12: 三重加密技术将保障 Deeper Connect 的数据安全

3.4 安全矿机

2018 年 5 月 28 日，以太坊被发现“致命报文”漏洞 (CVE-2018-12018)[53]，攻击者通过发送一个恶意报文即可向 geth 节点发动攻击。geth 是以太坊主流的官方客户端，

对于以太坊至关重要。有大约 70% 的节点运行在 geth 之上，包括交易所和矿池这些关键节点。通过这个漏洞，攻击者可以直接让以太坊瘫痪。一旦成功，以太坊市场将面临巨震。

目前的矿机产品都没有在安全上引起足够的重视。但我们可以想象，如果黑客能够利用挖矿软件或者矿机自身的漏洞来进行攻击，那么该矿机所承载的区块链的价值也将大打折扣。Deeper 的所有产品都自带安全基因，都是经过精密设计并且反复进行安全论证与测试的。运行 AtomOS 的 Deeper 安全硬件将是有史以来最安全的矿机，Deeper 的安全矿机将最大程度上保护 deeper 链的安全，同时也能最大程度的保护矿工的利益。

图 13: Deeper Connect 自带安全基因将为 deeper 链提供额外防护

4 操作系统

Deeper 的软件架构由数据平面，管理平面和控制平面组成 (图 14)。其中，数据平面负责用户数据包的收发与深度检测，它是由 Deeper 自主开发的 AtomOS 来实现的。管理平面负责为用户提供友好的使用界面，方便用户监控系统运行或更改系统设置。控制平面负责设备与区块链之间的交互，设备之间的交互以及区块链共识等功能。

图 14: 软件架构图

本章重点介绍 AtomOS，它是为网络深层安全而特别打造的网络操作系统，也是世界上第一个无锁的网络操作系统。它先进的设计是保障整个系统可靠性，高效性，安全性的基础。下面我们将从数据包收发，数据包调度和数据包深层检测三个部分来简要介绍 AtomOS。

4.1 数据包收发

数据包收发属于 AtomOS 的 I/O 层，它是决定用户数据流延迟和吞吐速率的关键技术之一。传统的操作系统利用内核网络协议栈收发数据。这个方法的缺点是高延迟和低吞吐。当数据包经过网络传输到达设备后，它需要经过网卡，网卡驱动，内核网络栈，Socket 等一系列中间处理才能抵达程序开始真正处理 (图 15)。另外，这个方法还会导致频繁的上下文切换和大量的中断处理，进一步加剧了数据延迟并且降低了吞吐速率。

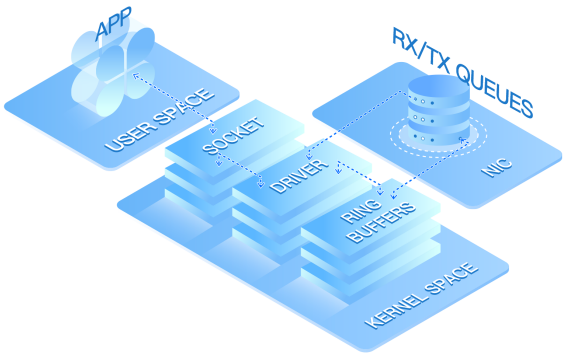

图 15: 传统操作系统数据收发

AtomOS 采用了零拷贝技术直接从网络设备上获取数据包 (图 16)。这不但绕过了繁琐的 Linux 内核网络协议栈，也避免了频繁的上下文切换以及大量的中断处理，从而大大降低了数据延迟并提高了吞吐速率。AtomOS 采用 Intel 发布的 DPDK[16] 开发套件来实现数据包的零拷贝。根据 Intel 提供的实验数据证明 DPDK 能够将吞吐速率提高 10 倍 [17]。

4.2 数据包调度

AtomOS 是采用独创的 HIPE 数据结构开发的世界上第一个无锁的网络操作系统。它将网络操作系统的设计难点通过 HIPE 一并解决，从而实现了 AtomOS 的设计哲学：

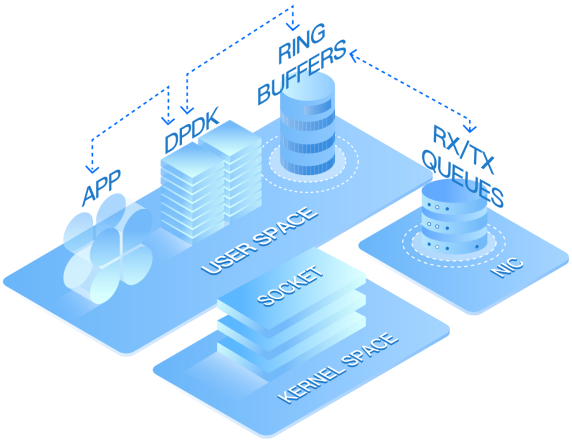

图 16: DPDK 数据收发

简单，高效，可控。在详细介绍 HIPE 之前，我们先来看看现有的网络系统存在哪些普遍的需求和问题。

首先是高性能和高可扩展性的需求。随着 CPU 晶体管的体积越来越小，登纳德缩放定律 [15] 逐渐失效。晶体管尺寸缩小以后，静态功耗不减反增，带来了很大的热能转换，加之晶体管之间的积热十分严重，让 CPU 散热成为亟待解决的问题。单纯提高 CPU 时钟频率由于随之而来的散热问题而变得不再现实，所以各大芯片厂商都很识趣地停止了高频芯片的研发，转而向低频多核的架构开始研究。著名的网络处理器生产厂商 Cavium 早在 2012 年就推出了 48 核心的网络处理器 [11]，而 AMD 也在 2019 年量产其 128 线程多核处理器 [36]。多核处理器的发展也为网络操作系统的设计带来挑战。传统的网络操作系统通常基于 vxWorks、FreeBSD、Linux 这些经典操作系统。vxWorks 在设计之初只是作为一个单核的嵌入式实时操作系统，最近十年来已被网络设备厂商逐渐淘汰。Linux 和 FreeBSD 都是基于 UNIX 衍生而来，而 UNIX 最初是以控制系统而非数据转发系统为应用场景而作出的设计。这些经典操作系统先天的设计缺陷使得他们完全无法充分发挥多核乃至众核处理器带来的优势。

其次是高可用性的需求。网络操作系统通常都部署在各种联网设备的边界，一旦网络设备失效，将影响该设备所连接网络中的所有设备的正常使用。因此人们对网络

设备的可用性要求非常之高。一般来讲，网络设备的可用度要求达到 99.999%，即每年只能有 5 分钟的故障时间。由于现在网络设备，尤其是网络安全设备所承载的流量和功能越来越多，想要保障设备的高可用性也变得越发困难。

最后，是数据包保序的需求。当用户访问互联网上的服务时，中间需要经过十几个甚至几十个网络设备。如果这些设备不按照约定对数据包进行保序的话，用户的数据包在经过这么多设备再到达终点的时候将严重乱序。乱序会触发 TCP 协议的拥塞控制算法 [33] 减小 TCP 发送窗口的长度，从而严重降低用户数据流的速度，影响用户的使用体验。正如我们在前面所讲，现在多核乃至众核处理器已经成为主流，多核处理器在对数据包进行并发处理时，虽然能够加快数据的处理速度，但如果处理不当也容易产生严重的乱序问题。如何既能充分利用多核处理器的潜力，又能保证数据包的顺序成为了网络操作系统必须解决的问题。

目前所有的操作系统都不得不用锁 [43] 来尝试解决这些问题。然而锁的设计已经成为了网络操作系统的一个难题。如果锁的粒度设计过大，对于当前核数越来越多的处理器而言，这些大锁会成为整个系统的瓶颈。如果锁的粒度设计过小，虽然操作系统的性能有可能得到提升，但是随之而来的就会引入让开发者最为头疼的死锁以及各种竞态 (race condition) 问题。这些问题如果处理不当，则会对系统的稳定性产生极大的影响。

为了满足以上网络系统的普遍需求并解决传统操作系统的问题，AtomOS 采用 HIPE 数据结构对操作系统的共享资源进行全局调度，既保证了系统的正确性又能让 AtomOS 充分发挥多核的性能优势。接下来，我们简单介绍一下 HIPE 的实现原理。

操作系统的各种共享资源被分为 N 个组。其中大的共享资源可能横跨多个组，小的共享资源则隶属于单个组。每个资源组的访问都是由事件触发。每个需要访问共享资源的事件都会被放入到相应资源组的无锁队列中。当队列中的事件出队时，会自动分配一个 CPU 核心来对其进行处理。由于 HIPE 限制每个资源组相应的无锁队列中的所有事件必须依次处理而不能同时处理，从而实现了对共享资源的保护。由于系统中资源组的数目远远大于 CPU 核心的数目，所有 CPU 核心都可以获得足够的数据

资源去不断处理数据，使得整个系统的性能和 CPU 核数完全成线性关系。

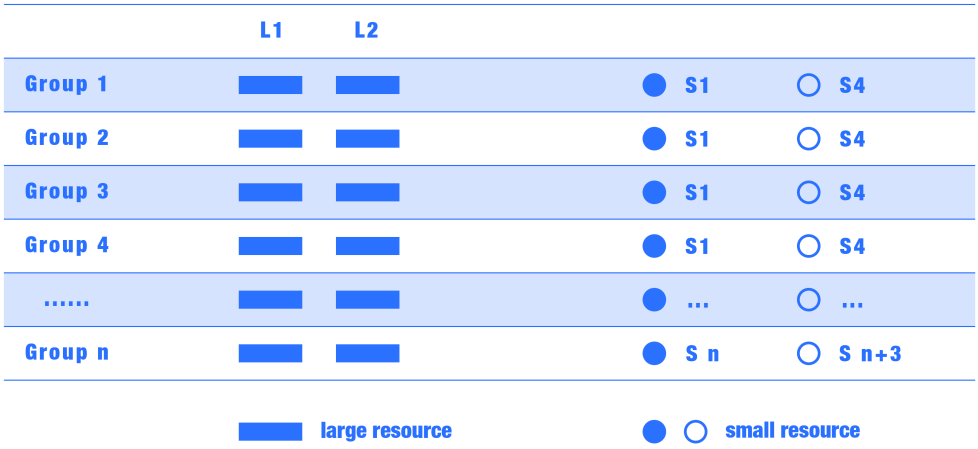

图 17: 操作系统资源被划分为 N 个组

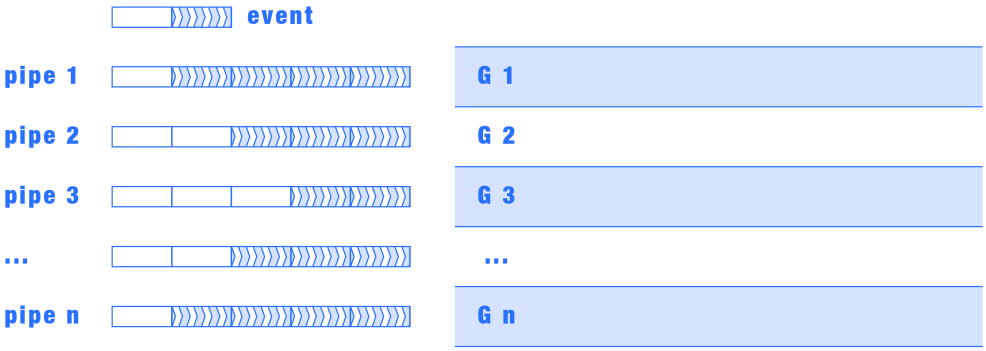

图 18: 对每个资源组的访问由无锁队列中的事件触发

无锁的设计不但使得包处理拥有较高的可扩展性 (scalability)，而且也避免了并发程序同时运行时容易引入的各种竞态 (race condition) 问题。不仅如此，由于数据包是在 HIPE 管道中进行顺序流动，这就保证了经过 AtomOS 处理后的用户数据流内的数据包顺序和原始数据流内的数据包顺序是一致的。

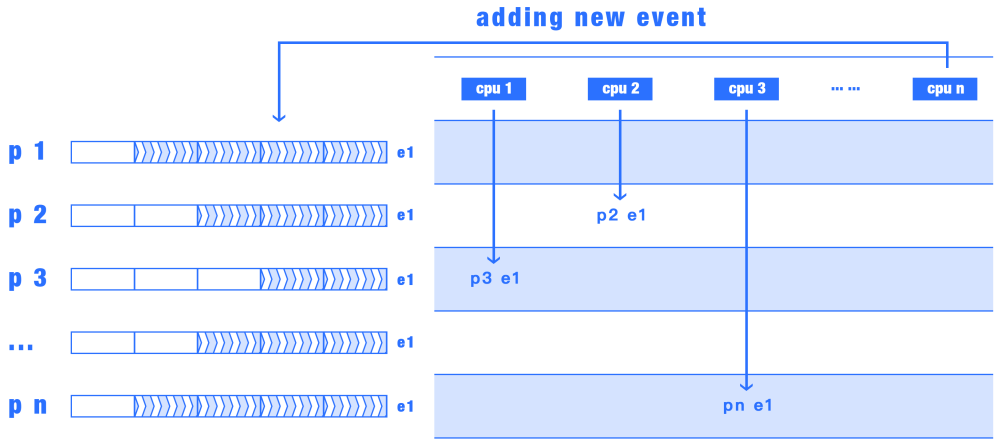

图 19: 每个 CPU 可以同时访问不同的资源组

4.3 数据包深层检测

数据包深层检测是保证用户数据流完全充分保护的关键技术。AtomOS 针对 OSI 七层模型的各个层面都做了相应的连接保障和安全防护 (表 2)，从而使 Deeper Connect 拥有一个完整的防火墙功能。

第七层：应用层	应用识别，恶意数据流检测
第六层：表示层	数据加解密，防止重放攻击
第五层：会话层	HTTP/SIP 等协议会话层检查
第四层：传输层	严格状态检查，防止 Flood 攻击
第三层：网络层	分片攻击防护，IP 欺骗防护
第二层：链路层	ARP 欺骗保护
第一层：物理层	掉电连接保持

表 2: OSI 七层深度防护

现在网络安全的重心已经从低层协议转移到了高层协议，AtomOS 除了对网络 1-3 层做了各种保护之外，还针对 4-7 层重点实现了以下高级防火墙功能：

- 严格的 TCP 状态检查以防止可能的 TCP 伪装和劫持：对于每个 TCP 连接，AtomOS 都会在会话表中跟踪其状态，只有严格满足 TCP 状态机的数据包才继续转发。同时在实现上参考了业内权威的 NSSlab 防火墙测试用例，以保证已知的各种 TCP 逃逸方法不能成功。

- 应用程序识别和流量控制：AtomOS 内集成了一个稳定高效、可扩展的应用程序识别引擎，可以识别常见的家用流量并根据需求进行流量控制或者智能路由，保证用户的关键应用的上网体验的同时，保证在对外提供隧道服务时不会占用过多的本地资源。

- URL 过滤：AtomOS 可以对恶意网站 (包括恶意软件下载、钓鱼网站等) 进行自动过滤，保证用户安全的上网环境。用户也可以根据需求启用家长控制功能，根据家庭成员的不同，来区分可以访问的互联网内容。

- 网络地址和端口转换 (NAPT)：默认情况下，AtomOS 尽可能不对内部流量进行网络地址和端口转换，目的是尽可能维持网线式零配置上网。某些情况下，根据需要，AtomOS 也可以完成对称模式的 NAPT，进一步隐藏用户的内网结构。

5 网络技术

除了前文所介绍的网络深层安全功能之外，Deeper 还独创了三叉戟协议，自适应隧道，智能路由，链路层隧道以及隧道层拥塞控制等创新技术。向用户提供最深层次的安全保障和更好的用户体验。

5.1 三叉戟协议

Deeper 的隧道技术的核心是实现自由无障碍访问互联网，这是由三叉戟协议来实现的。互联网访问审查是对用户的上网流量进行全方位的监视和过滤 [32]，依靠在核心网络和关键出口部署大量网络防火墙和离线分析设备来实现的。所以，为了介绍三叉戟协议的穿透性，我们先来回顾一下网络防火墙的工作原理。目前，网络防火墙从初级的基于端口的访问控制表模式已经进化到基于内容识别的智能模式。这个模式有以下诸多具体实现方法。前四个方法属于被动识别方法而第五个方法属于主动识别方法。部分防火墙可以同时利用其中几个方法对用户数据流进行应用类型识别，甚至结合贝叶斯 (Bayes’ theorem) [60] 或判决树 [58] 等人工智能算法进行智能识别。

5.1.1 端口粗过滤

端口粗过滤是指根据目的端口判断其可能的应用类型的方法。互联网号码分配局 IANA[30] 是制定网络端口及其相应网络应用的机构。截止目前，端口 0 至端口 1024 已经基本分配完毕 [42]。通过网络端口，防火墙可以大概判断其可能运行的协议。比如 NFS 协议常用的目的端口是 2049，只要出现了该端口的流量，即使没有出现明显的内容特征，也可以大概判定其应用类型。

5.1.2 内容识别

内容识别是指根据用户数据流内容来识别其网络应用类型的方法。由于网络应用是依照提前制定的网络协议来完成的，用户数据流往往会具有某种的内容特征。比如 HTTP 常用数个命令 (GET/POST 等) 都会出现在 TCP 协商完成的第一个数据包的最开始，并且第一个行总是以 HTTP/X.X (使用的 HTTP 版本号) 结尾，防火墙就可以使用该特征判断出在任何目的端口上允许的 HTTP 协议。类似的，所有国际标准组织的制定标准协议都有明显的内容特征。对于一些非标准协议，其内容特征可能随版本的升级而发生改变，就需要防火墙也相应的定期更新自己的特征库才能跟上众多软件的特征变化。

5.1.3 数据包长度识别

据包长度识别是根据交互数据包的长度序列和分布来进行应用识别的方法。在用户数据流没有明显的内容特征时，这个方法非常实用。在网络协议的协商阶段，服务器和客户端之间发送的网络包长度往往存在着一定规律。假如一个网络协议在协商阶段规定：客户端要发送一个负载长度为 60 字节的 TCP 数据包发起请求，服务器收到后需回复一个长度为 40 字节的数据包作为回复内容和一个长度在 20-30 字节之间的数据包作为另一个回复内容。那么这个网络协议就具有了一定数据包长度特征，这完全可以被防火墙加以利用并作为应用识别。为了躲过防火墙的这类识别，应用程序需要通过进行扰码或者加密等手段来打乱长度特征。

5.1.4 数据包间隔识别

数据包间隔识别是根据网络协议中规定的周期性的保活数据包来进行应用识别的方法。在隧道协议中，服务器和客户端为了监控隧道可用状态需要周期性的发送保活数据包。这个数据包一般会以固定的周期间隔发送并且长度较小。即使是一些非标准的隧道连接应用，也往往具有这个网络协议的规律。用来进行网络干扰的网络技术可以

利用这个规律来识别隧道应用从而进行屏蔽。

5.1.5 主动检测识别

主动检测识别是指防火墙作为中间人改动客户端发给服务器的数据包内容并根据服务器返回的数据包内容来进行应用识别的方法。比如恶意软件常用的 IRC[56] 控制通道虽然符合标准的 IRC 协议 (IETF 制定的网络聊天协议)，但是往往却并不支持常用的 IRC 命令的简单变形。防火墙利用这一特征通过主动发送一些命令来测试服务器回复，从而识别该网络应用是正常的聊天应用还是恶意软件的控制通道。可以看出，主动检测识别和上面所述的被动方法完全不同。它使得防火墙不仅仅通过监听数据流内容来识别应用，更通过主动修改或主动发送数据包来主动检测。

为了针对以上所有检测，三叉戟协议结合了两种隧道模式来阻止防火墙的检测：协议混淆模式和协议伪装模式。由于协议混淆模式无法被防火墙检测出任何特征，从而实现了突破网络干扰功能。但是在某些白名单系统下，凡是不能被识别的数据流同样遭到丢弃或屏蔽。此时，三叉戟协议将自动切换到协议伪装模式继续实现突破网络干扰功能。

5.1.6 协议混淆模式

协议混淆模式针对防火墙的各种检测手段作出相应的应对，使得防火墙无法识别出任何特征。此模式的工作方法如下：

- 随机端口：随机协商端口作为数据流端口。
- 加密内容：所有数据包内容全加密；保证无法用正则表达式 (regex) 抽取内容特征。
- 混淆数据包长度：所有数据包长度都进行随机化处理。
- 无定期保活数据包：数据包将自行携带保活数据；无明显的保活数据包独立存。

- 防止主动检测：服务器丢弃任何非协议规范的数据包并拒绝响应。

5.1.7 协议伪装模式

协议伪装模式是指将流量特征伪装成其它常见协议的流量特征。例如可以伪装成以下两种常见的协议：

- HTTP 协议：隧道协议被完全封装在一个“HTTP GET”和一个“HTTP POST”的消息体中。“GET Response”命令用于接收下行数据，而 POST 消息体用于发送上行数据。由于端口是客户端和服务器双方提前随机协商的，所有 HTTP 部分不会出现专有的字段名称等特征。

- TLS 协议：此时利用的是 TLS 1.2 的 session ticket 功能，隧道流量就像是在使用已经协商好的 session ticket 的一个标准的 HTTPS 连接，由于没有经过协商阶段，防火墙也不能作为中间人进行解密/加密。AtomOS 在此后负载中也会全部使用和上述协议混淆模式类似的加密和防识别机制。

5.1.8 NAT 穿越

P2P 网络的另一个常见问题是 NAT[50] 穿越。NAT 是当前网络设备在 IPv4 网络环境中的常用功能。网络设备在局域网内往往配置的是私有 IP 地址，但是要想在互联网中传输数据包，却必须要把数据包的目的 IP 地址和源 IP 地址配置为公有 IP 地址。为了解决这个矛盾，在局域网出口处的网络设备可以利用 NAT 把从局域网向互联网传输的数据包的私有 IPv4 地址转换为网关的公有 IP 地址，从而使得数据包得以在互联网内传输。这个做法不但解决了 IPv4 地址有限的问题，也解决了机构或企业隐藏内部网络结构并隔离外部网络的需求。对于 Deeper Connect 的用户来说，网络设备很可能处于运营商的 NAT 设备之后，这导致 Deeper Connect 不得不使用私有 IP 地址。此时 Deeper Connect 就无法接收到来自互联网设备发出的连接请求，我们采用以下技术来解决这个问题：

- 如果连接的接受方使用私有 IP 地址，而发起方使用公用 IP 地址，则由接收方发起反向的连接请求。

- 如果双方均使用私有 IP 地址，则需要进一步的 NAT 类型检测来判断如何发起连接请求。AtomOS 在这里实现了类似 STUN 协议 (RFC3489 [59]) 原理的私有协议，在设备进行网络注册的初期就能够知道自己所在的网络 NAT 类型并随本节点的其他信息一起发布到网络上。此后设备在建立端到端连接时会避免两个都在 Symmetric NAT 或者 Port Restricted Cone NAT 之后的设备直接连接，而对于其他的 NAT 类型 (Cone NAT 或者 Restricted Cone NAT)，AtomOS 都可以尝试进行两端的直接连接

5.2 自适应隧道技术

Deeper Connect 采用的是高效、灵活、自适应的专有隧道协议而不是标准的 IPSEC 之类的隧道协议。在自适应隧道技术设计和实现的过程中，我们广泛借鉴了在业内已经较为成熟的各种广域网加速技术 [71]。尤其针对跨国互联网存在的高延时、高丢包率和数据流乱序等问题，我们创新性的在数据流隧道层实现并改进了这些优化技术。这有效的提升了带宽利用率，并达到了显著改善用户的上网体验的目标。

5.2.1 自适应数据压缩和合并

通过自适应隧道技术，Deeper Connect 可以对用户数据流内的数据包进行可压缩判断并以此来决定是否进行压缩处理。比如互联网中最常见的 HTTP 协议，由于这类网络协议的内容主要是英文字符，经过压缩可以节约 70% 左右的带宽，这大大提高了传输效率。然而，对于视频音频流量中常见的 MP4 等格式或采用 SSL 和 TLS 加密的 HTTPS 和 SFTP 等网络协议，由于其本身信息熵 [62] 已经趋近该长度可携带数据的理论极限，压缩除了增加 CPU 消耗外并不能节约带宽，导致压缩处理反而降

低了传输速率。所以，自适应隧道技术需要根据内容进行判断并处理，以达到提高传输效率的目的。

通过自适应隧道技术，Deeper Connect 还可以通过合并发送数据量较小的数据包，以达到提高传输效率的目的。有不少网络协议由于本身设计的原因导致用户数据流内存在大量的数据量较小甚至完全没有的控制包。拿一个 30KB HTTP 传送数据流举例来说，即使客户端的协议栈对 TCP 的优化为每两个数据包才返回一个接收端的确认包，也导致数据流内存在 40% 的小于 100 字节内容的数据包。这么大比例的数据量极小的数据包大大降低了用户数据流的传输效率。自适应隧道技术可以在不影响 TCP 连接延时的情况下，对多个数据流内的数据包大量合并发送并再次压缩，以达到提高提高传输效率的目的 (图 20).

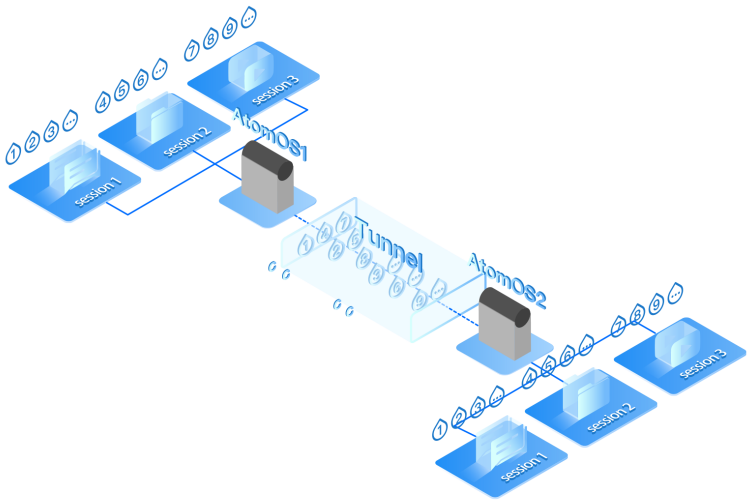

图 20: 数据包自动合并压缩传送示意图

5.2.2 基于应用类型的流量控制

基于应用类型的流量控制可以根据用户数据流的应用类型进行相应的流量控制，以保证用户延迟敏感或流量敏感的应用数据流享有更高的网络隧道使用级别。在家用网络

中，网络带宽往往有限。当用户通过多个应用程序同时使用带宽时，网络带宽的需求往往远大于实际网络带宽，这就带来了如何分配有限网络带宽的难题。自适应隧道技术可以根据用户数据流自动判断出应用类型并给其赋予相应的网络隧道使用级别。比如，网页浏览或电子邮件下载这类应用就属于用户延迟敏感或流量敏感的应用类型。而文件下载这类应用就属于用户延迟不敏感或流量不敏感的应用类型。自适应隧道技术首先可以自动估算网络隧道的实际带宽和网络隧道的带宽需求。如果供不应求的话，自适应隧道技术会根据应用的网络隧道使用级别来控制网络隧道带宽的使用。级别较低的应用数据流将被暂时缓冲在有限的数据包队列中。如果数据包队列已满，溢出的数据包将被丢弃。这虽然影响了某些应用的正常处理造成了延迟，但是在带宽有限的情况下，自适应隧道技术已经最优化了用户的上网体验。

5.3 智能路由技术

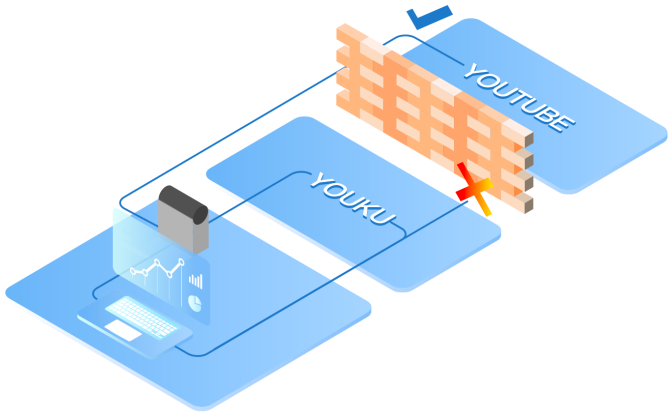

图 21: 智能路由技术

智能路由技术是指根据用户数据流特征自动决定网络路由并判定是否通过隧道传输的技术。我们提供两种模式，隐私保护模式和突破网络干扰模式。在隐私保护模式

下，涉及用户上网痕迹的用户数据流将根据用户设置的匿名服务级别来决定是否经过网络隧道封装处理；在突破网络干扰模式下，访问互联网的用户数据流将根据访问对象网址及其相应的允许访问地区和屏蔽访问地区数据库来决定是否经过网络隧道封装处理。

智能路由为用户提供了以下好处：

1. 节约成本：网络隧道是通过两个或多个 Deeper Connect 设备建立的，所以隧道的两端都是 Deeper Connect。如果一个 Deeper Connect 寻求和别的 Deeper Connect 建立隧道连接，就必须要通过网络共享平台寻找服务器并且根据流量或网速支付数字货币。用户并不是免费使用网络隧道的。智能路由技术可以根据数据流的属性自动判定是否通过网络隧道传输。这个做法不仅减少了网络隧道的使用量，而且避免了网络隧道带来的网络延迟，使用户既保持了正常数据流的原始体验又不会造成额外的开支。

2. 匿名服务：匿名服务指的是隐藏用户的 IP 地址，以达到难以追踪上网痕迹的目的。由于网络隧道是经过端到端的加密处理的，通过网络隧道传输的用户数据流将不会在互联网上留下任何痕迹。我们会根据用户访问对象的公开性设置级别，并根据用户的设置来决定是否对相应的数据流进行网络隧道封装处理。网页访问等这类公开性很强的用户数据流属于匿名服务最高级别。对于这个级别的用户数据流，网络隧道封装处理属于必选的设置。而 P2P 下载等这类公开性较弱的用户数据流属于匿名服务次高级别。对于这个级别的用户数据流，网络隧道封装处理属于可选的设置，以减少用户的使用成本。不仅如此，用户还可以选择多跳路由模式，以实现更加严格的匿名服务。在多跳路由环境下，网络隧道将由大于两个 Deeper Connect 来建立而不是一般情况下的两个 Deeper Connect。这样做的好处是作为中间节点的 Deeper Connect 由于无法解密用户数据流而无法偷窥内容。而作为最后一个节点的 Deeper Connect 虽然可以解密用户数据流，但是却无法知道数据流的来源。可以看出，如果组成网络隧道的

Deeper Connect 越多，那么用户数据流将越难以追踪而相应的成本也越高。

5.4 链路层隧道技术

AtomOS 是世界上首个不需要任何配置，在虚拟网线模式下即可以实现智能路由和隧道封装的设备。当前市面上所有实现了隧道功能的网络设备都是工作在路由模式，也就是说，用户需要具备一定的网络技术能力，学会 IP 地址规划、隧道协议配置，才能正确的建立起隧道。还需要一定的路由知识才能把需要的流量转发到隧道中进行正确的封装、解封装。而 AtomOS 完全改变了对终端用户的专业知识需求，Deeper Connect 设备不用具备任何专业知识，用户将 AtomOS 设备接入家用路由器的上行链路后，AtomOS 会先进入学习阶段，此时进行流量监听的同时不影响流量的转发，并根据两个端口出现的 IP 地址的统计规律自动判断其连接的方向。我们知道，互联网上分部着数以亿计的节点，而个人用户的出口 IP 数目很少而且固定，所以分析很短一段时间的流量之后，我们就可以知道哪一端是上联口，哪一端是下联口。紧接着 AtomOS 会进一步学习上联网关 IP/MAC 地址，DNS 服务器等一系列信息，供以后可能的隧道协商和封装使用。

我们认为，智能家庭网关本身是一个用户操作频度很低的产品，越是不需要用户随时感知到它的存在，只在需要改变功能时做最少的配置，越是满足最大部分用户的真实需求。特别的，结合上面我们独创的智能路由技术，在零使用门槛下用最低的成本完成用户的隐私保护和网络穿越需求。

5.5 隧道层拥塞控制技术

Deeper Network 的重要应用场景之一就是为用户提供网络匿名服务，使用户的隐私得到保护，并且可以自由地访问任何互联网内容而不被干扰和屏蔽。在匿名服务的应用场景中（如图 22），用户通过 Deeper 节点之间的安全 AtomOS 隧道传输数据，使得被访问的网络服务无法追踪用户的隐私数据 (例如用户的 IP 地址)。同时，由于

AtomOS 隧道中的数据包都经过了严格的加密处理，使得访问互联网干扰无法识别用户访问的内容，从而避免了用户的访问被干扰。

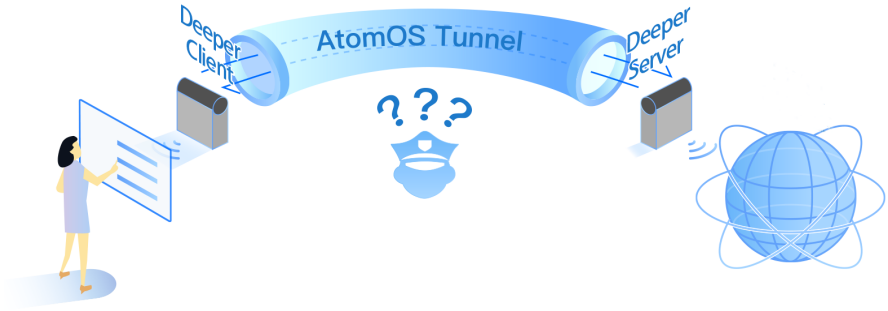

图 22: Secure Shared Service (SSS)

通过 Deeper 独创的网络安全技术与区块链技术的结合，SSS 能够有效地保证 AtomOS 隧道连接的安全与稳定，访问互联网不被干扰。然而，AtomOS 隧道的数据传输效率，包括传输速度与传输延迟，仍然是一个有待解决的问题。在匿名服务的应用场景中，对数据传输有两大主要挑战

1. 匿名服务主要是为了访问更多的互联网内容。在跨国的互联网访问中，存在着数据传输距离远、高延迟、高丢包率和乱序概率的问题。

2. 虽然 AtomOS 隧道中的数据包都经过了严格的加密处理，使得不受干扰，但一些技术可能会针对不能识别的数据流采取随机丢包的策略 (例如 1% 的丢包) 以破坏用户体验。

针对以上挑战，Deeper 首次提出在隧道层建立面向连接的可靠的传输协议，并主要从网络拥塞控制的角度来探讨解决匿名服务中的网络数据传输效率问题。Deeper Network 中的一整套拥塞控制解决方案包括两个核心部分：一是在 AtomOS 隧道层中实现部署一种新型的拥塞控制算法 TBBR，使得在高丢包率的情况下，AtomOS 隧道层任然能维持有效的数据传输速度，并且大幅降低传输延迟；二是对网络丢包事件

进行快速检测并且实现快速重传，从而更好地适应匿名服务应用场景中的高丢包率环境。

TBBR 的两个核心部分均是对发送端的改进，而接收端不需要做任何改变，即发送端不依赖于接收端任何额外的信息反馈。这也是 TBBR 的重要设计原则之一。在网络匿名服务的高延迟、高丢包率应用场景中，接收端任何额外的信息反馈都将无疑增加网络负载，并且在这样的环境中，无法保证任何稳定的反馈。

传统的拥塞控制算法 (例如 CUBIC [26], TCP Vegas [8], TCP Reno [52]) 通常是基于丢包事件的，即将丢包作为网络拥塞的信号。这类算法通过一个发送窗口来控制数据的发送速度，并通过 AIMD (Additive-Increase/Multiplicative-Decrease) 算法来控制在时间 t 时窗口 $W(t)$ 的大小：

$$W(t+1) = \begin{cases} W(t) + \alpha & \text{如果没有检测到丢包} \\ W(t) * \beta & \text{如果检测到丢包} \end{cases} \tag{1}$$

从以上算法不难看出，这类基于丢包的拥塞控制算法的特点是在发现丢包之前会不断地增大发送速度，而一旦检测到丢包事件会突然急剧减小发送速度。由此导致两个方面的主要问题：

1. 将所有丢包事件都当作网络拥塞的信号是不恰当的。事实上，丢包事件也有可能是网络传输错误导致的。另外，在匿名服务的应用场景中，网络干扰也可能故意导致人为的丢包。按照 AIMD 算法，当丢包事件发生时，网络传输速度会急剧减小。当丢包率达到一定程度时 (例如网络干扰导致的 1% 故意丢包)，将会导致整个网络传输几乎陷入停滞。

2. 由于在发现丢包之前都会不断地增大发送速度，这类算法倾向于占满整个网络的缓存空间。缓存中的数据包越多，就会导致网络排队延迟 (queueing delay) 越高。由于内存价格变得越来越便宜，当今网络中的缓存空间也在不断增大，从

而导致上述排队延迟的问题日益严重。

由此可见，传统的拥塞控制算法既没有达到最佳的传输速度，也没有实现最佳的网络延迟。

Deeper 在 AtomOS 隧道层部署了一种新型的拥塞控制算法 TBBR (Tunnel Bottleneck Bandwidth and Round-trip propagation time)。TBBR 是在 BBR [10] 的基础上结合隧道技术发展而来。BBR 最早由 Google 提出，并且已经广泛部署在 Google 的广域网 WAN 之中。不同于传统的拥塞控制算法 TBBR/BBR 不再依赖于丢包事件作为网络拥塞的信号，而是回归到网络拥塞的本质，即发送端向网络中发送数据的速度超过了网络的承载能力。为了测量当前网络承载能力，TBBR/BBR 会不断地检测两个核心指标，即网络的瓶颈带宽 BtlBw (Bottleneck Bandwidth) 和往返传输延迟 RTprop (Round-trip propagation time)。如果将网络传输通道比作一根水管，那么瓶颈带宽 BtlBw 就是水管中最窄处的截面积，而往返传输延迟 RTprop 就是水管的长度。整个网络的容量 BDP (Bandwidth Delay Product) 就是两者的乘积：

$$BDP = BtlBW * RTprop \tag{2}$$

BDP 也可以理解为在不造成任何排队延迟 (即不占用任何缓存空间) 的情况下，网络中最大可以承载的数据量。

TBBR/BBR 的核心思想就是当网络瓶颈处数据到达速度刚好等于瓶颈带宽 BtlBw，并且整个网络中正在通过的数据量刚好等于网络容量 BDP 时，网络处于最大传输速度和最小传输延迟的最佳状态。TBBR/BBR 通过测量 BtlBw 和 RTprop 来控制发送速度，使得整个网络尽可能保持最佳状态。值得注意的是整个网络的属性是不断动态变化的，因此 TBBR/BBR 需要不断的测量 BtlBw 和 RTprop 以及时更新发送速度。另外，BtlBw 和 RTprop 两个指标无法同时获得。为了测量瓶颈带宽 BtlBw，我们需要在数据填满网络传输通道时才能知道网络的最大传输速度；为了测量往返传输延迟 RTprop，我们需要在网络尽可能空载 (即没有排队延迟) 的时候才能知道网络

的最小传输延迟。为了解决这个问题，TBBR/BBR 采用两者交替测量的方式，并用一段时间窗口 W_R 内的测量值来估算两个指标在当前时间 T 时的值：

$$\hat{BtlBw} = \max(r_t), \forall t \in [T - W_R, T] \tag{3}$$

$$\hat{RTprop} = \min(RTT_t), \forall t \in [T - W_R, T] \tag{4}$$

其中 r_t 为在时间 t 时测得的数据传输速度，RTT_t 为在时间 t 时测得的往返延迟。

从 TBBR/BBR 的设计思想不难看出，TBBR/BBR 具有以下两大特点：

1. 在一定的丢包概率下，TBBR/BBR 仍然能保持接近网络带宽的稳定传输速度。
2. 在保持最大传输速度的情况下，TBBR/BBR 并不倾向于过多地占用网络缓存空间，从而降低了排队延迟。

Google 已经在 Google.com 和 Youtube 的服务器上部署了 BBR。从 Google 的实践经验来看，BBR 成功地将 YouTube 的全球网络传输延迟的中位数降低了 53%。在发展中国家，这个数值甚至高达 80% [10].

Deeper 独创地将 BBR 的成功经验引入到网络匿名服务的应用场景中，实现了世界上第一个隧道层拥塞控制协议 TBBR。通过 TBBR，我们发现 Deeper Connect 能够有效地降低跨国互联网访问的网络延迟，并且在有防火墙故意丢包的情况下仍然能够维持稳定的网络传输速度，给用户带来良好的上网体验。

图 23 对比了部署 TBBR 后的 AtomOS 隧道层与不做拥塞控制的传统隧道层 (IPSEC) 在模拟不同丢包率情况下的网络传输速度。实验环境为 1 个数据流，BtlBW=100Mbps，RTT=100ms。图中最上面灰色曲线代表理想情况下的传输速度，即 BtlBW * (1 - p)，其中 p 为丢包率。从图中可以看出，传统隧道层在丢包率 0.01% 的情况下，传输速度就只能维持在网络带宽的 30% 左右了。随着丢包率的进一步提高，传输速度只剩下带宽的 5%，几乎停滞。作为鲜明的对比，AtomOS 隧道层即便在

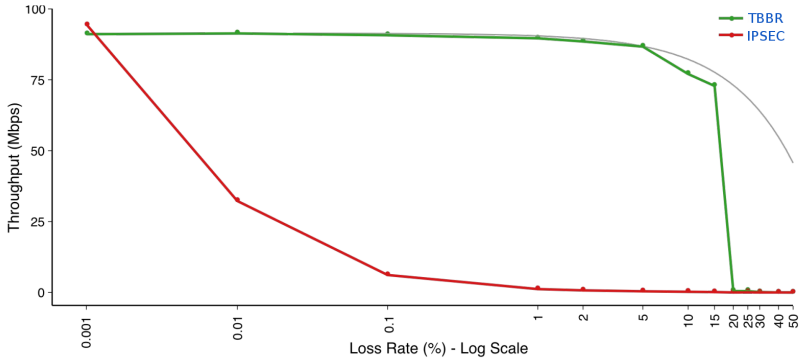

图 23: 不同丢包率下的网络传输速度

5% 丢包率的极端情况下，仍然能够保持与理想传输速度一致。在 15% 丢包率下，仍然能维持 75% 带宽的传输速度。在网络匿名服务的应用场景中，假设网络干扰对无法识别的数据流造成 1% 的故意丢包，此时 AtomOS 隧道层的传输速度几乎不受影响，仍然保持理想传输速度；而传统隧道层此时传输速度几乎只相当于 5% 的带宽了。

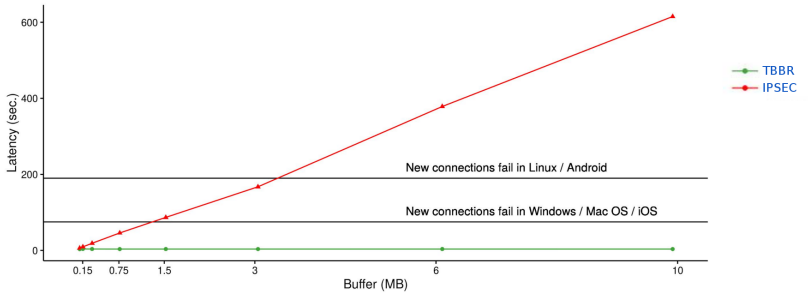

图 24: 不同缓存大小情况下的网络延迟

图 24 对比了 AtomOS 隧道层与传统隧道层在不同缓存大小情况下的网络延迟。实验环境为 8 个数据流，BtlBW=128kbps，RTT=40ms。传统隧道层倾向于不断占用网络缓存空间而导致其网络延迟随着缓存空间大小呈线性增加。更加严重的是，当延迟大到一定程度时，会导致不同操作系统中网络初始连接 (SYN) 超时，从而导致连接失败。与之形成鲜明对比的是，AtomOS 隧道层始终保持很小的网络延迟，并且不

随缓存空间大小而变化

Deeper 在 BBR 的基础之上对于 AtomOS 隧道层做了进一步的优化，增加了对网络丢包事件的快速检测与快速重传

传统 TCP 对于网络丢包事件的检测主要有两种方法：

1. 如果在一段时间内没有收到接收端的确认 (ACK)，则认为该数据包丢失。这个超时重传时间被称为 RTO (Retransmission Timeout)。

2. 如果从接收端收到了三次重复的确认 (duplicate ACK)，也认为发生了丢包事件，从而触发重传机制。

在 TCP 中，当接收端发现有的数据包被跳过时，会导致接收端发出重复的确认。而数据包被跳过有两种可能：一是该数据包被丢掉了；二是发生了网络乱序，即原本排在该数据包后面的包先到达了接收端。因此，当发送端收到重复的确认时，并不能马上断定是否发生了丢包，而是需要在多次重复确认之后才认为大概率发生了丢包事件。如果过早地认定丢包，将会导致不必要的重传，增加网络负担；如果过晚，则会导致对丢包事件反应迟钝，效率不高。

目前通用的基于三次重复确认的快速重传机制要求发送端至少要能发出 4 个数据包 (即发送窗口大小至少为 4) 的情况下，才有可能出现三次重复确认；否则只能依赖 RTO 超时来触发重传，效率很低。因此基于三次重复确认的快速重传机制在以下情况下效果并不理想甚至根本不起作用：

1. 研究表明 [1] 从应用层的角度来讲，很多时候一个 TCP 连接总共所需要发送的数据包不到 4 个。此时，目前的快速重传机制根本不起作用。

2. 网络出现拥塞导致发送窗口变得很小 (例如 <4)。

3. 接收端为了充分利用带宽，可能会延迟发送确认。在累积确认 (cumulative ACK) 的模式下，甚至会把多个确认合并为一个。此时，发送端需要发送更多的数据包才有可能触发三次重复确认。

为了更加有效地利用快速重传机制，做到既能及时地检测到丢包事件并快速重传，同时又减少不必要的重传，TBBR 采用一种动态的快速重传阈值的算法。其核心思想是当不能发送更多数据包时 (受发送窗口大小限制或者应用层没有更多数据要发送)，按照当前还未确认的数据包数量来动态调整快速重传的阈值；否则仍然沿用阈值为 3。

Algorithm 1 Algorithm for fast retransmission threshold τ in TBBR

```
Assume that the number of currently unacknowledged packets is k
if there are no more packets to send then
    τ = max(min(k − 1, 3), 0)
else
    τ = 3
```

关于重传超时的 RTO，传统 TCP 中采用一种被称为指数退避 (exponential backoff) 的算法，即如果一个数据包在当前 RTO 下超时，则重传该数据包，并将 RTO 更新为之前的两倍。在极端情况下，如果一个数据包连续 n 次超时，RTO 会爆炸性增长为之前的 2^n 倍，极大地影响传输速度。TBBR 采用一种更加平滑的 RTO 增长曲线，每次超时时，将 RTO 设为之前的 1.5 倍。

虽然 TBBR 的整体设计是关于发送端的，但是对于接收端，我们仍可做一些改进来提高网络传输效率。这其中主要包括两个方面：

1. 在接收端采用选择性确认 (SACK [46]) 机制。相比于累积确认机制中接收端只反馈当前还没有收到的包的最小序列号，SACK 允许接收端明确地告诉发送端当前窗口中哪些包已经收到，哪些包还没有收到。当发送端需要重传时，可以选择性地只重传那些还没有被确认的包。另外，在累积确认机制下，如果有多个数据包丢失，发送端每次只能得知一个数据包的丢失，导致效率不高。而 SACK 则可以一次性反馈所有丢失的包的信息。研究表明，在高延迟，高丢包的网络中，采用 SACK 可以极大地减少重传的包的数量，提高传输效率。

2. 动态地调整确认延迟。如前面所述，接收端可以延迟发送确认信息。这样做固

然可以充分利用带宽，但却也延长了数据包能够被确认的时间，并且给快速重传机制带来困难。尤其是在高延迟、高丢包率的环境中，更加需要接收端及时地确认每一个收到的数据包。因此，在接收端，可以根据当前网络的延迟和丢包状况动态的调整确认信息的延迟。

6 区块链

Deeper 链的构架分为两层, 顶层 (top layer) 和底层 (bottom layer) (见图25)。顶层由数百个验证节点组成，功能和其他的区块链一样。底层也被称为 Deeper 层，由数百万个 Deeper 设备组成。这些设备通过提供服务来获得信用积分，例如共享带宽，提供 VPN 服务。

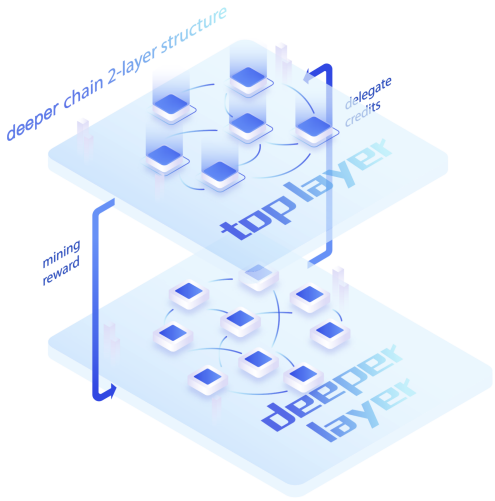

图 25: deeper 链双层结构

与标准的 Nakamoto 共识协议不同，我们的信用证明 (PoC) 不使用工作量证明 (PoW)，因此具有较低的能耗。我们的共识机制与权益证明 (PoS) 类似，但验证节点的投票权取决于押金和信用分数两个因素。一方面，顶层的安全性由底层设备的信用分数来保护。加入底层的设备越多，网络就越安全。另一方面，底层的设备收到的奖励 (reward) 将激励更多人参与深层网络。这种闭环的形成将扩展并和保护整个网络。

6.1 共识机制

6.1.1 概述

Deeper 使用 HotStuff [74] 作为其状态机复制 (SMR) 框架。HotSuff 是第一个同时具有线性 (即 $O(n)$) 通信复杂度和响应网络延迟（即网络延迟时间取决与实际网络速度) 的拜占庭容错 (BFT) 协议。HotStuff 从 BFT 系列的协议中抽象出链式模式，并引入了流水线结构，极大地提高了网络的吞吐量。

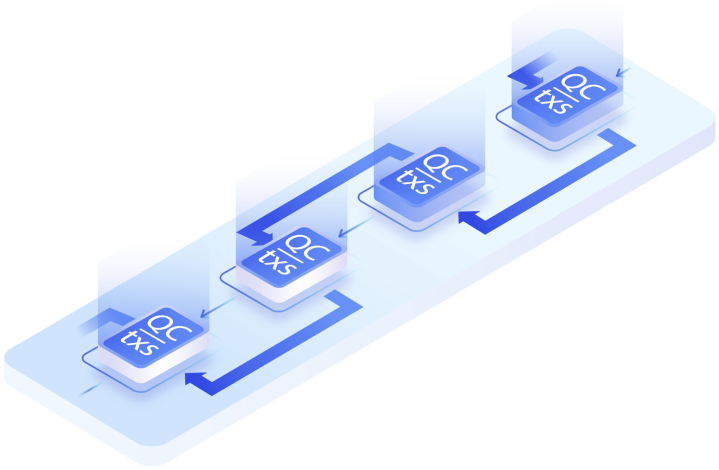

图 26: HotStuff 流水线结构

相比与其他 BFT 协议，每一轮（即提议、预提交、提交等不同阶段）中有不同投票格式，Hotstuff 中的每一轮不再区别对待。对某个区块投票也可以视为对它引用的父区块的下一阶段投票。也就是说对一个块的投票被认为是对区块本身的提议投票，同时也是对其父区块的预提交投票，对其祖父区块的提交投票，以及对其第三代祖先区块的决定性投票。块只有在其第三代区块被成功投票时才执行。与其他 BFT 共识协议相比，流水线结构的引入提高了吞吐量大约 3 倍。

此外，HotStuff 使用星形通信模式（即每个人都直接与领导节点进行通信）和门限签名 (threshold signature) 来确保每个块需要的网络通讯流量: 领导节点将区块发送给验证节点，验证节点生成各自的签名，领导者收集其他节点的签名然后构造一个门限签名，作为区块的有效性证明。这样可以保证最佳的通信效率。

在 Tendermint 和 PBFT 这些共识算法中，每一个区块达成共识需要 2 轮。Hotstuff 通过增加一轮共识，同时借助于门限签名可以把领导节点变更 (leader change) 的复杂度变成线性的，并且保证出块速度等于实际的网络延迟。相比之下，PBFT 的领导节点变更复杂度是 $O(n^2)$，而 Tendermint 的出块速度取决与系统定义的参数，没有根据网络速度达到最优。deeper 链提供了用户隐私保护功能，因此除了需要防止针对公共区块链的女巫 (Sybil) 攻击外，节点还可能会遭遇政府和服务提供商有针对性的禁令，这可能导致领导节点被封锁。由于 HotStuff 发起领导者变更是线性复杂度，这种单点故障不会显著降低网络运行速度。

6.1.2 活跃性与节点甄选

HotStuff 抽象出了共识中的活跃性 (liveness) 和领导节点变更。这些功能的实现被 HotStuff 独立出来。此外, HotStuff 协议并不考虑参与共识的节点选举问题，这个额外的功能对于公链是必须的，需要我们自己添加。

进一步说，活跃性是通过所谓的超时证书 (timeout certificates) 来实现的。当验证节点在指定的时间内没有收到领导节点的信息时，它会向通过协议定好的规则选择下一个领导节点，并发送附带签名的领导者变更消息。新的领导节点在收到足够的签名后，生成一个超时证书，并用广播给所有节点。

在任何人都可以加入的系统中，为了保证网络的安全性，验证节点需要每隔一定时间重新选举。这就是所谓的委员会轮换。委员会轮换的时间不能够太长，也就是需要在网络大部分节点被渗透之前就进行选举。只要在两次选举的时间内，攻击者控制的节点不超过总数的 1/3 即可。

对于委员会轮换，Deeper 使用基于 VDF 的随机信标 (random beacon) [7]。VDF 与 VRF 类似，VRF 是一种输出不可预测的加密函数，它还可以生成一个可用于验证 VRF 计算正确性的证明。相比之下，VDF 需要大量的计算步骤，因此任何机器进行 VDF 的计算时间大于一个系统设定的下限。而验证 VDF 计算结果则要快得多。通过 VDF，我们在随机数的输入和输出之间施加了一定的延迟，这样可以确保任何人都无法提前预知到随机数。

在第 k 轮中，基于 $k-2$ 轮的门限签名来作为 VDF 的输入，这里 k 代表纪元 (epoch) 的最后一个区块。VDF 的计算延迟时间大约设定为需要两轮时间。这样，恶意领导节点没有足够时间提前得到 VDF 输出 (决定了委员会选举的随机数)，从而操纵委员会的选举。委员会的选举参见算法 2.

Algorithm 2 Algorithm for committee members selection

R – the value of the randomness beacon in the current epoch;
$H(x)$ – a hash function;
n – the total number of staking validators;
m – the total number of selected validators;
W_i – the weight of the i-th validator in consensus;
TW – the sum of all validator weights in consensus;

$C \leftarrow \{\}$
$S \leftarrow 0$
for $k \in \{0, \ldots, m-1\}$ **do**
    $V \leftarrow H(R||k)\%(TW - S)$
    $P \leftarrow 0$
    for $i \in \{0, \ldots, n-1\}/C$ **do**
        $P \leftarrow P + W_i$
        if $V < P$ **then**
            $C[k] \leftarrow i$
            $S \leftarrow S + W_i$
            break
return C

此算法意味着每个验证节点在选举时候不会被重复选中，并且每个验证节点被选

中的概率与它们的权重成正比。委员会选出后，里面的节点将轮流作为领导节点。每个时代大概出块 17,300 (即假设每块需要 5 秒时间，24 小时的出块总量)。

6.2 信用证明

Deeper 网络由两层组成。顶层包含数百个验证节点，它们不断生成新的块。而 Deeper 层是由数百万个 Deeper 网络设备组成的。信用证明允许 Deeper 的网络设备通过共享带宽来获得新的代币。每个设备将与一个帐户相关联。设备分享的带宽越多，相应帐户获得的信用分就越高。每个设备可以把它的信用评分委托 (delegate) 给验证节点。如果超过总投票权 2/3 的验证节点对新区块投票，则此区块被确定下来。在新的区块被确认后，这些设备将获得与其信用评分成比例的代币奖励。与现代社会的信用系统一样，每个账户的信用记录 $\mathcal{C}$, 都有一个最大值作为上限 $\mathcal{C}_{max}$.

6.2.1 微支付与信用评分更新

Deeper 的网络设备有两个角色 — 服务端提供带宽分享；客户端接受分享的流量。服务端提供给客户端每 MB 的流量，都将收取一定的代币作为服务费。这很类似小额付款。如果客户不进行小额付款，服务器可以随时停止提供带宽。服务器可以自己选择微支付的中止期限，即在提供超过一定量的网络带宽却没有收到微支付后，则停止服务。微支付发生在 Deeper 层，不占用上层的验证节点的资源。一台设备可以累积多个微额支付后，并最后的总支付额提交给上层的验证节点。被验证通过后，相关账户的信用分数将被更新。

6.2.2 网络模型与 API

Deeper 层的拓扑结构是一个包含数百万个节点的大图，每一个节点代表 deeper 层的一个设备。在每个时代 (epoch)，我们都认为图是固定的。不同时代之间，图是随机生成的。更具体地说，给定一个 deeper 设备，我们将随机分配 8 到 16 个邻居节点。

因此，图中每个节点有 8 到 16 个边。我们通过智能合约来进行节点的随机匹配。我们定义与网络, 付款和信贷相关的几个 API:

- Fn randomized_graph() $\rightarrow$ Graph$\langle V, E\rangle$: 返回当前时代的节点拓扑结构;
- Fn nbr$\langle V : Node\rangle(n : V) \rightarrow$ Vec$\langle V\rangle$: 给定一个节点，返回它的邻居节点列表，这里我们假设列表大小在 8 到 16 个之间;
- Fn submit(payments: Vec⟨MicroPayment⟩, ledger: &mut Ledger): 服务器节点将累积的微支付提交到验证节点。这里 Vec 的长度代表它在某段时间内服务的客户端数量;
- Fn collect_fee(account: &Account, payments: Vec⟨MicroPayment⟩, ratio: f32): 收取付款的一小部分 μ 作为佣金，并将剩余的 $1-\mu$ 的付款存入节点账户；
- Fn update_credit_score(account: &Account, payments: Vec⟨MicroPayment⟩): 根据账户收到的微支付来更新账户的信用积分；
- Fn reward(ledger: &Ledger, n: &mut Node, credits:Vec⟨Credit⟩, amt: u32): 在新区块确认后，将奖励分配给各个节点。这里的奖励取决于参加设备的信用分多少。

6.2.3 PoC 的安全性

预防女巫 (Sybil) 攻击是公共区块链的一个关键安全考量。目前有许多不同的方法：工作量证明 (PoW)、权益证明 (PoS)、代理权益证明 (DPoS) 等。比特币和以太坊 1.0 使用工作量证明，来创建一个新的区块。在以太坊 1.0 之后，许多区块链采用权益证明，被选出的验证节点通过协作投票决定下一个新区块的诞生，节点的投票权与它抵押的代币总量成比例。我们使用类似权益证明的方法来出块，但节点的投票权不仅取决于抵押的代币，还取决于委托给它的信用分数。因此，deeper 链实际上是权益证明

和信用证明的结合。权益证明的安全性已经被很多项目进行了深入的研究。因此，我们主要关心的是信用证明 (PoC) 的安全性。

保证 PoC 安全性的第一步是控制 Deeper 网络中恶意节点的数量。为了实现这一目标，我们的协议增加了恶意控制节点的难度和成本，包括两个方面是：1）抵押代币。所有设备在注册加入网络时都需要存入一定数量的代币作为抵押。因此，如果恶意方想要控制大量的节点，它必须首先存放大量的代币，这本质上就是利益证明机制。2）最低信用要求。一个节点在加入网络后，在它可以获得奖励之前，必须达到最小的信用阈值 τ。通过这种方式，我们鼓励用户参与带宽共享来积累积分，同时也防止新创建的恶意节点加入网络后就可以得到奖励。

接下来，我们将从奖励的分配方式和信用积分更新来讨论 PoC 的安全性。假设一个服务端节点在一定时间内从 m 个客户收集付款 $[p_1, p_2, \cdots, p_m]$，并获得代币奖励 R。交易佣金比例为 μ。净利润 P 由以下公式得出：

$$P = R + (1 - \mu) * (p_1 + p_2 + \ldots + p_m) \tag{5}$$

现在我们来分析 PoC 的安全性。假设恶意方可以控制比例 θ(例如 $\theta = 10\%$) 的设备 (假设设备总数 n)，在每个期间，假设一个恶意节点随机选取 k 个邻居，其中恶意节点的个数为随机变量 X，存在 i 个恶意邻居的概率为：

$$P(X = i) = \frac{\binom{n\theta}{i}\binom{n(1-\theta)}{k-i}}{\binom{n}{k}} \tag{6}$$

假设 k 相对于 n (i.e., $k \ll n$) 较小, 则有一个恶意邻居的概率接近 θ (i.e., $P(X = 1) \approx \theta$) 而有多个恶意邻居的概率 $P(X > 1)$ 远小于 θ. 假设该恶意服务器是虚设的，不能实际提供网络带宽，因此只能向其恶意邻居节点收取费用，则净利润为 $P = R + (1 - \mu) * p_1$, 这里假设它只能获得一个恶意邻居，因为多个恶意邻居概率极低。

设计 **1**: 注意到奖励 R 是关于 $[p_1, p_2, \ldots, p_m]$ 的函数. 当 $m = 1$ 时，我们定义 $R = 0$，也就是说，如果一个服务器只服务了一个邻居，则收不到任何奖励。在这种情况下，恶意节点的净利润为负 $-\mu * p_1$ 而诚实节点的净利润为正 $(1 - \mu) * p_1$. 这个简单的设计相当于从我们的系统中删除了 PoC 组件。

我们的假设是，从长期来看，小额支付将接近服务器节点的运营成本。因此，如果删除 PoC，用户没有足够的动力来共享他们的带宽。由于奖励与信用评分成正比，信用评分更新功能的设计应激励节点为更多客户服务。即使比率 μ 不设为 0 时，当一个节点服务于多个节点时的奖励也可以将补偿费用。

设计 **2**: 我们也可以设置 $\mu = 0$. 在这种情况下，如果它只为一个客户端提供服务，我们不会更新服务器节点的信用分数。因为之前我们计算过随机分配时候，恶意节点匹配到两个或更多恶意节点的概率是非常小的。因此，在下一个块 $T + 1$ 更新信用分时候，我们可以通过阻尼因子 λ 进行调整:

$$\mathcal{C}(T+1) = \begin{cases} \min(\mathcal{C}(T) + \lambda \sum_{i=1}^{m} p_i, \mathcal{C}_{max}) & \text{if } m > 1 \\ \mathcal{C}(T) & \text{otherwise} \end{cases} \tag{7}$$

设计 **3**: 在实际应用中，我们采取设计 2 的方案，同时系统会收取 10% 的佣金。收取佣金有两个用途。第一个是相比方案 2，收取佣金会让系统更加安全，更有效的防止女巫攻击。另一个主要通途是收取的佣金将会组成一个资金库。资金库的具体用途将会在后面的章节中详细描述。

在上面的分析中，我们假设 θ 很小，这个代表恶意设备所占有的比例。这是可以通过代币抵押和最低信用分要求做到。因此恶意方遵循协议来合法赚取奖励更加有效。

6.2.4 其他奖励机制

我们描述了几种激励机制，鼓励更多的用户加入网络。

信用衰减: 当一个设备停止加入 Deeper 网络时，系统将逐渐降低其信用，直至达到预定义的阈值 τ_0。假设 τ 为用户可以通过委托信用分以获得奖励的阈值，我们设置预定义的阈值 $\tau_0 < \tau$。如果该账户的信用评分小于 τ_0, 则不存在信用评分下降的情况。如果该账户的信用度大于 τ 且不参与网络共享活动，即长期闲置的话，其信用评分将逐渐降至 τ (大概几个月)，然后其信用评分将逐渐渐进下降至 τ, 但不会进一步下降。

初始信用购买: 为了鼓励更多用户参与网络，我们需要一种方法，让他们能够尽快赚取信用分。初始信用购买就可以做到。它只作用于信用分数小于 τ 的账户 (即允许用户获得奖励的阈值)。如果用户当前信用评分 $\mathcal{C}$ 小于 τ, 用户可以支付 $\delta(\tau - \mathcal{C})$ 的代币来购买其积分达到 τ, 其中 δ 是系统可调参数。用于购买信用的代币将作为奖励分发给矿工，包括验证节点，抵押代币者和信用委托者。

7 代币经济

7.1 概述

Deeper 使用的代币名为 DPR，主要用于经济激励以及各种服务的支付。它是 Deeper Network 的主要价值货币。

DPR 的总供应上限为 100 亿。其中 60 亿作为区块奖励来分配。初始区块奖励为 90 DPR。每个区块所创建的 DPR 数量会随着时间的推移而减少，这与比特币类似。每个区块的分发量在每 518,400 个区块时将重新计算，分发量等于 $Rem/77,760,000$，其中 Rem 代表剩余的代币，即是 60 亿代币与目前已开采的代币之间的差额。

时间	区块	剩余	产出的 **DPR %**	增加的 **DPR**
2021/04	0	6,000,000,000	0.00%	0.00%
2022/04	6,220,800	5,531,030,851	4.69%	100.00%
2023/04	12,441,600	5,104,417,550	4.27%	47.64%
2024/04	18,662,400	4,710,709,310	3.94%	30.54%
2025/04	24,883,200	4,347,368,134	3.63%	21.99%
2026/04	31,104,000	4,012,051,785	3.35%	16.87%
2027/04	37,324,800	3,702,598,683	3.09%	13.47%
2028/04	43,545,600	3,417,013,972	2.86%	11.06%
2029/04	49,766,400	3,153,456,662	2.64%	9.26%
2030/04	55,987,200	2,910,227,761	2.43%	7.87%
2031/04	62,208,000	2,685,759,320	2.24%	6.77%

表 3: 预计的 DPR 发布时间表（前 10 年）

DPR 代币涉及的两个主要机制是微支付（与信用证明密切相关）和抵押 (与权益证明密切相关)。

7.2 权益机制

Deeper 使用权益机制和 VDF 来选出一个时代 (epoch) 的委员会成员。网络中任何参与者都可以通过抵押一定数量的 DPR 来成为验证节点。

共识网络参与者的权重（即他们在特定 epoch 被选为验证者的概率）由它账户下锁定的代币总量和 PoC 的参与者总信用评级决定。TS 代表 epoch 初始的总权益（total stake），TC 代表 epoch 初始的总信用积分（total credit）, PS 代表参与者的对应权益（participant's stake), PC 代表参与者的信用积分（participant's credit）。那么参与者的共识的权重等于：

$$(0.5 * \frac{PS}{TS} + 0.5 * \frac{PC}{TC}) \tag{8}$$

根据时间表，当被选为委员会成员的验证者成为新一轮（round）的领导者（leader）时，将会获得区块生产的奖励。如果领导者作恶，诚实的委员会成员不会签署错误的区块提案。作恶节点会导致超时，领导者将在超时后被更换，作为惩罚，犯了错误的领导者也将无法在该轮次获得奖励。

7.3 治理

主要有两种治理类型：链外治理和链上治理。链外治理需要开发者和社区之间的大量协调。在 deeper 链中，我们选择后者。在大多数链上治理模型中，人们使用他们的代币来获取选项列表。例如，最常见的情况是系统只有在大多数利益相关者选择升级的情况下才能升级。

这在 PoS 模型里会产生一个问题。与普通用户相比，大股东拥有更多的投票权。比如一种流传的说法是区块链是由风投公司控制的，因为风投公司是早期的投资者，他们拥有大量代币。有不同的机制来解决这个问题。例如，二次投票 (quadratic voting) 就是其中之一。然而，这些设计要么过于复杂，要么不能从根本上解决问题。

在 deeper 链中，我们使用 PoC（信用证明）来解决这个问题。对于任何系统升级或协议变更，提议者将发布一份选项列表并给出投票时间窗口。任何用户帐户都将根据其信用评分进行投票，而不是抵押代币。只要它的信用评分大于某个阈值（例如，信用总分为 100，阈值为 60），那么它就是合法选民。这很类似现实生活一个人到了法定投票年龄。在 PoS 中，一个大的利益相关者可以立即获得大量的投票权。但在信用证明体系下，大股东不能很简单快捷地提高信用评分。在 PoC 中，一个大的利益相关者仍然可以通过分成多个账户和累积信用来获得优势，但是增加和维持信用评分需要时间和精力。当一个大的利益相关者创建并维持了大量高信用账户，这意味着她对网络的贡献比其他人更大，作为回报，她将拥有更多的投票权，这也具有合理性。总的来说，这种简单有效的设计可以极大地缓解贫富不均问题。

7.4 资金库

在之前讨论 PoC 安全性的章节里面，我们提到了系统会收取 10% 的微支付手续费。这里有两个目的。一个是可以防止假账户之间通过互相转账来提高信用记录。另外一个目的就是把手续费汇总起来做成一个资金库。资金库可以有很多不同的用途。

我们可以把一部分资金库用来发展区块链的生态。比如任何一个开发者都可以从资金库里申请一笔基金用来改进生态系统。比如可以开发对用户友好的工具，以及修补系统的安全漏洞等。

我们可以把一部分资金库用来回购 DPR 代币，并销毁。也就是说，这部分的 DPR 将会被兑换成稳定币，当用户销毁了对应的 DPR 以后，就可以获得相应数量的稳定币。这种回购机制可以帮助我们以去中心化的形式有效的控制货币的发行总量。

最后，社区将会接管资金库的运营。社区将通过自治的方式来决定资金库的使用方式。

7.5 信用推荐系统

信用推荐系统是激励更多用户在早期采用 Deeper network 的一种方式。这一节没有被收录在区块链部分，是因为这个系统是独立的并可以在链上或链外实现。想法如下: 信用积分高的账户可以推荐新用户加入网络。高信用积分账户推荐的新用户将以一定的初始信用积分开始。当新用户积累了足够的信用积分，从而达到能够获得区块奖励的阈值后，推荐者的账户也将获得一部分代币奖励。社区可以决定推荐系统生效的时长。例如，如果有效期窗口为 6 个月，那么在此期间之后，推荐者和被推荐者将没有奖励/初始信用积分奖励。

我们在这里定义了几个阈值 $C0 < C1 < C2 < C3$。$C0$ 为被推荐的新用户将收到的初始信用积分。$C1$ 是一个账户可以委托信用积分来获得奖励的阈值。$C2$ 和 $C3$（我们可以有更多层级，为了简单期间，这里只用两层）是一个账户可以推荐新用户的阈值。比如，如果一个账户的信用积分 $>= C2$ 但 $<= C3$，它最多可以推荐 5 个新用户。如果一个账户的信用积分 $>= C3$，它最多可以推荐 10 个新用户。以下是一种可能的链上实现：

1. 赞助者 (即推荐者) 根据确定性密钥方案 (deterministic scheme) 生成推荐密钥，通过私钥签名，并发送到被赞助地址;

2. 一个被赞助地址向智能合约（SC）提交一个推荐密钥，SC 重构签名者 (即赞助者)，检查他们是否有赞助的资格;

3. 如果检查通过，一定的初始信用积分添加到被赞助地址，同时被赞助地址添加到链上（可以储存为映射表，key：赞助者，value：被赞助地址的动态数组）;

4. 赞助者节点随时查询智能合约，检查来自每个被赞助地址的信用积分;

5. 如果被赞助地址信用达到奖励的资格，智能合约发送代币给赞助者作为奖励。

最后两个步骤也可以在链外完成，我们可以使用一个脚本来扫描，然后通过我们自己 (开发者) 的代币账户来奖励合格的赞助者。

8 项目规划

8.1 项目发展路线图

见表 4.

2018 Q3	无锁式操作系统 Atom OS 发布 高性能七层网络安全检测发布 独创三叉戟协议完成
2018 Q4	Deeper Connect 原型机搭载 Atom OS 操作系统研制成功
2019 Q1	Deeper Connect 原型机公网测试，200+ 付费节点参与测试
2019 Q2	与多个硅谷传统创投圈和区块链产业头部机构达成合作
2019 Q3	Deeper Connect Lite 发布
2020 Q1	Deeper Connect Mini 测试完成，批量生产
2020 Q2	Deeper Connect Mini 上线 Indiegogo 平台
2020 Q3	产品上线全球最大 3C 销售平台 BestBuy 与中国移动达成合作，共同开发智慧家庭，智能家居领域的网络安防产品
2021 Q1	Deeper 去中心化公链完成主网上线，并开启挖矿

表 4: 项目发展路线图

8.2 代币经济

我们的代币缩写为 DPR (Deeper Token)。

代币通过以太坊存款的形式，通过法定价值进行发行。

Deeper 项目一共发行的代币总量:100 亿枚。(10,000,000,000).

未发售完的 DPR 代币将被重新分配到“挖矿”和奖励 (bounty) 项目中分配给社区参与者。

8.2.1 代币分配

我们非常感谢我们的主要贡献者 — 各位! 这也是为什么我们决定将 60% 的代币分配给社区、我们的参与者和 Deeper Network 的支持者（见表 5）。通过“分享即挖掘”的理念，您可以毫不费力地享受采矿之旅并从中获利。

分项	分配比例
挖矿	60%
代币私募销售	20%
团队 + 投资人	10%
市场运营 + 合作 + Token Treasure	5%
核心用户 IDO	5%

表 5: 代币分配

附录 A　术语

A. IDO

IDO 模式不从用户手里融资，不为圈钱，只为圈人，圈的人的身份是多重身份，他既是产品的用户使用项目的服务、又是项目的员工可以为项目来进行工作得到报酬、因为奖励的 Token 又相当于项目的股权又有股东的身份。

B. SSS

Secure Shared Service 的缩写。是结合了网络安全，共享经济，区块链技术的新物种。

C. HIPE

HIPE 是 Deeper 独创的数据结构。AtomOS 通过 HIPE 来对共享资源进行管理，可以实现整个网络操作系统无锁化，从而大大提高系统的可靠性，性能和可扩展性。

D. Middleman changes

或称中间人攻击 (英语:Man-in-the-middle attack，缩写:MITM) 在密码学和计算机安全领域中，是指攻击者与通讯的两端分别建立独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制。

E. NAT traversal

NAT 穿越是指连接的服务器处于 NAT 设备之后时的连接建立问题。由于 NAT 之后的设备没有专门的公网 IP 地址，所以需要一些方法来检测是否有内网到公网 IP 和端口的映射关系: 如果有，则可能可以进行直接连接; 如果没有，则可能需要一个中介服务器来完成双向的转发，参见 STUN 协议 [59].

附录 B　免责声明

本白皮书是一份描述我们提出的 Deeper 平台和 Deeper 代币的概念性文件，可以随时修改或者替换。但 Deeper 没有义务更新白皮书或向接收人提供访问任何其他信息的权限。本白皮书不构成在任何司法管辖区 (无论是在美国或其他地方) 购买证券的要约或投资证券的征集，也不构成任何形式的合同。此处提供的信息未经任何监管机构审核。发布和分发本白皮书不得解释为本白皮书符合您所在司法辖区的法律、监管要求、规则和/或法规。对于本文件中描述的信息、陈述、意见或其他事项的准确性或完整性，或其他与项目相关的信息，不做任何陈述或保证。在没有限制的情况下，对于成果和任何前瞻性或概念性陈述的合理性，不作任何陈述或保证。本文件中的任何内容均不是或不应被视为对未来的承诺或陈述。在适用法律允许的最大范围内，对于因本白皮书或其任何方面的任何人所引起或与之相关的任何损失或损害 (无论是否可预见) 的全部责任，不论是由于任何疏忽、违约或未加小心，均予以免责。在责任可能受到限制但未完全免责的情况下，应在适用法律允许的最大限度内加以限制。虽然公司已采取合理步骤以确保此处包含的信息被准确发布且包含在适当的上下文中，但公司未对从第三方外部来源提取的信息进行任何独立审查，也未确认此类信息和其所依据的假设的准确性或完整性。因此，公司没有义务提供有关此类信息的准确性或完整性的陈述或保证的任何更新。此处提供的信息不应被解释或视为有关 Deeper、公司和/或 Deeper 代币的商业，法律，税务或财务建议。如果您不确定相关财务和法律决策，您应向独立的专业顾问 (如财务和法律顾问) 咨询关于 Deeper 代币、Deeper 和/或公司及其各自的经营和业务，以及你所在辖区内的加密货币和其他数字资产的一般状况。须知，您可能被要求无限期承担任何购买 Deeper 代币的法律和财务风险，或承担在不可预见情况或外部因素的干扰下遭受的损失。

参考文献

[1] M. Allman, K. Avrachenkov, U. Ayesta, J. Blanton, and P. Hurtig, "RFC5827: Early retransmit for TCP and stream control transmission protocol (SCTP)," Tech. Rep., 2010.

[2] "Apple Privacy Policy." [Online]. Available: https://www.apple.com/legal/privacy/en-ww/.

[3] "Bitcoin is a Highly Centralized Network, Says Harvard Researcher." [Online]. Available: https://www.ccn.com/bitcoin-highly-centralized-network-says-harvard-researcher/.

[4] "Bitcoin Energy Consumption Index." [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption.

[5] "Bitcoin Market Cap." [Online]. Available: https://coinmarketcap.com/currencies/bitcoin/.

[6] "Block Internet." [Online]. Available: https://en.wikipedia.org/wiki/Block_(Internet).

[7] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch, "Verifiable delay functions," in *Proc. Annual international cryptology conference*. Springer, 2018, pp. 757–788.

[8] L. S. Brakmo and L. L. Peterson, "TCP Vegas: End to end congestion avoidance on a global Internet," *IEEE Journal on selected Areas in communications*, vol. 13, no. 8, pp. 1465–1480, 1995.

[9] "Cardano." [Online]. Available: https://www.cardano.org/en/home/.

[10] N. Cardwell, Y. Cheng, C. S. Gunn, S. H. Yeganeh, and V. Jacobson, "BBR: Congestion-based congestion control," *Queue*, vol. 14, no. 5, p. 50, 2016.

[11] "Cavium™ Unveils 48-core, 2.5GHz OCTEON® III MIPS64 Processor Family: First SoC with Breakthrough Search Processing and Over 100Gbps Single-chip Application Performance for Enterprise, Data-Center and Service Provider Infrastructure." [Online]. Available: https://www.cavium.com/newsevents-cavium-unveils-48-core-octeon-iii-mips64-processor.html.

[12] "Cyberattack." [Online]. Available: https://en.wikipedia.org/wiki/Cyberattack.

[13] "Data Breach." [Online]. Available: https://en.wikipedia.org/wiki/Data_breach.

[14] "Data Breach." [Online]. Available: https://www.privacyrights.org/data-breaches.

[15] R. H. Dennard, F. H. Gaensslen, V. L. Rideout, E. Bassous, and A. R. LeBlanc, "Design of ion-implanted MOSFET's with very small physical dimensions," *IEEE Journal of Solid-State Circuits*, vol. 9, no. 5, pp. 256–268, 1974.

[16] "DPDK." [Online]. Available: https://www.dpdk.org/.

[17] "DPDK Performance." [Online]. Available: https://www.intel.com/content/www/us/en/communications/data-plane-development-kit.html.

[18] "Ethereum," 2013. [Online]. Available: https://github.com/ethereum/.

[19] "Ethereum Market Cap." [Online]. Available: https://coinmarketcap.com/currencies/ethereum/.

[20] S. Frankel, R. Glenn, and S. Kelly, "RFC 3602: The AES-CBC cipher algorithm and its use with IPsec," Tech. Rep., 2003.

[21] L. Gil, "How to configure VPN access on your iPhone or iPad." [Online]. Available: https://www.imore.com/how-configure-vpn-access-your-iphone-or-ipad.

[22] T. Goodwin, "The Battle Is For The Customer Interface," 2014. [Online]. Available: https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/.

[23] "Making it easy to understand what data we collect and why." [Online]. Available: https://safety.google/privacy/data/.

[24] M. Gromek, "Are The Crazy Rides Of Bitcoin Controlled By The Invisible Hand Of The Market?" 2018. [Online]. Available: https://www.forbes.com/sites/michalgromek/2018/07/23/are-the-crazy-rides-of-bitcoin-controlled-by-the-invisible-hand-of-the-market.

[25] D. Gudkova, M. Vergelis, T. Shcherbakova, and N. Demidova, "Spam and Phishing in 2017," 2018. [Online]. Available: https://securelist.com/spam-and-phishing-in-2017/83833/.

[26] S. Ha, I. Rhee, and L. Xu, "CUBIC: a new TCP-friendly high-speed TCP variant," *ACM SIGOPS operating systems review*, vol. 42, no. 5, pp. 64–74, 2008.

[27] "Hashrate Distribution." [Online]. Available: https://www.blockchain.com/en/pools?timespan=4days.

[28] A. Hertig, "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular." [Online]. Available: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/.

[29] A. Hertig, "Major Blockchains Are Pretty Much Still Centralized, Research Finds." [Online]. Available: https://www.coindesk.com/major-blockchains-pretty-much-still-centralized-research-finds/.

[30] "Internet Assigned Numbers Authority." [Online]. Available: https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority.

[31] C. India, "Privacy Awareness Week-Are We Responsible for Our Data Breach?" [Online]. Available: https://securingtomorrow.mcafee.com/consumer/privacy-awareness-week-are-we-responsible-for-our-data-breach/.

[32] "Internet Censorship." [Online]. Available: https://en.wikipedia.org/wiki/Internet_censorship.

[33] V. Jacobson, "Congestion avoidance and control," in *Proc. ACM SIGCOMM computer communication review*, vol. 18, no. 4. ACM, 1988, pp. 314–329.

[34] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols," in *Secure Information Networks*. Springer, 1999, pp. 258–272.

[35] A. Johnson, "Trump Signs Measure to Let ISPs Sell Your Data Without Consent," 2017. [Online]. Available: https://www.nbcnews.com/news/us-news/trump-signs-measure-let-isps-sell-your-data-without-consent-n742316.

[36] P. Kennedy, "AMD EPYC Rome Details Trickle Out 64 Cores 128 Threads Per Socket." [Online]. Available: https://www.servethehome.com/amd-epyc-rome-details-trickle-out-64-cores-128-threads-per-socket/.

[37] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, 2012.

[38] M. Kosinski, D. Stillwell, and T. Graepel, "Private traits and attributes are predictable from digital records of human behavior," *Proceedings of the National Academy of Sciences*, p. 201218772, 2013.

[39] "List of Websites Blocked in India." [Online]. Available: https://en.wikipedia.org/wiki/Websites_blocked_in_India.

[40] "List of Websites Blocked in Russia." [Online]. Available: https://en.wikipedia.org/wiki/List_of_websites_blocked_in_Russia.

[41] "List of Data Breaches." [Online]. Available: https://en.wikipedia.org/wiki/List_of_data_breaches.

[42] "List of TCP and UDP Port Numbers." [Online]. Available: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

[43] "Lock (computer science)." [Online]. Available: https://en.wikipedia.org/wiki/Lock_(computer_science).

[44] C. Malmo, "One Bitcoin Transaction Consumes As Much Energy As Your House Uses in a Week." [Online]. Available: https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change.

[45] L. Mathews, "Phishing Scams Cost American Businesses Half A Billion Dollars A Year." [Online]. Available: https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year.

[46] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Proc. Conference on the theory and application of cryptographic techniques*. Springer, 1987, pp. 369–378.

[47] "Mirai Source Code." [Online]. Available: https://github.com/jgamblin/Mirai-Source-Code.

[48] S. Morgan, "Cybercrime Damages $6 Trillion By 2021," 2017. [Online]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[49] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009. [Online]. Available: http://bitcoin.org/bitcoin.pdf.

[50] "Network address translation." [Online]. Available: https://en.wikipedia.org/wiki/Network_address_translation.

[51] M. Orcutt, "Hijacking Computers to Mine Cryptocurrency Is All the Rage," 2017. [Online]. Available: https://www.technologyreview.com/s/609031/hijacking-computers-to-mine-cryptocurrency-is-all-the-rage/.

[52] J. Padhye, V. Firoiu, D. F. Towsley, and J. F. Kurose, "Modeling TCP Reno performance: a simple model and its empirical validation," *IEEE/ACM Transactions on Networking (ToN)*, vol. 8, no. 2, pp. 133–145, 2000.

[53] PeckShield, "EPoD: Ethereum Packet of Death (CVE-2018 - 12018)." [Online]. Available: https://medium.com/@peckshield/epod-ethereum-packet-of-death-cve-2018-12018-fc9ee944843e.

[54] "Phishing." [Online]. Available: https://en.wikipedia.org/wiki/Phishing.

[55] M. Rechtoris, "Data breaches cost healthcare industry $6.2B." [Online]. Available: https://www.beckersasc.com/asc-turnarounds-ideas-to-improve-performance/data-breaches-cost-healthcare-industry-6-2b-4-points.html.

[56] D. Reed *et al.*, "RFC 1459: Internet Relay Chat Protocol," 1993.

[57] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[58] L. Rokach and O. Z. Maimon, *Data mining with decision trees: theory and applications*. World scientific, 2008, vol. 69.

[59] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy, "RFC3489: STUN-Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)," 2003.

[60] S. J. Russell and P. Norvig, *Artificial intelligence: a modern approach*. Malaysia; Pearson Education Limited,, 2016.

[61] T. Schleifer, "Uber' s latest valuation: $72 billion." [Online]. Available: https://www.recode.net/2018/2/9/16996834/uber-latest-valuation-72-billion-waymo-lawsuit-settlement.

[62] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE mobile computing and communications review*, vol. 5, no. 1, pp. 3–55, 2001.

[63] C. Shapiro, S. Carl, H. R. Varian *et al.*, *Information rules: a strategic guide to the network economy*. Harvard Business Press, 1998.

[64] O. Solon, "Facebook Says Cambridge Analytica May Have Gained 37M More Users' Data." [Online]. Available: https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought.

[65] "Study: Attack on KrebsOnSecurity Cost IoT Device Owners $323K," 2018. [Online]. Available: https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot-device-owners-323k/.

[66] B. Sullivan, "Online Privacy Fears Are Real." [Online]. Available: http://www.nbcnews.com/id/3078835/t/online-privacy-fears-are-real/.

[67] T. Team, "As A Rare Profitable Unicorn, Airbnb Appears To Be Worth At Least $38 Billion." [Online]. Available: https://www.forbes.com/sites/greatspeculations/2018/05/11/as-a-rare-profitable-unicorn-airbnb-appears-to-be-worth-at-least-38-billion.

[68] "Timeline of computer viruses and worms." [Online]. Available: https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms.

[69] J. Tuwiner, "Bitcoin Mining in China," 2018. [Online]. Available: https://www.buybitcoinworldwide.com/mining/china/.

[70] "Oracle VM VirtualBox." [Online]. Available: https://www.virtualbox.org/.

[71] "WAN optimization." [Online]. Available: https://en.wikipedia.org/wiki/WAN_optimization.

[72] "Websites Blocked in Mainland China." [Online]. Available: https://en.wikipedia.org/wiki/Websites_blocked_in_mainland_China.

[73] S. Williams, "4 Reasons I'll Never Invest in Bitcoin (and You Shouldn't Either)." [Online]. Available: https://www.fool.com/investing/2017/06/14/4-reasons-why-ill-never-invest-in-bitcoin-and-you.aspx.

[74] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "Hotstuff: Bft consensus in the lens of blockchain," *arXiv preprint arXiv:1803.05069*, 2018.

[75] M. Zomorodi, "Do You Know How Much Private Information You Give Away Every Day?" [Online]. Available: http://time.com/4673602/terms-service-privacy-security/.