

ISP • 信息共享协议

基于零仲裁证明的 ISP 价值协议

摘要

本文介绍了一个基于零仲裁证明的共享 ISP（Information sharing protocol）价值协议。支持所有智能设备共享其 ISP 价值，并完成价值交易。在交易过程中，协议将提供完善的解决方案，涵盖了价值登记认证、价值匹配使用和价值链上验证。

我们尤其为协议的使用者提供了完备的底层基础技术调用能力，通过调用这部分技术，可以加速商业化落地，使当前任何基于移动互联网提供的应用服务，均可以在本协议的基础上，无需二次开发，即可完美调用 ISP 价值协议的应用云技术服务。由此，基于本协议可以帮助参与者创造出众多令人兴奋的、具有颠覆性的新型商业服务。

目录

目录.....	3
1. 背景.....	6
2. 协议设计.....	7
2.1. 市场现状.....	7
2.2. ISP 价值协议使用流程.....	9
2.3. ISP 价值登记.....	10
2.4. ISP 价值使用.....	11
2.4.1. 矿工匹配.....	11
2.4.2. 费率介绍.....	12
2.4.3. 应用云技术服务内容.....	14
2.4.4. 应用云技术服务原理.....	15
2.5. ISP 价值验证.....	16
2.5.1. 零仲裁证明的思想.....	17
2.5.2. 零仲裁证明的应用.....	17
2.5.3. 零仲裁证明的算法.....	18
2.6. 防作弊和防攻击.....	19
2.6.1. ISP 价值作弊.....	19

2.6.2. 尘埃订单攻击.....	20
2.6.3. 矿工拒绝上链.....	21
2.6.4. 共享设备提供低质服务.....	21
3. 协议落地场景.....	22
3.1. 广告领域.....	22
3.1.1. 互动式广告.....	22
3.1.2. 去中心化应用市场.....	23
3.2. 游戏领域.....	23
3.2.1. 游戏试玩服务.....	23
3.2.2. 手游挂机交易服务.....	24
3.3. 电商领域.....	24
3.3.1. 手游账号买卖服务.....	24
3.4. 其他领域.....	25
3.4.1. App 内测服务.....	25
3.4.2. 科学研究服务.....	25
3.4.3. 分布式视频转码.....	26
3.4.4. 多屏互动娱乐.....	26
3.4.5. 视频交互直播.....	26

4. ISP 代币.....	27
4.1. 什么是 ISP 代币.....	27
4.2. ISP 应用场景.....	27
4.3. ISP 分配方案.....	29
4.4. ISP 发行计划.....	29
5. 开发路线图.....	29
6. 风险提示.....	31
6.1. 反洗钱规定.....	31
6.2. 反资助恐怖主义（CFT）.....	31
6.3. 购币者限制.....	32
6.4. 文档声明.....	32

1. 背景

从 2009 年，中本聪正式发布《比特币：一种点对点的电子现金系统》起，到 2014 年，Vitalik Buterin 受比特币启发，提出“下一代加密货币与去中心化应用平台”即“以太虚拟机”Ethereum Virtual Machine 来处理点对点合约。越来越多人高度认可由区块链改变价值传递方式而带来的系统性社会变革。但是当前区块链依然面临一个重要问题：如何将区块链技术扩展到现实世界更多的应用场景里，即区块链如何与链下信息进行可验证的有效共识。

解决区块链与链下信息进行可验证的共识问题，将会为区块链技术的普适性带来更广阔的市场，尤其是在共享经济领域。我们相信基于区块链技术的共享经济服务将会是一个明显的趋势，它天然具有去中心化的特点，一方面基于分布式账本创建去信任的服务可以降低参与者的信任成本；另一方面服务资产化，资产代币化后可以依靠其全球性、全天候的特点为共享经济提升交易的流动性。

现阶段共享算力服务+区块链技术是区块链+共享经济典型应用场景之一。目前普遍的共享算力区块链类项目呈现几个显著问题：

1. 共享算力所提供的服务难以差异化。和中心化算力相比，目前所有区块链共享算力项目所提供的服务不具有创新性的差异化特点，这也导致基于这类项目所提供的服务无法具有独特的商业模式和产品创新，甚至还有性能和稳定性方面的劣势。

2. 链外数据难以验证。由于共享算力必须在链外进行数据交互，因此如何对链外数据可以在区块链上达成统一共识是所有共享项目面临的共同问题。

本文介绍的基于零仲裁证明的共享 ISP 价值协议就是为了彻底解决上述问题。

ISP 价值，即 Information sharing protocol 所带来的使用价值，它是智能设备客观运行能力的一种具象化总结，是智能设备独特能力的一种集中体现。

ISP 价值协议的核心优势是将 ISP 价值结合创新性的云应用技术服务，为其他合

作方调用本协议提供独特的产品服务，从而带来全新的商业模式改变。并依靠创新的零仲裁证明解决链外数据验证问题，使所有交易数据无争议，可以被链上所有节点共同验证。

上述核心优势将会促进共享经济+区块链交易具有更大、更广阔的市场前景，并为区块链解决链外数据验证问题提供全新的解决思路。

2. 协议设计

2.1. 市场现状

随着传统互联网进入公认的“下半场”发展阶段，线上流量吃紧，线下成本昂贵已经成为困扰所有互联网企业的一大心病。为此，众多公司提出了不同的解决方案，希望能破局突围。

- 微信——小程序

2017 年 1 月微信小程序正式上线，其背后的设计思想是用户即点即用，用完即走，希望通过提高 App 的使用效率来提高用户的体验，并为 App 探索新的出路。截止到 2018 年，已上线 58 万个微信小程序，日活 1.7 亿用户，引流能力已不容小觑。

- 手机联盟——快应用

微信小程序的崛起也让国产手机厂商产生了压力。2018 年 3 月 19 日，小米、中兴、华为、金立、联想、魅族、努比亚、OPPO、vivo 九大手机厂商将共同发起快应用标准。与微信小程序背后的设计理念一致，希望通过提供即点即用的新型应用服务，赋能开发者以标准化的方式接入，拓展更多场景。

- Google——即时应用（Instant App）

在国外，基于类似免下载即点即用理念改造 App 的市场也蓬勃发展。如美国的

mNectar、CrossInstall、法国的 Playdigious 等，其中尤其以 Google 的即时应用（Instant App）最受瞩目。Google 已经将即时应用（Instant App）功能应用在游戏中。这意味着玩家只需轻轻一点，无需下载，便可马上体验游戏。

通过上述市场变化我们可以预见，在未来将会有越来越多的公司切入到这个领域，并由此带来巨大的行业性变革。很幸运，我们在此领域也拥有数年的技术积累，并且相比目前市场上主流的解决方案，我们拥有非常大的技术优势：

	二次开发	应用范围	客户端支持
微信-小程序	需要	轻量级应用，不适合大型游戏	支持 iOS 和 Android 用户
手机联盟-快应用	需要	轻量级应用，不适合大型游戏	仅支持 Android 用户
Google- 即时应用 (Instant App)	需要	部分适合	仅支持 Android 用户
ISP	不需要	适合所有应用及大型游戏	支持 iOS 和 Android 用户

基于我们的技术积累，结合区块链所带来的技术更新，我们创造出安全性更高，流通性更广，激励性更强的全新服务协议——ISP 价值协议。

基于 ISP 价值协议，我们将搭建完备的价值交易流程，为参与者提供全方位的服务。



2.2. ISP 价值协议使用流程

在 ISP 价值协议里，我们定义三个参与者：

- 共享设备方：提供 ISP 价值的参与者，将会获得一定数量的代币激励；
- 使用者：消耗使用 ISP 价值的参与者，并为其使用支付一定的代币；
- 矿工：矿工执行匹配服务，为 ISP 价值的使用者匹配到最合适的设备，并在交易完成后将零仲裁证明的结果上链记录；

三个参与者共同完成下列使用流程：

S0: 共享设备方、使用者、矿工均需要调用 ISP 智能合约，并抵押一部分代币完成角色注册。

S1: 使用者通过区块链调用 ISP 智能合约创建一个订单，订单包括：为矿工所支付的费用、为共享设备方所支付的费用、服务使用时长、服务筛选条件、所选矿工等信息。

S2: 矿工监听区块链上的订单。

S3: 使用者在创建订单后与矿工建立连接，向矿工传递订单号。 **S4:** 矿工验

证订单信息，确定当前服务无误。

S5: 矿工开始执行订单的筛选条件, 选出一个符合条件的共享设备方, 并确定设备状态。

S6: 矿工将设备信息发送给使用者, 使用者开始与共享设备方通讯。 S7: 使用者开始执行订单前, 向共享设备方请求获得一个资源 R 。

S8: 共享设备方将该资源拆分为若干份, $R = [R_1, R_2, \dots, R_n]$ 。

S9: 共享设备方提供资源 R_1 后, 向使用者发起一个待确认的承诺 P_1 , 即使用者承诺承认收到 R_1 , 并会为此付费 V_1 。

S10: 当使用者收到 P_1 后, 验证 P_1 内容, 用使用者的私钥对 P_1 签名得到 P_1' , 并将 P_1' 发送给共享设备方。

S11: 共享设备方收到使用者已签名的承诺 P_1' , 则继续发送下一个资源 R_2 , 并重复 S9-S10, 直至完成最后一份资源 R_n 的发送, 获得最终结果 P_n' 。

S12: 共享设备方将最终的 P_n' 广播给所有矿工。

S13: 执行匹配设备的矿工通过调用智能合约将 P_n' 写入区块链, 以完成支付及相关数据记录。

2.3. ISP 价值登记

ISP 价值协议通过对不同智能设备所提供的 ISP 价值进行定向多维度测算, 定义了参与共享的智能设备 ISP 潜在可利用的数字化价值。ISP 价值协议试图在区块链世界建立一个具有普适性的 ISP 价值度量测算方案, 将每个智能设备进行多维度登记, 为 ISP 价值协议提供统一的价值衡量基础。

ISP 价值协议会提供测试程序对每个共享设备进行能力测量，测量后得到一个能力集合：

Map:

```
{  
  cpu:valuec, gpu:valueg,  
  ram:valuer, storage:values, bandwidth:valueb,  
  ...  
}
```

上述能力测量，依靠共享设备运行 ISP 客户端程序完成，并在执行完成后，调用链上 ISP 智能合约完成设备注册。

4. ISP 价值使用

在 ISP 价值协议中，矿工是重要的参与者，他负责将订单与合适的设备进行匹配，并最终完成上链记录。矿工在完成设备匹配后，ISP 价值将正式被使用方使用，在这过程里，ISP 价值协议将提供完善的底层技术服务供使用方轻松调用。

因此一个 ISP 价值使用的过程，可以看做是一个矿工执行一次匹配订单，并由使用者调用 ISP 底层技术服务的过程。

1. 矿工匹配

● 注册矿工

任何人在提供了满足 ISP 指定的设备硬件条件后，均可以发起注册请求，成为 ISP 价值协议中矿工的一员。注册流程如下：

S1: 安装并运行 ISP 矿工服务端程序。

S2: 按要求提供区块链账户地址，并确保地址内的指定代币数量不低于 S 值。

S3: 调用 ISP 在区块链上的智能合约，使用账户地址完成矿工信息注册。

● 选择矿工

由于 ISP 价值协议是完全去中心化的价值协议，因此我们不对某个时间段内执行订单的矿工做任何形式的指定操作。即所有的矿工的选择将交由使用者在智能合约里完成选择。

同时，我们将对使用者在智能合约内选择矿工的行为做“强制平均”的约束。即使用 ISP 价值协议创建订单的使用者需要确保历史累计选择的矿工分布是呈现平均分布的状态，即严禁出现选择矿工执行订单时的最终矿工分布呈现明显偏向性。

由于执行订单的矿工是由使用者通过“强制平均”选择出来的，因此可以避免出现如下情况：

- 少数矿工垄断 ISP 价值协议订单的情况。
- 矿工间恶性竞争的情况。
- 无效服务的情况。将矿工收益与匹配设备相挂钩，鼓励矿工提高设备匹配效率，从而提高服务质量

2.4.2. 费率介绍

使用者建立订单时需要标识两笔支出：付给矿机的匹配服务费 E_1 和付给设备的服务费 E_2 ，其中 E_1 为固定值由社区确定。 E_2 由使用者自由给出。

现有一笔订单，由使用者指定矿机 M_a 进行匹配。矿机 M_a （直连设备数为 m ）可能会为使用者匹配到直连到该矿机的设备 D_{ai} 。 D_{ai} 所要求的服务费为 E_{ai} ，则：

$$E_{ai} \leq E_2, i \in (1, m) \text{ 且 } i \in N$$

此时，使用者的付给设备的服务费意愿 E_2 与设备所要求的服务费 E_{ai} 差额

($E_2 - E_{ai}$) 归矿机 M_a 所有，故

$$E_{M_a} = E_1 + E_2 - E_{ai}$$

矿机 M_a 也可能会为使用者匹配到直连到矿机 M_b (直连设备数为 n) 的设备 D_{bj} 。

则：

$$E_{bj} \leq E_2, j \in (1, n) \text{ 且 } j \in N$$

此时，由于设备 D_{bj} 是直连到 M_b 的， M_b 会要求一定比例 $\omega_b\%$ 的分润 (该比例由矿机自行确定)： $E_M = \omega_b\%(E_2 - E_{bj})$ 。矿机 M_a 得到的利润为：

$$E_M = E_1 + (1 - \omega_b\%)(E_2 - E_{bj})。$$

矿机 M_a 为了使得自己的利润最大化，会在要求的响应时间内，搜索矿机 a, b, c, \dots 下的设备，并匹配其中使得自己利润最大化的设备 D_{qk} (D_{qk} 直连矿机 M_q ，直连设备数为 $l, q \in (1, l) \text{ 且 } q \in N$)，使得自己得到的利润为：

$$E_{M_a} = E_1 + \max \{ \max_{i=1}^m (E_2 - E_{ai}), \max_{j=1}^n (1 - \omega_b\%)(E_2 - E_{bj}), \dots, \max_{k=1}^l (1 - \omega_q\%)(E_2 - E_{qk}), \dots \}$$

上述经济模型的意义：

- E_i 并非主要利润来源，是为了防止尘埃攻击
- 矿机得到了有效激励。
- 给矿机提供了提高自己性能的动机：高性能能在要求的响应时间内搜索到更有利于利润最大化的设备，高性能能吸引更多的设备直连自己。
- 高性能的矿机可以更好地服务社区，从而吸引更多参与者。形成正向循环。

2.4.3. 应用云技术服务内容

应用云技术核心为开发者使用共享 ISP 价值提供了具有颠覆性的服务体验。这部分服务包括：

1. 应用云端化部署

依托 ISP 团队的技术积累，可以实现目前所有的智能 App 无需二次开发，直接完成云端化部署。从而减少开发者调用服务过程中的工作量，提高 ISP 价值协议的使用效率。

2. 智能云场景定制

通过 ISP 网络共享的设备 ISP 可以被精准调用，并且参与更为智能化的定制服务。智能云场景支持开发者对 App 运行的内容进行智能定位，可以自动执行若干应用内场景，为用户直接展示定制化的应用画面。

3. 应用云端化操作

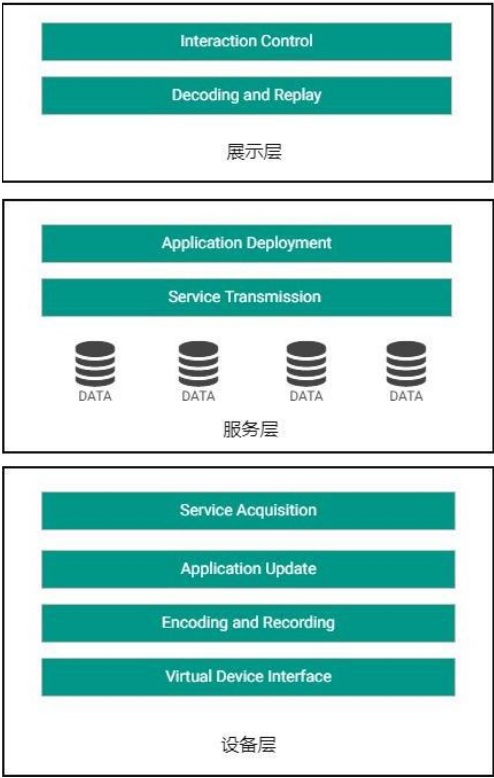
通过应用云技术完成部署的 App，可以实现在任何地方无需下载、无需安装，即点即玩，甚至是打开一个 URL 就可以即点即玩皇室战争等移动游戏。

4. 分布式 ISP 调用

基于 ISP 网络对智能设备的支持，将为开发者提供丰富的 ISP 价值调用服务，减轻开发者在 ISP 层面的成本问题，并为支持更大型应用服务提供强有力的分布式 ISP 价值支持。

2.4.4. 应用云技术服务原理

在 ISP 价值协议提供的应用云技术服务架构里，分为三个层级，从下到上依次为：设备层、服务层、展示层。



● 设备层

Virtual Device Interface: 虚拟设备接口，用于管理调度设备层内所有资源，使 ISP 价值高效的在各个环节里完成流动；

Encoding and Recording: 音视频编码，录制

Application Update: 应用更新服务，即当存在应用更新时，在设备层完成应用的统一化更新。更新分两类：增量更新和全量更新，由使用方触发相应的更新指令；

Service Acquisition: 服务采集，此部分将承担双向采集检测服务，即设备层传递上来的动态流媒体信息和展示层传递来的动态指令信息。具体来说，设备层通过服务层的服务采集感测是否有来自展示层的输入，以获取输入数据，并将触发后的流媒体信息再通过服务采集完成输出；

- 服务层

Service Transmission: 服务传送，此部分负责将转码后的动态流媒体信息由服务层传送到展示层；

Application Deployment: 应用部署服务，可以实现无需二次开发即自动完成部署；

- 展示层

Decoding and Replay: 解码和重放，利用此服务将服务层编码过的应用视频和音频进行解码，并渲染为可在任何设备展示的文件格式。

Interaction Control: 交互控制，收集和传递用户的交互行为

2.5. ISP 价值验证

现有的智能合约存在缺陷，只能解决特定的场景问题：数据存在于区块链上且是可以验证的。如果数据在区块链之外，或者虽然数据在区块链上但是无法验证，那么智能合约就无法使用。

在 ISP 价值协议内，需要大量验证链外的数据，因此 ISP 价值协议提供了一种解决链外数据验证的新方法——零仲裁证明。

1. 零仲裁证明的思想

零仲裁证明的思想，来自现实世界中的交易的启发。

假设 A 和 B 是交易的双方，A 是商品的卖方，B 是买方，双方距离非常远，无法当面交易，而且双方此前从未交易过，对对方的信誉也一无所知。A 和 B 要完成交易，主流的方式是：通过双方都信任的第三方中介 C 进行交易，B 先将钱交给 C，随后 A 发货给 B，B 确认后，C 再将钱给 A。还有一种用的比较少的方式：A 先发少量的货给 B，B 付钱后，再发少量的货给 B，B 再次付钱后，A 再次发少量的货.....这其实是双方建立信任的过程。如果 A 发货后，没有收到钱，那么后继交易自动终止，A 只是损失最后一次货物。

AB 双方在没有引入第三方中介的情况下，以很小的风险，完成了交易，这就是一种零仲裁证明的实现。

第二种交易方式面临的问题是：多次交易的成本如果比一次交易的成本高很多（商品运输的费用，货币转账的费用），双方就不会采用这种方式。

幸运的是：1.很多商品或者服务，已经可以数字化，而数字化的传递成本更低。
2.以数字加密货币为代表的区块链方案，相比传统跨境等转账方式，已经将货币转账的费用大幅度降低。因此增量交易的方案在区块链上就可以实现。

2. 零仲裁证明的应用

零仲裁证明的核心是增量承诺算法，正如其名字所示，适合那些可以把大交易分成多个小交易的场景。例如服务的时间、距离、带宽等。如果一个交易，无法分割，就不适合。如房产的交易，只有一个最终的结果，无法采用增量承诺算法。

我们现在假设有一个叫 DUber 的共享出行项目采用了零仲裁证明方案：

司机端的数据（如地理位置、在线状态）实时上链，乘客端的数据（如出发点、目的点灯）也实时上链。建立一个智能合约，撮合司机和乘客。撮合成功后，司

机端的 GPS 数据不停的发给乘客端，乘客端比较数据后，发承诺 P_x 给司机端。

最终，司机端把 P_x 上链，智能合约以 P_x 来结账。

这样，完全不需要一个中心化的系统来提供服务。

2.5.3. 零仲裁证明的算法

在一般交易过程中，交易双方很可能对于交易行为进行否认，例如买方否认收到货物而拒绝付款，一般解决交易纠纷的方式就是仲裁，仲裁需要交易双方提供可验证的证明。然而并非所有的交易都能提供可验证的证明，也可能提供证明及验证需要耗费大量的资源。

有一种可以在即使存在双方作弊的情况下也能将损失降低的方案：双方以更小的交易粒度进行交易。一旦某次交易失败，则后续交易停止，这样双方只会在最后一次交易出现争议。当交易粒度足够小，这种损失也将变得微不足道。

然而在此过程中将产生大量微交易，在实际交易存在开销（手续费等）的情况下，交易粒度将会被限制，特别是在区块链中，更小粒度的交易开销将变得难以接受。

为解决上面的问题，我们引入了一种新的算法：增量承诺算法。

增量承诺算法，要求交易双方在资源交易的过程中严格执行以下步骤：

S1：资源使用者 A 向资源提供者 B 请求资源 R

S2： B 以 A 和 B 的地址，当前时间戳 ts 及一个随机 $salt$ 来生成当前交易的唯一标识 TID （Transaction ID），并将 TID 发送给 A

$$TID = H(addrA, addrB, ts, salt)$$

S3： B 将资源 R 分成若干份

$$R = [R_1, R_2, \dots, R_n]$$

S4: B 向 A 提供资源 R_x ，并向 A 请求得到承诺 P_x : A 承认收到之前 $\sum_{i=1}^x R_i$ ，并会为此付费 V_x

$$P_x = \left\{ TID, addrA, addrB, V_x, \sum_{i=1}^x R_i \right\}$$

S5: 当 A 收到 P_x 后，验证 P_x 内容，用 A 私钥对 P_x 签名得到 P'_x ，并将 P'_x 发送给 B

$$P'_x = \text{Sign}(P_x, Key_A)$$

S6: B 收到 A 已签名的承诺 P'_x ，则继续发送下一个资源 R_{x+1} (跳到步骤 4)，否则进入下一个步骤

S7: B 完成或中断交易，并将最后一次收到的 P'_x 放到区块链上进行验证

S8: 区块链验证 P'_x 内容并检查 TID 是否唯一，通过后根据内容执行相关的合约

在此交易过程中，无论交易粒度划分多小，实际只执行一次交易，开销很低，并且交易内容不可否认。在整个过程中都不需要第三方的介入，而且可以实时验证。

6. 防作弊和防攻击

1. ISP 价值作弊

ISP 价值协议力求确保每一个智能设备所提供的 ISP 价值都是真实可信的，这是打造公平健康生态的基础。目前可以预见的 ISP 价值作弊分为两种：设备信息伪造和一机多记（即一台设备伪造独立设备登记多次）。

针对设备信息伪造，我们提供如下方案防止作弊：

1. 建立完备的市场设备信息仓库。针对目前市场上可以共享加入 ISP 价值协议的智能设备，收集整理完备的设备信息情况数据。当执行 ISP 价值测量 App 时，检测实际设备的核心软硬件数据是否与仓库内数据一致，当数据不一致时，拒绝接受该设备。
2. 标识模拟器设备。ISP 价值协议允许 PC 或服务器接入共享 ISP 服务，但是针对他们所模拟出来的环境将会做智能标识，识别出设备的真实状态。
3. 随机性复测。已经通过登记进入 ISP 价值协议内的智能设备，我们将不定期的对包括但不限于硬件数据、带宽数据、系统数据等进行随机复测，当复测结果与初次结果不一致时，将回退该设备的 ISP 资源，并没收其锁定的保证金代币。
4. 建立设备黑名单。针对每个设备，我们将建立唯一的标识 ID，对于频繁作弊的设备，将列入黑名单，不再接受其任何共享请求。

针对智能设备一机多记，我们提供如下方案防止作弊：

1. 建立全网唯一标识。我们将根据设备的综合属性，建立全网唯一标识，当出现疑似一机多记时，再对设备拥有者进行二次确认。
2. 设立代币锁仓保证金。所有参与共享的智能设备，需要绑定钱包地址，并且确保钱包地址内 ISP 代币数量 $S \geq YN$ ，其中 N 为共享的设备数量，Y 为单台设备固定数量的 ISP 代币。

2.6.2. 尘埃订单攻击

ISP 价值协议的使用者可以通过发起大量的尘埃订单（即服务时长非常短，单次价格非常低）试图对矿工发起攻击。不过由于匹配尘埃订单的获利是固定的，即矿工单次匹配订单的利润与订单具体的服务时长、单次价格等参数无关，因此矿工不会受到尘埃攻击的影响。

当 ISP 价值协议的使用者利用尘埃订单对 ISP 价值协议发起攻击时，如果服务时长非常短，那么设备的占用状态会被迅速释放，因此不会出现协议内大量设备异常使用。如果单次价格非常低，此时无论服务时长多久，都会被共享设备方拒绝提供服务，因此不会产生实质性的攻击影响。

3. 矿工拒绝上链

在正常情况下，注册成为 ISP 价值协议的矿工默认是接收所有协议约定，并按照“谁匹配谁上链”的原则将其匹配完成的设备所执行的增量承诺结果（即订单结果）上链记录。由于每次增量承诺的执行结果，均是由当前匹配的矿工完成上链，其他的矿工进行记录，当存在某个坏矿工拒绝为某次订单提供上链服务时，此时在超过有效上链时间 T_s 后，任何其他的矿工均可以进行抢先交易，谁先完成上链记账，谁最终获得有效报酬。

4. 共享设备提供低质服务

一个健康的生态，需要有稳定健康且优质的服务。在 ISP 价值协议中，在写入区块时，我们会对共享设备的每一次订单执行情况进行拆分记录，记录的数据包括：

- 执行订单的次数 N
- 提供服务累计时长 T
- 完成服务的总价值（代币数量） S

这些统计结果可以由任意矿工从区块上获取，并通过函数计算活动设备健康情况的有效反馈：

$$Q = f(N, T, S)$$

而所有提供低质服务的设备，矿工有权利降低其在匹配订单时候的优先级。

3. 协议落地场景

当前互联网有三大已经得到验证的商业模式：广告、游戏、电商。但是随着互联网进入下半场，三大商业模式也逐渐暴露出转化效率低下、产品创新不足、运营成本较高等问题。

面对新的问题，ISP 价值协议可以为三大商业模式提供全新的技术解决方案，助力商业模式革新，提高运营效率。

以下我们试列举部分落地场景旨在抛砖引玉，我们相信在整体市场追求应用使用效率提升、追求用户体验提升的大环境下，未来基于 ISP 价值协议的落地场景将会更多，应用范围将会更广，为合作方所带来的收益将会更大。

1. 广告领域

1. 互动式广告

传统的移动互联网广告模式大致可以分为三类：文字广告、图片广告和视频广告。三者共同特点均是用户被动接受广告信息，通过有限的富媒体内容来决定是否下载安装广告内容。

未来基于 ISP 价值协议，将会诞生全新的移动互联网广告模式——互动式广告。互动式广告是指用户无需下载，无需安装，可以像在线播放视频一样实现对广告 App 的即点即玩。从体验上来说，使用户由被动接受，变为主动探索，在最短的时间内让用户通过真实的体验去感知 App 的内容，继而做出是否下载安装的决定。

目前被动式的广告推广使得市场大量存在过度宣传、夸大宣传等，用户常常被精美的海报吸引，但是下载安装后又高呼“上当”，从而导致 App 的留存和付费结果差强人意。而全新的互动式广告将彻底解决这个问题，大幅度提高用户留存率和付费转化率等多项数据，为广告市场带来全新的活力。

3.1.2. 去中心化应用市场

目前传统的应用市场有两大弊端：

1. 高度中心化，应用的分发权掌握在应用市场管理者手中，由此导致流量的展示不是根据游戏的好坏，而是根据运营和推广费用进行倾斜，使大量小而美但推广费用捉襟见肘的好应用无法脱颖而出；
2. 用户体验差，目前应用所占的资源越来越多，单个应用的安装包也越来越大，而用户对一个应用自己是否愿意下载的判断依然停留在非常简单粗暴的“看图说话”程度，无法真实体验，可能导致下载后才发现不是自己喜欢的类型，浪费大量资源和时间。

基于 ISP 价值协议的去中心化市场，可以完美解决上述问题。未来任何一个移动 App 都可以成为一个应用市场，一个真正人人拥有，人人管理的去中心化应用市场。同时依靠云应用技术服务，可以实现所有应用市场的应用无需下载、无需安装，即点即玩，从而为用户提供颠覆性的应用市场体验。

2. 游戏领域

1. 游戏试玩服务

一款游戏的受欢迎的程度大致上取决于它对用户心理的捕捉。因此越来越多游戏厂商在游戏开发过程里纷纷引入用户内测试玩的服务，用以获取用户反馈。但是传统的游戏试玩，需要将安装包公开出去，用户获得安装包后再安装体验，这就为泄密和知识产权保护带来了挑战，尤其对中小型开发者以及个人开发者。

未来基于 ISP 价值协议的游戏试玩服务，可以完美解决上述问题。游戏开发者不再需要公开游戏安装包，甚至仅需要在微信里向用户发送一个 URL，就能让用户进入体验游戏，继而获得用户的真实反馈。这将大大缩短用户反馈获取的时间，同时降低在用户反馈上产生的成本，并且高度保障游戏信息安全。

同时，游戏试玩还可以应用在其他领域，可以让用户即点即玩，先玩后下载，真正掌握决策权，提升整体体验。

3.2.2. 手游挂机交易服务

手机挂机，即通过一些特定软件，模拟玩家在手游中的操作，实现玩家在非游戏时段对游戏自动操作，从而快速提高游戏等级、装备数量、材料数量以及金币数量等。

目前随着手机游戏的蓬勃发展，手游挂机已经演变为一个巨大的市场。拥有众多需求明确的用户支持。在传统挂机市场，提供挂机服务的公司需要自己采购大量的硬件设备来提供稳定的服务，并且成本会随着挂机需求量的增加而增加。

未来通过 ISP 价值协议，可以方便的接入庞大的手机资源，让提供挂机服务类的公司服务器成本大幅度降低，用户挂机体验得到提升。

3. 电商领域

1. 手游账号买卖服务

在手游账号买卖交易里，二手账号的价值大约是玩家充值比例的 30%-40%，按照 2016 年手游市场约 600 亿的充值金额来算，手游账号交易平台至少帮助玩家回收 180 亿的游戏成本。

手游账号二手交易能进一步刺激游戏玩家的活跃度。被出售的账号会在新玩家手中继续发挥最大价值，而老玩家也极有可能将通过交易回收的成本投入另一款新游戏当中。如此循环下来，手游账号交易将极大延长一款手游的生命周期，从而促进整个手游市场的健康发展。目前玩家对于手游交易的认知度还处于最早期，主要受制于游戏账号交易过程中验证麻烦、担心交易被骗等原因。

开发者可以通过 ISP 价值协议，轻松搭建基于智能合约的账号交易应用。在当前传统二手交易模式下，验证账号需要第三方平台进行手机和密码的修改，有时

候还需要卖方在线提供手机验证码等。未来，通过 **ISP** 价值协议可以完美解决账号交易过程中的繁琐流程，同时大大降低交易过程的欺诈风险。进而促进手游二手交易市场的发展。

同时，类似的解决方案还可以应用在手游代练市场。

4. 其他领域

1. App 内测服务

在传统互联网开发中，App 研发阶段的硬件适配性测试是困扰许多开发者的重要问题之一。尤其对于中小型开发团队或个人开发者，通过自己购买不同的终端设备进行适配性测试是极大的一笔花销。

目前市场上提供的云测服务均为中心化的服务，面临许多弊端，如设备覆盖面不足，热门设备需要排队等待，产品内测版存在泄露风险等

通过 **ISP** 价值协议，开发者可以提供 App 内测相关的服务，依靠去中心化的特点，将会大大提高设备的覆盖面，并且可以避免产品内测版本的泄漏。也就是说，未来这类落地在 **ISP** 价值协议上的应用，将不需要花一分钱购置任何手机，却可以调度成千上万台手机进行内测服务。

2. 科学研究服务

随着智能设备硬件能力的日益提高，加之高渗透率的特点，使得利用移动终端设备参与科学研究成为可能。在过去，已经有许多项目进行了类似的中心化管理形式的设备 **ISP** 共享，为科学研究提供 **ISP**。如加州大学的 **BOINC** 项目，旨在通过的手机资源，参与到寻找外星文明的 [SETI@home 计划](#)，以及为其他寻找脉冲星、黑洞、引力波的科学研究提供支持。但是，由于用户激励较弱和中心化管理调度难度较大等问题，目前项目的参与设备数呈现递减趋势。

通过 **ISP**，我们将为科学研究解决用户激励问题，并提供完备的去中心化设备管

理服务。所有进行科学研究的项目，均可以简便快捷地接入 ISP，实现大规模 ISP 的支持。

3. 分布式视频转码

传统模式的视频转码，需要开发者消耗大量资源维持转码的进度，通过 ISP 价值协议，可以利用特定的编码技术，将某个视频文件分割后由 ISP 价值协议分配给多个节点进行转码和合并工作。

4. 多屏互动娱乐

多屏互动娱乐是完全基于 ISP 价值协议的全新应用场景。是涵盖了多人直播、多人同时操作、多人同步验证等综合体验。

可期待的场景包括，例如主播在直播平台进行游戏的时候，在进行游戏内开箱、抽奖、摇奖等游戏内操作时，为了增加与用户的互动性，可以直接由用户进入多屏互动娱乐场景里，直接以第三方身份进行操作参与；

又例如在教育领域，老师通过网络进行一对多教育时，可以支持多人同时在线操作，如 100 人同时参与一幅画的绘制，100 人同时参与一个课程的笔记等。

5. 视频交互直播

传统的直播对于用户而言有两个弊端：

1. 不同的 App 直接是信息孤岛，用户的等级、状态无法同步，同时主播也被垄断而依附于直播 App，造成用户为了看不同的主播需要下载不同的直播 App 并在不同的直播 App 里充值消费才能获得对应的等级。
2. 用户观看时无法获得更深层次的参与感，仅仅作为观众被动观看。

基于 ISP 价值协议，开发者可以轻松调用服务解决实际产品中的问题。例如，

开发者可以基于 ISP 价值协议提供一个直播协议，使加入协议的直播 App 彼此用户信息共享共认。同时，由于 ISP 独有的云技术服务，可以无需下载和安装就能打开任何直播 App，客观上增加了用户流量的流动。最后，依靠云技术服务，开发者可以想象出更多的互动玩法，例如可以直接通过云技术授权主播使用自己的游戏账号去玩游戏，而无需在直播内告知主播相关密码等。

4. ISP 代币

4.1. 什么是 ISP 代币

我们将为 ISP 价值协议发行原生数字代币，其符号为 ISP。

ISP 是基于去中心化的区块链数字加密资产，是基于 ISP 价值协议而发行数字代币。应用于 ISP 生态系统里的所有使用场景中。ISP 总量恒定为 21,000,000 枚。

4.2. ISP 应用场景

ISP 代币在 ISP 价值协议中将发挥如下作用：

1. 作为共享凭证

ISP 将作为共享设备方共享设备的 ISP 能力后获得的数字凭证，并通过智能合约确保 ISP 代币的分配。

2. 作为 DApp 空投凭证

ISP 基金会未来基于 ISP 价值协议开发的 DApp，将会按项目的实际情况，将其中一部分比例的 DApp 代币以糖果的方式空投给 ISP 代币的持币用户。持币用户只需按要求将 ISP 代币转入智能合约内锁仓即可。具体细则我们将根据不同项目出台规则。

3. 作为支付矿工交易费用

基于 ISP 价值协议的服务，将有矿工完成服务双方的匹配，作为回报使用者需要向矿工支付 ISP 代币。

4. 去中心化自治

随着 ISP 价值协议生态的完善和发展，整个生态的建设需要不断升级和更多持币用户参与。任何 ISP 的持币用户均可以通过锁定 ISP 代币的方式获得 ISP 生态去中心化自治系统内的投票权。投票权益 V 的大小是一个有关 ISP 锁定数量 M 和锁定时长 T 的函数： $V=f(M,T)$

在 ISP 价值协议去中心化自治系统中，任何决定都要在一个固定时间内完成投票，这个时间根据提议内容不同而发生改变。当且仅当收集到足够高权益的投票，提议才会执行，否则提议将会关闭。由此在 ISP 去中心化自治系统中，并不是权益高者的一言堂，权益低者可以联合在一起制衡权益高者。

未来所有自愿共享的智能设备，均需要账户内持有一定数量的 ISP 代币作为共享权益的证明，同时所有注册的矿工也需要持有一定数量的 ISP 代币，以此避免无效智能设备和矿工对生态的破坏和滥用。

4. 3. ISP 分配方案

比例	用途	额度	说明
10%	团队	2, 100, 000	分两部分锁仓： 5%锁仓 1 年，随后在 24 个月内解锁 5%锁仓为阶段性目标达成后锁仓。包括但不限于多项目标或单项目标达成时解锁。项目包括但不限于终端设备接入数，开发者参与数，社区影响力等。具体锁仓计划将在社区内另行公布。
10%	市场和运营	2, 100, 000	5%用于生态建设 3%用于社区运营 2%用于市场推广
75%	挖矿产出	15, 750, 000	每一年减产一次
5%	前期流通量	1, 050, 000	交易所交易

5. 开发路线图

时间	开发节点
----	------

2019 年 5 月	完成 ISP 技术可行性研究并正式启动研发
2019 年 8 月	智能设备容器化技术测试运行大型 App 游戏
2019 年 10 月	完善区块链技术方案细节 完成 ISP 价值协议白皮书撰写
2019 年 12 月	服务器控制与传输协议 音视频编解码开发 设备 App 容器开发
2020 年 1 月	零仲裁证明-增量承诺算法 共享端 App 内测版 使用端 SDK 内测版 ISP 价值协议内测版发布
2020 年 3 月	云场景协议 开发者辅助工具 ISP 价值协议正式版 1.0 发布 落地项目 1 启动
2020 年 4 月	VDI 方案 beta 版 H5 解决方案 beta 版

	ISP 价值协议正式版 2.0 发布 落地项目 2 启动
2020 年 6 月	VDI 方案稳定版 ROM 方案启动

6. 风险提示

6.1. 反洗钱规定

反洗钱规定（AML）购币者同意在购买 ISP 代币时承诺他 / 她将不会通过 ISP 代币及其衍生品（如 DApp）参与任何形式的洗钱、非法换汇和其他违法法律的行为。购币者应当了解到他 / 她将会被禁止交易、买卖、兑换和处置 ISP 代币的行为是直接或间接参与洗钱活动中。

6.2. 反资助恐怖主义（CFT）

购币者同意在购买 ISP 代币时承诺他 / 她将不会通过 ISP 代币及其衍生品（如 DApp）参与任何形式资助恐怖主义活动中。购币者应当了解到他 / 她将会被禁止交易、买卖、兑换和处置其 ISP 代币假设该处置 ISP 代币的行为是直接或间接参与到资助恐怖主义活动中。

3. 购币者限制

因为一些法律问题，本项目推介不接受任何来自下列区域的居民或公民的参与：中国大陆区域、香港、澳门、美国和其他禁止 ICO 的国家或区域。请禁止 ICO 的国家的居民或公民务必谨慎对待，ISP 基金会将不承担任何因此引起的法律责任。

4. 文档声明

本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不组成也不理解成为提供任何买卖行为，或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。

ISP 基金会明确表示相关用户明确了解参与购买 ISP 代币所存在的风险，投资人一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。