超算力

SPoC

--欢迎来到超算力世界--

目录

摘要 5

1、PoC 与 5G 产业发展趋势 7

1.1 概述 7

1.1.1 加密货币 7

1.1.2 寻求替代者 8

1.1.3 5G 时代 9

2、5G 时代的区块链视角 11

2.1 区块链发展历程 11

2.2 区块链为 5G 赋能 12

2.2.1 5G 创造的万物互联为区块链带来万亿市场机遇 12

2.2.2 区块链为 5G 应用场景提供数据保护能力 12

2.2.3 区块链促使 5G 实现真正的点对点的价值流通 12

2.3 5G 给区块链技术带来的挑战 13

3、解决方案 14

3.1 技术要求 14

3.1.1 支持海量设备并发接入 14

3.1.2 支持海量数据存储 14

3.1.3 超高性能 14

3.1.4 极具竞争力的运行总成本 15

3.1.5 支持新型软件开发流程——敏捷开发和 DevOps 15

3.2 总体架构 15

3.3 部署结构…… 16

3.4 SPoC Cloud OrePool(SPoC 云矿池）…… 16

3.4.1 原理…… 16

3.4.2 基于状态转移的区块链系统…… 21

3.4.3 虚拟机…… 21

3.4.4 智能合约安全检查…… 21

3.4.5 Map Reduce…… 21

3.4.3 程序完整性证明…… 22

4、核心技术…… 22

4.1 超级节点…… 22

4.2 边缘节点…… 23

4.3 分层共识机制…… 25

4.4 文件加密去重…… 25

4.5 分块技术…… 26

4.6 侧链技术…… 26

4.7 纠删码技术…… 26

4.8 人脸识别技术…… 27

4.9 超级算力技术…… 28

4.10 核心优势…… 28

5、5G 实现技术核心…… 29

5.1 低时延传输与交换技术…… 29

5.1.1 ROADM…… 29

5.1.2 超低时延 SPoC……30

5.2 高智能的端到端灵活调度技术……31

5.2.1 ODUflex……31

5.2.2FlexO……32

5.3 总结……32

6、应用场景……34

6.1 视频流场景……34

6.2 车联网和无人机……35

6.3 软件定义广域网和网络附加存储（SD-WAN+NAS）……35

6.4 无线 Mesh 产品……36

6.5 边缘计算……36

7、经济模型……37

7.1 价值体系……37

7.2 通证分配……37

8、发展规划（IPFS 联盟）……38

8.1 时间规划……38

8.2 未来规划……38

8.2 矿机业务……38

8.2.1 云矿机上线……38

8.2.2 云矿石上线……38

8.2.3 实体矿机……39

8.2.4 实体矿场……39

9、管理团队、投资机构和合作白名单 40

9.1 核心团队 40

9.2 顾问团队和投资机构 41

9.3 合作白名单 41

IPFS 41

BHD 41

IPFS&Filenet（FN） 42

YottaChain 42

Galaxy Network 42

10、免责申明和风险提示 43

摘要

早在 2014 年，随着 Burst 的上线和 POC（Prove of Capacity）共识机制的提出，POC 便进入了公众的视野，后因影响力相对较小，也就没能成为链圈的大趋势。近期，随着 SPoC、BHD 等项目的上线，“POC”成为了新的链圈热词。

POC 共识机制开创了硬盘挖矿模式的先河，利用的是计算机的硬盘空间大小而不是电脑的计算能力。硬盘的容量越大，可储存在硬盘里的方案值就越多，矿工就越有机会匹配到其中所需要的哈希值。简单点来说，就是通过某种既定的算法产生数量众多的伪随机数，并将这些随机数存入硬盘，在竞争打包区块的时候，只需要通过读盘（根据现有的散列函数预先计算出结果），就可以随机加以匹配来打包区块，从而获得相对应的奖励。

与此同时作为引领数字经济创新的重要推动力，5G 技术正以其高吞吐、低延迟、高并发、低功耗等优质特性，与人工智能（AI）、区块链（Blockchain）、云服务（Cloud）、大数据（BigData）一起，构建新时代的全球 IT 基础设施。5G 所延伸出的万物互联将有利于提升整个社会效率，促进物联网、人工智能、边缘计算、AR、VR、超高清视频流等应用的大规模兴起和繁荣。

但是，伴随着设备的大规模接入、数据的海量增长及计算需求的剧增，以下问题也接踵而至，引起人们的广泛关注：

- 数据缺乏安全保障，容易被黑客窃听
- 海量数据采集、GDPR 法例生效突显隐私保护责
- 在 5G 网络上开发各种物联网应用的成本高昂
- 除了通信以外，终端之间难以实现价值的交易和互换。

SPoC（Super Proof of Concept ）全称为：面向 5G 时代的分布式存储和私有云储存打造的存储与游戏产

业的共有区块链系统；其核心技术是基于以太坊智能合约技术、POC 容量证明共识，利用区块链技术，构建了 5G 架构下终端上链的网络安全和信任机制。

- 实现高吞吐、低延迟、高并发、低功耗的价值生态网络体系
- 能够支撑未来数字时代大数据上链的多源信息互联交换，以及多元化的资产登记、交换、交互及流动
- 实现万物互联、构建链上数据世界，促成信息获利的新经济体

SPoC 作为公链，可以更加安全、高效、稳定，也极其方便的为 DApp 开发者在发布相关应用、部署相关数据、存储相关内容等工作中

提供一条快速通道，并且打造出一个在各个游戏中通用的 token 结算系统以及存储服务平台。以此连接各层级之间的用户关系，形成一个新型的区块链中层生态社区，并支持任何人在其主网上发布自己的 token 资产与应用。另外，其独特的挖矿模式也让开发者与用户和矿工之间形成一个新型的区块链生态社区。

作为面向 5G 数字经济时代的基础公链，SPoC 旨在利用区块链技术实现复杂的应用场景业务上链，为 5G 数字时代的产业发展助力。在主网上线之后，SPoC 将广泛应用于 5G 环境的云 VR/AR、智慧安防、**车联网、智慧城市、智能制造、**无人机、SDWAN+NAS、Mesh 产品、边缘计算模块等应用领域。PoC 挖矿 5G 时代的到来，必将是一个大爆.

1、PoC 与 5G 产业发展趋势

1.1 概述

1.1.1 加密货币

提到加密货币，Bitcoin(比特币，以下简称（BTC）是最广为人知的，在其之外，整个加密货币产业已经开始尝试一些新的技术方案来提高支付速度，扩大支付范围，很多改进型加密货币应运而生，比如 Dai-Wei 的 B-Money 和 Ripple。Ripple，我们已经看到，其已被少部分不同国家银行之间用于结算，由于其在生产方式上过于中心化，并未得到大面积的应用。相较于更去中心化的加密货币(如 BTC)，项目中心化的运作更易受到其他应用型公司的青睐。在这个体系内自然也不会有加密货币矿工的出现，毕竟大多数的步骤和矿工无关，因其发行方主要以公司性质的身份参与整体项目。

B-Money 由于其设计中需要大量的网络同步操作，使得其很容易产生网络阻塞，而当时的网络速度并没有那么快，信息在传输的的途中经常卡顿而出现问题，或者全体网络都在等待一个比较慢的包，最终因得不到回复信息而导致传输失败，使其在使用上不尽人意。BTC 通过自己 nakamoto 型共识，也就是现在大家熟知的异步 proof of work(以下简称 POW)，走到了舞台前。在初期，看好这个项目的人并不多，源于其共识并没有通过同步转账结果来保证转账的结果不会出错，而是使用很有趣的方式——最长链。也就是说，这个分布式系统中节点更认可哪个包，那个包中的交易就是正确的结果，那么怎么出现这个包呢，当然是通过这个系统中的节点来共同验证，只给定一个超时打包的时间，这个包在这段时间中只要有更多的节

点参与认可，那么它就是对的。在这个逻辑中，会存在一种情况，那就是系统中的节点可以集体做坏事，让正确的交易没有被打包，这样网络的传输就是无效的，这也是这个方式中有趣的地方，因为它既对又不对。对，是因为它避免了网络中很大量的通讯，异步更加适合交

易的步骤；不对，是因为在极端情况下，即系统中坏人占多数时，系统就变成无效系统，这也是在后期大家经常提到的 51%双花攻击。金融系统最不能做的就是回滚和双花，这也是一开始 BTC 没有被大规模接受的原因。

随着时间的推移，拥有了很多由于利益而进入到系统的参与者，系统层面由于出块（也就是上文提到的打包）难度的存在，将坏人进入的成本大大提高，系统也随之变得更加稳定，毕竟做好人比做坏人得到的收益要高多了。这时候人们开始认可这个新型的加密货币，其从一个不稳定的金融系统，通过多年的难度增加，让双花和回滚变得非常困难，系统逐渐趋于稳定。也因此产生了 BTC 的原教义者：加密货币爱好者。这时就有很多新型的加密货币以分叉的方式被制造出来，又因为其算力的独占的问题被 51%双花攻击，其主要原因就是在低难度下，这个系统是一个不安全的；而高难度安全系统则需要非常大能源的消耗。

我们可以通过观察发现 BTC 的一些技术特征：

BTC 从来都不是技术激进派，反而是挑选了相当成熟的现有技术去完成安全可信的点对点现金系统，越是被验证过、越是简洁、成熟的技术，越是安全、可信。例如 nakamoto 共识中用到的 SHA256 这个算法，是由 NSA（美国安全局）设计，其安全可信性是被有效验证过的，说明初期设计之时可能根本没有考虑到现在的 ASIC（Application-Specific integrated Circuit，专用集成电路，以下简称 ASIC）和电力垄断问题，只是为了极致的可信而设计，为了极致的安全可信，甚至牺牲了互联网原有的高效交易并发量。

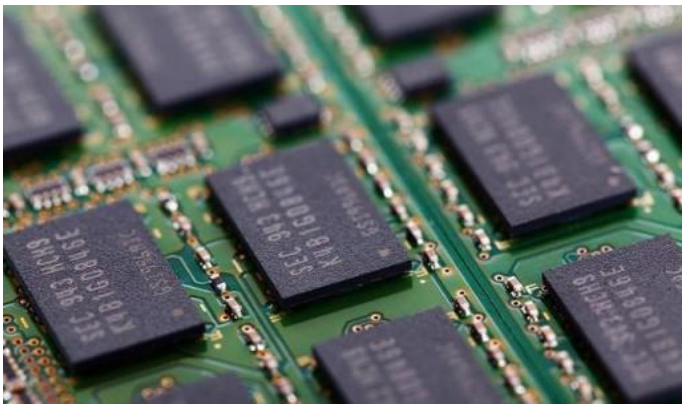
1.1.2 寻求替代者

在资源被大量用来出块，成本逐渐提高的时候，加密货币爱好者开始致力于寻找更低功耗的替代者，主要分为两类：更低成本获得收益的替代者和更通用可堆叠组件的替代者，这就是 ASIC 挖矿以及抗 ASIC 算法开发的大航海时代。其中 ETH，

Mon

ero 的初衷都是以抗 ASIC 为目的，他们希望出块的计算方式能够抵抗 ASIC 芯片，并且维持比较低的出块成本，让它变成一个不受控于 ASIC 芯片进行挖矿的加密货币，不过在加密货币发行之后，市值一旦达到 ASIC

芯片投入的范畴，ASIC 的开发商依然会想办法将这些通过计算方式去挖矿的加密算法设计成为矿机。另外一个著名的加密货币 LTC 也是其中的代表，使用



Scrypt 算法的 LTC，以对抗 ASIC 为技术亮点，不过很快 ASIC 设备生产商就优化了他的算法，将其做成了矿机，形成了设备以及算力的垄断，带来了巨大的能源消耗。电力的依赖和矿场的门槛让挖矿成为少数人的游戏。

而 SPoC 则是一个集大成者，其既能达到更低的能源消耗，又能方便矿工自制通用组件参与其中，同时维持相对高的难度来保证系统的稳定性。SPoC 使用的 CPOC 共识，是非常去中心化的一个共识算法，相对于 POW 引起的算力证明大航海时代，CPOC 将会开拓一个基于硬盘容量证明的新大航海时代。CPOC 使用硬盘作为共识的主要载体，让更多的普通人可以通过自己的电脑参与到算力的组建中去，能够回归到中本聪设计 POW 的部分初衷，让每个人都能参与到去中心化的革新之路。

SPoC 与此同时继承了 BTC 的传统，因为 BTC 在设计之初便是一个服务于多数参与者的系统，即每一个参与的者都可以是一个思考、支持、甚至是颠覆系统的角色。CPOC 继承了这种开放性、包容性，伴随着更加亲民的硬盘容量共识，可进一步将加密货币推向大众视野，让更多的人参与到 SPoC 经济系统的建设。

1.1.3 5G 时代

5G 即第五代移动通信系统（5thGenerationMobileNetwork），是新一代的无线通信网络标准。相比 4G，5G 在移动宽带、时延可靠和海量连接等方面都产生了质的飞跃，具体表现为：

- 能以 10Gbps 的数据传输速率支持数万用户
- 能以 1Gbps 的数据传输速率同时提供给在同一楼办公的许多人员
- 能支持数十万的并发连接以用于支持大规模传感器网络的部署
- 频谱效率相比 4G 显著增强
- 覆盖率比 4G 有所提高
- 信令效率得到加强
- 延迟显著低于 LTE1.2 关键技术和应用场

景根据 IMT-2020 发表的《5G 概念白皮书》，5G 的创新技术包括大规模天线阵列、超密集组网、新型多址、全频谱接入和新型网络架构。

其中大规模天线阵列、超密集组网、新型多址和全频谱接入等技术是业界关注的无线领域创新焦点；基于软件定义网络（SDN）和网络功能虚拟化（NFV）的新型网络架构是网络架构领域的未来标准。

此外，基于滤波的正交频分复用（F-OFDM）、滤波器组多载波（FBMC）、全双工、灵活双工、终端直通（D2D）、多元低密度奇偶检验码、网络编码、极化码等也是 5G 重要的潜在无线关键技术。

5G 通过融合上述关键技术，能应对多样化场景的极端差异化性能需求，其适用的应用场景包括连续广域覆盖、热点高容量、低时延高可靠和低功耗大连接等四个 5G 典型适用场景，包括云 VR/AR、智慧安防、车联网、智能城市、智能制造、无人机、SDWAN+NAS、Mesh 产品、边缘计算模块等应用领域。

◆ 商业前景

作为未来创新技术的标准，全球各国给予高度重视，制定了明确的 5G 商用时间表。这当于所有美国消费者在 2016 年的全部支出，并超过了 2016 年中国、日本、德国、英国和法国的消费支出总和。

到 2035 年，全球 5G 价值链将创造 3.5 万亿美元产出，同时创造 2200 万个工作岗位。上述数字超过了今天整个移动价值链的价值。5G 价值链平均每年将投入 2000 亿美元，持续拓展并增强网络和商业应用基础设施中的 5G 技术基础。

此外，5G 部署将支持全球实际 GDP 的长期可持续增长。在 2020 年至 2035 年间，5G 对全球实际 GDP 增长的贡献预计将相当于一个与印度同等规模的经济体。

简而言之，5G 将会通过以极高的速度实现各种设备之间的实时通信，成为 AI、大数据、云服务等新一代创新技术的推动者，最大限度地发挥这些创新的影响。数字领域的数据爆炸可以帮助大规模转变业务，并为用户提供丰富、有意义和身临其境的体验。随着 5G 数据经济的充分发展，人们的工作和生活方式将发生根本性的变

化，全球经济也将迈向新的数字时代。

2、5G 时代的区块链视角

2.1 区块链发展历程

区块链是分布式数据存储、点对点传输、共识机制、加密算法等新型计算机技术，具有去中心化、全网记录、低成本、高效率、安全可靠等技术特点。

从 2009 年 1 月 3 日中本聪挖出创始区块开始，比特币不间断运行至今，用长达 10 年的不间断安全运行成果，比特币证明了其背后区块链技术的可行性。2014 年 1 月 23 日，年仅 19 岁的以太坊创始人 VitalikButerin 发布了以太坊白皮书。2015 年，经济学人报一篇《区块链：信任机器》的报道，将区块链技术引入了全球风口。2017 到 2018 年迎来了区块链概念大爆发，越来越多的公司、创业者开始涉足区块链，区块链项目呈井喷式增长。

大型企业也开始纷纷涉足区块链领域。2018 年 8 月 10 日，中国深圳开出第一张区块链电子发票，由腾讯 FiT 区块链团队提供底层技术。2018 年 10 月 10 日，IBM 宣布 IBMFoodTrust 正式商用。2019 年 2 月，摩根银行宣布将发行银行系统稳定币 JPM，一个 JPM 锚定一美金。2019 年 3 月，彭博社报道拥有 20 亿用户的 Facebook 正在战略转移区块链，研究利用 WhatsApp 推出一款稳定币，瞄准汇款市场。

区块链技术潮流不可逆转，并正在以其自身的运行规律不断地完善和优化，分片技术、侧链、跨链、共识算法、抗量子等领域技术也在不断突破中。从区块链产业看，随着行业龙头的出现，市场向精细化划分，再加上法律法规的逐步健全，未来三年内，区块链产业格局将基本形成，区块链对社会经济各领域的推动作用快速显现，区块链在全球范围内对人类的生活产生广泛而深刻的影响。

2.2 区块链为 5G 赋能

5G 是未来网络的基础设施架构，区块链是业务开展的新框架，区块链如何与 5G 技术紧密融合，是区块链设计者们目前重点研究的课题。

2.2.1 5G 创造的万物互联为区块链带来万亿市场机遇

当前全球上万亿的商品中，有 99.99%的商品都没有接入区块链网络，其中一个原因是受制于终端的不成熟，众多依赖于物联网终端的区块链产业应用无法商业化，其中包括云 VR/AR、智慧安防、车联网、智能城市、智能制造、无人机、软件定义广域网+网络附加存储（SDWAN+NAS）、无线 Mesh 产品、边缘计算模块等。

而 5G 技术能够给物联网带来更广的覆盖、更稳定的授权频段、更统一的标准，从而对基于物联网的区块链应用提供有力的支持。因此，依托高速的 5G 通信技术，以及物联网、大数据和人工智能等各项技术的发展，区块链将能为全球上万亿的商品，提供稳定的跟踪、溯源能力和分布式的点对点交易功能。

2.2.2 区块链为 5G 应用场景提供数据保护能力

5G 时代对数据的保护能力提出了更高的要求。5G 出现后网络速度将大幅度提升，数据量也将随之急速增长，此外，更多计算和存储将由智能终端和边缘计算节点来承担。

区块链技术旨在打破当前依赖中心机构信任背书的交易模式，用密码学的手段为交易去中心化、交易信息隐私保护、历史记录防篡改、可追溯等提供技术支持，天然适用于对数据保护要求严格的场景。

2.2.3 区块链促使 5G 实现真正的点对点的价值流通

5G 重点布局分布式的场景，比如车联网、远程视频、智慧城市等。区块链可以做到在分布式部署的架构下，

无需中心机构做确权，而由去中心化的节点在链上来确权和分发。这就促使点对点的价值交换成为可能，而不需要通过中心化的中转、提成，大大提升了终端交易的效率，降低交易成本。比如 5G 带宽租赁服务、新能源电表交易等等商业模式，很适合通过区块链来完成点对点的交易，实现价值交换。

2.3 5G 给区块链技术带来的挑战

5G 依托光纤网络，比现在的 4G 快 10 倍，并提供更低的延迟和更大的带宽，面向 5

G 的应用场景通常具有高性能、低延时的并发存储、协同网络、并发计算的技术需求。要管理这样复杂的“生态系统”，需要更高的计算能力和存储容量。

而区块链不可能三角的问题成为制约其技术发展的关键瓶颈。当前区块链的共识技术、交易处理能力、数据吞吐能力还无法应对复杂的应用场景需求。此外，随着区块链平台的不断丰富，更多的终端接入区块链世界，必然出现多种区块链平台共存的情况，5G 时代的跨链需求更加迫切。

3、解决方案

SPoC 是全球首个专注于 5G 应用场景的公链项目。针对以上挑战，SPoC 提出了下列技术要求，并设计了完善的“区块链+5G”解决方案。技术创新上的创新解决了四大痛点问题：

- 1.人人可参与。PoW 挖矿容易形成矿霸，打破公平性，PoC 挖矿机制与 5g 技术的完美融入，更多设备矿机的加入，同时因其随机性，人人都可参与。真正做到在兼顾效率的同时，又保护公平
- 2.资金零风险。应对盗币风险，采用先进的人脸识别技术，扫脸转账，分布式存储支付信息，保障资金安全，真正实现钱包零盗币，资金零风险
- 3.生态有保障。很多项目，往往有一个美好的愿景，然而没有技术与生态保障，最终整个生态也成为“空气”生态，虚假生态。SPoC 项目，技术有保障，生态健全，覆盖通证经济，软硬结合，拥有真正的生态保障。
- 4.社群可持续。做为优质的项目，社群基础是重要的衡量因素，SPoC 具备优质社群并与各大知名项目方保持良好关系，与此同时，各节点的持续深入，促进了社群发展，真正做到社群可持续！

3.1 技术要求

3.1.1 支持海量设备并发接入

为了支撑终端设备产生的海量数据上链需求及复杂应用的边缘计算需求，SPoC 需能够处理海量用户设备所产生的并发数据。

3.1.2 支持海量数据存储

5G 网络对传输带宽的大幅提升，使得大数据应用、超高清视频应用向区块链存储数据成为可能，SPoC 需具备高存储能力，以便承载复杂的 5G 数据存取需求。

3.1.3 超高性能

为实现 5G 时代链上存储和链上计算的目标，SPoC 需要提供超高的性能，包括网络访问、数据存储、顺序计算、并行计算等各方面的超高性能指标。

3.1.4 极具竞争力的运行总成本

伴随云计算、云存储以及区块链等技术发展，以 AWS、阿里云、Azure 为代表的传统云计算公司，和以 EOS 为代表的第三代区块链应用公链，正在不断降低开发者和企业的使用和运营成本。SPoC 需要从技术架构、经济模型层面设计一套自适应的运营体系，允许用户免费访问网络，开发者免费发布应用，并为开发者和企业创建有效的盈利模式。

3.1.5 支持新型软件开发流程——敏捷开发和 DevOps

随着 5G 应用需求的不断多样化，以及区块链基础设施的不断更新换代，完全不依赖于中心服务器的复杂场景应用将成为主流。因此，基于智能合约开发的 DAPP 应用应能满足用户需求快速迭代，满足开发者使用现代化软件开发流程和运维流程的需求，比如互联网流行软件开发流程——敏捷开发和 DevOps。

3.2 总体架构

SPoC 突破性地提出了基于区块链的自动设备认证技术，在基于会话和特征识别的基础上，通过智能合约和挑战应答（challenge-response）的通讯方式实现自动设备绑定请求、设备认证，并支持用户级别的身份绑定，结合人脸识别技术，通过扫码进行 ETH 的转账，使得终端设备信息无法被篡改，为万物互联和边缘计算应用提供最基础的终端设备认证。

为支持 5G 环境高并发和网络存储需求，SPoC 选用了 IPFS 为其存储基础架构。IPFS 的网络提供了动态的、细粒度的、分布式的网络存储支撑，可以更好地适应 5G 内容分发网络（CDN）的要求。SPoC 大文件会被切分成小的加密分块，下载的时候可以从多个服务器同时获取。在对象层和文件层，大部分数据对象都是以 MerkleDAG 的结构存在，并具备双重哈希去重，能够灵活支持内容寻址和去重存储。

在此基础上，SPoC 网络提供了一系列应用框架，包括分布式数据交换协议、分布式流程管理协议等等，使用通用 API、SDK 以及各种应用功能组件，能够实现开发部署的便捷化，支持互联网产品敏捷开发。

SPoC 这种高度封装化的分布式账本架构、快速地支持大量并发进程的存储结构，使得 SPoC 具备了应对 5G 复杂应用场景需求的能力。

3.3 部署结构

SPoC 的总体部署架构如下图所示：5G 网络构成基础设施，超级节点负责执行智能合约和出块，边缘节点则负责涉及智能终端的分布式计算和存储平台，提供海量计算和存储能力。分布式账本负责链上及链下核心处理。

3.4 SPoC Cloud OrePool(SPoC 云矿池)

3.4.1 原理

POC 共识算法最早被 StefanDziembowski 在 2013 年被提出，Burst-coin 则是第一个以 POC 共识算法为基础的区块链项目，同时，Burst-coin 在 2018 年完成了 POC2 的共识升级，使得 POC 网络更加安全。

3.4.1.1 术语

在基于 POC 的区块链系统中，有些术语和基于 POW 挖矿的系统类似，但是不太一样，为了方便理解，我们将一些主要的需要强调的术语列在下面。

Shabal/Sha256/Curve25519

Shabal,Sha256,Curve25519 是 SPoCkNetwork 中使用的加密哈希函数，Shabal 是主要使用的函数，Shabal 是一个并不是一个高效的加密哈希函数，但是由于我们的哈希计算主要发生在 plot 阶段，对于我们运行时所需要的验证工作来说它已经足够了。我们主要使用它的 256 字节的版本，也就是 Shabal256。

哈希值

哈希值表示一次加密哈希函数的计算结果，如果没有特别说明，本文中提到的哈希值一般为 32 个字节。

Plot 文件

当挖矿时，挖矿程序会从磁盘中读取事先计算好的 Hash 值，这些值被存储在磁盘的文件中，这些文件就是 Plot 文件。

Nonce

一个 plot 文件中，存了若干组 nonce，一个 nonce 包含 8192 个哈希值，因此一个 nonce 的大小为 256K 字节，每个 nonce 都有一个独立的长度为 8 字节的的编号，编号范围为 0-18446744073709551615(2^64)。

Scoop

每个 nonce 所包含的 8192 个哈希值被放入 4096 个不同的地方，每个 scoop 中放入 2 个哈希值。

Account ID

当创建 plot 文件时，这个文件是和矿工的数字账号 Account ID 关联起来的，这个 ID 会被用于创建 nonce，不同的矿工创建的 nonce 不一样，尽管可能他们使用的 nonce 编号是一样的。

Deadline

Deadline 是挖矿过程中不同矿工之间用于互相竞争的值，这个值是基于 plot 文件上的 nonce 计算出来的，当这个值被提交到钱包时，并且钱包没有在 deadline 时间(秒)内收到网络中来自其他节点的区块广播，则会进行打包。

Block Reward

当某个矿工负责打包区块时，他就能获得区块奖励。区块奖励详细信息见第 3 章。

Base target

Base target 是根据过去 24 个块的出块情况计算出来的。这个值用于调整挖矿的难度，这个值越小，则对于矿工想找一个小的 timeline 越难。

Network Difficulty

这个值相当于用于体现当前网络中用于挖矿的总的硬盘空间，以 T 为单位。

Block Generator

当新的区块被打包时，打包时需要用到的账号就是 block generator。也就是找到 deadline 所需要用到的 nonce 所对应的账号。

Generation Signature

Generation signature 是基于上一个区块的 generation signature 和 block generator，这个值被用于打包一个区块，长度为 32 字节。

Block Signature

Block signature 是被 block generator 在打包区块时创建的，是将 block 内大部分数据以及 block generator 的私钥进行 Sha256 和 Curve25519 哈希计算后的签名，长度为 64 字节。

Solo/Pool 挖矿

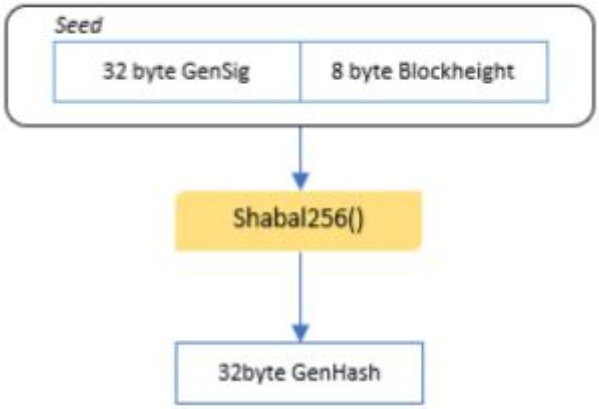
独立挖矿和矿池挖矿，独立挖矿也就是矿工提交的结果是跟整个网络内其他独立矿工和矿池提交的结果进行直接竞争，获胜时则可获得全部区块奖励。矿池挖矿则是将结果提交给矿池，由矿池在收获了矿池内其他矿工的以确定拿到的最小的 deadline 值之后，和网络内其他独立矿工和矿池提交的结果进行比较，若胜出，则矿池会根据自己的分配机制，公平的分给相关参与挖矿的矿工。

奖励分配

奖励分配主要针对矿池挖矿说的，当矿工设置了奖励分配归属为矿池之后，矿工相当于通知了网络矿池接管了矿工的区块奖励，也就是说当本来区块奖励时分配给矿工的，现在分配给矿池的账号，同时，若从矿工处接收到的 deadline 值，则由矿池负责打包出块。

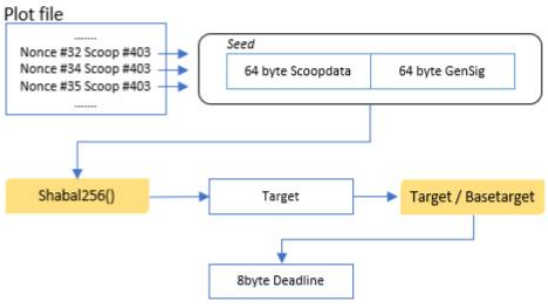
3.4.1.2 挖矿过程

当开始挖矿时，挖矿程序会从钱包这里获取挖矿信息，如 generation signature, base target 和下一个区块高度，其中，generation signature 是由钱包程序在上一个 generation signature 和上一个出块的矿工 Id 组合在一起后通过 Shabal256 计算后生成。挖矿程序将 generation signature 和区块高度组合在一起作为 Shabal256 的 seed，以得到一个 generation hash。



接下来挖矿程序会将 generation hash 值对数值 4096 取模来计算该使用哪个 scoop 中的数据。

然后挖矿程序会读取所有 nonce 所对应的该 scoop 的数据，将 scoop data 和 generation signature 作为 seed 得到一个新的 target 值，再将 target 值除以 base target 并取前 8 个字节作为 deadline 值。



挖矿程序会所有计算得出的 deadline 值中选取一个最小的值，如果该值还有值得提交的意义(如果数值过大，则没有必要提交结果，因为提交了也不会被采纳)，提交的信息中包含和该 plot 文件关联的矿工 ID，以及通过当前的 scoop data 所找到的最优 deadline 所对应的 nonce 值。

3.4.1.3 打包过程

钱包程序(或者矿池程序)在接收并验证了挖矿程序提交的信息之后，会观测在 deadline 数量的时间(秒)内，是否收到网络上别的矿工广播的有效区块，如果收到，则钱包放弃打包区块，否则钱包将使用目前的 deadline 信息打包区块。

每个区块可以最多包含 255 个交易信息以及最多 44880 字节的 payload 数据。钱包程序会尽可能的将

未确认的交易信息放入正在打包的区块中，针对每一笔需要打包的交易，钱包程序会对签名、timestamp 等信息进行校验，校验通过才会放进区块中。区块信息只包含打包的交易的 Transaction ID，每个交易的详细信息如交易数量，手续费等信息是独立存储的。

3.4.1.4Nonce 生成

前面我们已经提到，和 POW 的 nonce 是通过执行随机预言函数计算得出不同，POC 则是将 nonce 值进行处理后存储在硬盘中，每个 nonce 的大小是 256K 字节，并且 8192 个哈希值组成。

创建 nonce 的第一步是创建 seed，第一个 seed 是一个 16 字节长的值，有矿工 ID 和 nonce 编号组成，我们通过 Shabal256 获得第一个哈希值，我们将这个值放在第一个 seed 前，形成第二个 seed，同时再通过 Shabal256 函数获得第二个哈希值，再将这个值放到上一个 seed 前，形成第三个 seed，以此类推来产生 8192 个哈希值（当拼接的 seed 超过 4096 个字节时，会选择前 4096 个字节作为 seed），最后我们将所有 8192 个哈希值并且初始的 16 个字节拼接，作为最终的 seed，通过 Shabal256 得到一个最终的哈希值。以上过程的伪代码如下：

- seed=account_id+nonce_id//8bytes+8bytes2.for(i=0;i<4096;++i){3.hash=Shabal256(first4096bytesofseed)4.seed=hash+seed;5.}6.7.final_hash=Shabal256(seed);

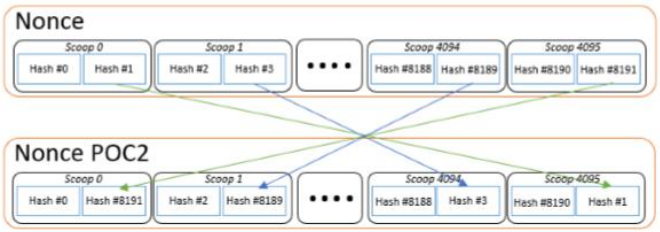
```
1.  seed= account_id+ nonce_id //8 bytes + 8 bytes
2.  for(i = 0; i < 4096; ++i){
3.      hash = Shabal256(first 4096 bytes of seed)
4.      seed = hash + seed;
5.  }
6.
7.  final_hash = Shabal256(seed);
```

这个哈希值会和以上 8192 个哈希值进行一一异或计算以得到一组总共 8192 个新的哈希值，这组哈希值就是我们写入磁盘的 plot 文件的内容。

3.4.1SPoC

nonce 生成是基于 POC1.0 的，但是它存在一个公平性问题：由于一个产生的哈希值是顺序的方式依次存入 scoop 中，对于某些”作弊”的矿工，它可以不预先生成 8192 个哈希值，而是只生成 1 个哈希值，剩下的 8191 个哈希值可以在需要进行 deadline 计算时再算出来，

如此，原本矿工需要 256K 字节空间的数据，只需要 32 个字节就可以了。这个问题并不是一个严重的安全漏洞，因为这些”作弊”的矿工只是利用数据结构的特点节省了空间，并没能改变打包区块、验证区块的规则。基于此，POC2.0 被提出来解决这样一个问题，主要就是将原本依次顺序存储在 scoop 中的哈希值进行了调整，调整规则如下：



在 SPoC 中，我们将采用 POC2 来作为共识算法，POC1 的数据格式不会被兼容。

3.4.2 基于状态转移的区块链系统

和以太坊一样，SPoC 是一个状态转换系统，通过建立终极抽象的基础层和内置的图灵完备编程语言的系统使得任何人都可以创建智能合约和去中心化应用。账户在 SPoC 中，状态是由账户的对象和两个账户之间转移价值和信息状态转换构成。账户包含以下几个部分的：随机数，用于确定每笔交易只能被处理一次的计数器账户目前的代币账户的合约代码，如果有的话账户的存储账户的标识标号

3.4.3 虚拟机

虚拟机环境(SVM)是任何一个支持脚本语言的区块链项目都需要的功能，同时为了更好更快速的发展开发者生态，SVM 将支持 Solidity 语言，使得现有的 Solidity 开发者几乎不需要二次开发就可以引入到 SPoCk Network 中。

3.4.4 智能合约安全检查

以太坊上的智能合约经常会爆出层出不穷的安全漏洞等方面的问题，通过系统进行智能合约的部署的时候会通过智能检测平台检测智能合约漏洞，让对应的智能合约能够将一些潜在的安全隐患扼杀在摇篮之中。

3.4.5 Map Reduce

云矿池是典型的分布式计算。我们以 MapReduce 为基

础，结合 SPoC 云存储架构 SPoC 云矿池。MapReduce 是面向大数据并行处理的计算模型、框架和平台，它隐含了以下三层含义：

1）MapReduce 是一个基于集群的高性能并行计算平台（ClusterInfrastructure）。它允许用市场上普通的商用服务器构成一个包含数十、数百至数千个节点的分布和并行计算集群。

2）MapReduce 是一个并行计算与运行软件框架（SoftwareFramework）。它提供了一个庞大但设计精良的并行计算软件框架，能自动完成计算任务的并行化处理，自动划分计算数据和计算任务，在集群节点上自动分配和执行任务以及收集计算结果，将数据分布存储、数据通信、容错处理等并行计算涉及到的很多系统底层的复杂细节交由系统负责处理，大大减少了软件开发人员的负担。

3）Map Reduce 是一个并行程序设计模型与方法（Programming Model & Methodology）。

它借助于函数式程序设计语言 Lisp 的设计思想，提供了一种简便的并行程序设计方法，用 Map 和 Reduce 两个函数编程实现基本的并行计算任务，提供了抽象的操作和并行编程接口，以简单方便地完成大规模数据的编程和计算处理。基于 Map Reduce，我们将挖矿所涉及到的工作量证明函数进行并行化处理，分解到 SPoC Cloud 中运行。借助网络中庞大的算力，SPoC 云矿池相较其他矿池均具有强大的竞争力。

3.4.3 程序完整性证明

由于 SPoC 云矿池以算力比例分配挖矿收益，为了避免参与者算力造假，我们对植入到终端设备中的挖矿程序进行定期的完整性证明。完整性证明算法与 SPoC 云存储采用类似算法。通过完整性证明避免参与者篡改挖矿程序，对挖矿算力进行造假。

4、核心技术

4.1 超级节点

SPoC 对超级节点机制进行了优化，使其可以更好地管

理核心网络和系统功能的任务，包括在侧链上运行多种服务，支持 5G 模块组扩展，跟踪并测量设备的正常运行时间，并为矿工安排节点报酬支付时间表。

与 EOS 超级节点不同的是，SPoC 超级节点除了执行智能合约和出块，还为整个网络的海量数据提供存储服务，作为类 IPFS 分布式存储网络的主节点，确保整个 SPoC 网络提供高效、可靠、可信的区块链网络服务。此外，SPoC 超级节点还具有设备模块，能够接入智能终端设备，适应视频、网络等多种终端接入模式。在共识机制上，超级节点采用 PBFT-DPoS 共识机制，负责区块产生和存储关键数据。智能合约和运算量小的计算工作在超级节点上执行。

4.2 边缘节点

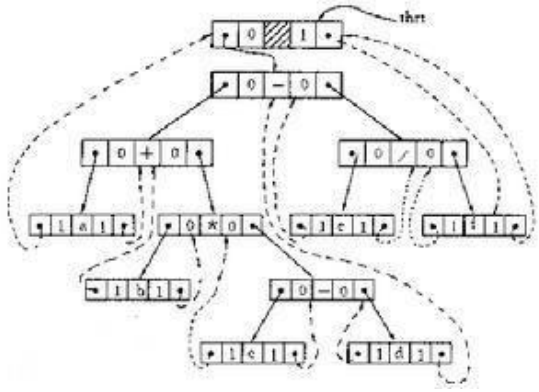
海量计算需求会给超级节点带来严重的负载。经过对超级节点模式的压力测试，团队认为超级节点不适合处理万物互联环境下复杂的长时间计算任务，因此需要边缘计算节点接入来执行计算密集型任务。另一方面，在一些高响应要求的物联网应用中，云端响应的延时会造成整体效率的低下。

SPoC 引入了边缘节点（EdgeNode）的概念，边缘节点机制作为超级节点的必要补充，可以将密集计算业务下沉至边缘节点，这有助于降低响应时延和带宽成本，满足去中心化架构模型下各类智能场景的需要。

边缘节点作为 SPoC 网络海量计算和海量存储资源的来源，可以是未来所有的具备一定计算或存储能力的终端设备，通过让超级节点为边缘节点担保，确保边缘节点为大数据存储和超高速智能合约边缘计算处理提供高效、可靠、可信的区块链网络服务。

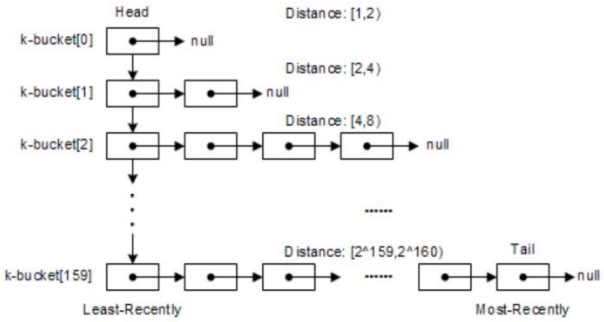
通过将海量的边缘节点的闲置计算能力和存储能力组成一个分布式计算和存储平台，执行耗时较长的计算任务，包括 AI 应用，图片处理，基因测序等使用边缘节点的场景，把密集计算任务从云端卸载到边缘之后，整个系统对能源的消耗减少了 40%以上，数据在整合、迁移等方面可以减少 90%以上时间。边缘节点数据存储采用如下算法：

SPoC 采用 kademlia 算法改进版实现数据存储与检索。在 SPoC 中节点 Nid 长度取值 512；节点冗余参数 k 取

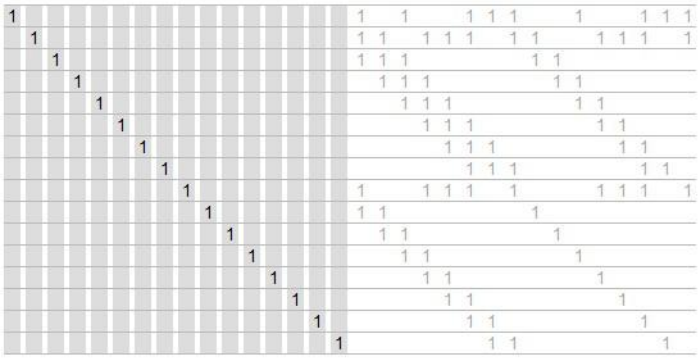


值 32；

kademlia 二叉树



每个节点内部 k-bucket 存储示意图



Reed-solomon 数据还原示意图

SPoC

1)边缘节点 E1 加入 SPoC 后,向 SPoC 超级节点请求节点 id，临近超级节点 H1 从 id 池中选取未使用 id1 节点分配给该边缘节点(节点 id 一旦分配其整个生命周期内维持变)；

2) 边缘节点 E1 收到 id1 后计算 Nid1=sha3-512(id1)（即本节点标识)。

3）E1 收到终端设备发来数据 Data1 存储要求时,根据 Data1 大小将其切分，假设节点长度为 L,切分后长度结果表示为 L=∑ni·bi（其中 bi 依次取 256M，256K；n0 为 256M 分块数,n1 为 256K 分块数)；相应的数据切分为 Bj，即 Data1=∑Bj；

4）根据用户支付 SPoC 通证情况，选择矩阵 M，根据 M 生成冗余数据：

a.用户选择普通安全模式，系统按 10%比例生成冗余数据：mi= ┌ni*10%┐，(i=0,1)

b.用户选择中等安全模式，系统按 20%比例生成冗余数据：mi= ┌ni*20%┐，(i=0,1)

c.用户选择强安全模式，系统按 30%比例生成冗余数据：mi= ┌ni*30%┐，(i=0,1)

d.新生成的整体数据记为：Data1=∑Bj(i≤n0+n1 时 Bj=Bj,i › n0+n1 时 Bj 为冗余数据)

5）针对每个 j,计算 Nid'=h=sha3-512(B')，根据 h 在边缘节点查询相关数据表项是否已存在，若已存在则扣除相关 SPoC 通证后继续下一 j 处理；否则转入 a.处理；

a.计算待存储节点 E1,i 与本节点 E1 距离 d=Nid1⊕Nid'，根据 kademlia 二叉树路由表查找其位置；

b.通过 ping 命令探寻 E1,i0 是否存活：c.如果存活向 E1,i0 发送 storeBj 指令；下一 j 处理；d.如果节点 E1,i0 非存活（将该非保活节点则上报超级节点扣除相关 SPoC 奖励），则在相应 K-kucket 集合{E1,i1E1,i2,...E1,ik}（这里 it 表示待存储节点与本边缘节点距离,2i≤it<2i+1,t=1,2,...,k,k 最大选取 32，超过该值还未找到则将本次数据丢弃)中选取第一个存活节点进行存储；

4.3 分层共识机制

共识机制是所有公链的技术核心。共识机制存在一个 CAP 原则，即一致性、可用性和分区容错性难以同时得到保障。同时，还需要确保所有诚实节点都保持一致性，避免分叉。对于 SPoC 而言，由于存在边缘节点，使得共识算法更加复杂。为此，SPoC 采用分层共识机制：

·超级节点通过投票机制产生，使用 PBFT-DPoS 机制轮流打包出块，获得奖励。边缘节点使用 PoT（即 ProofofTelecommunication，通信证明)，每个节点依据其提供的通信服务获取奖励。请注意，这里的通信服务不是单纯的存储容量、网络流量、计算能力等，而是所有与通信有关服务的集合。

为保证边缘节点的服务质量，边缘节点需要向超级节点获取担保，担保过程采用投票和抵押机制。

4.4 文件加密去重

传统存储网络中，如云盘、CDN 甚至 IPFS，对于明文文件的去重技术已相当成熟，只需要对比两个文件的指纹信息，即可判定是否内容相同。但在加密存储应用中，上述方法已经失效，两个相同文件使用不同的公钥加密后产生的密文内容并不一样，无法简单地基于密文的指纹信息实现去重，同时数据的分片存储也使得去重变得

更加复杂。

SPoC 利用非对称加密和零知识证明技术，研发了一套文件加密去重技术。利用零知识验证方法，基于二次哈希，实现了密钥与文件分离、完整所有权认证、不使用第三方传递密钥等功能，解决了“收敛加密（CE）对重复数据的无用加密操作使计算开销随着数据负载去重率的提高而增加”的问题。即使是不同的用户同时在 SPoC 网络上存储相同文件，整个网络也只需要保存一份加密后的内容拷贝，而不用担心内容和隐私泄露，从而提升整个网络的存储效。

4.5 分块技术

SPoC 对待存储数据进行预处理，即将数据文件分割成多个碎片，并将其存放在不同的
SPoC 节点上。每个节点只需处理一小部分传入的交易，并且通过与网络上的其他节点并行处理，就能完成大量的验证工作。

在 SPoC 网络中，分块技术具有多层含义：在超级节点网络中，利用分片技术提升 TPS 和智能合约执行速度；在边缘节点网络中，通过将计算密集型和存储密集型任务进行分片，提高整个网络的计算能力和存储能力。

4.6 侧链技术

侧链技术可以提供交易效率，还可以在 SPoC 主链的基础上提供隐私保护等新功能。用户在使用这些新服务的时候，不会对主链产生任何影响，以满足未来 5G 时代不同的行业应用需求。

以侧链锚定的方式在更多的区块链上进行流通．开发者们可以根据业务形态的需要开发不同的侧链来接入 SPoC。侧链技术进一步扩展了区块链技术的应用范围和创新空间，使 SPoC 可以支持多种资产类型，并可以在侧链上建立智能合约开发 DAPP。

4.7 纠删码技术

由于闲置设备的不可靠性，设备掉线等现象时有发生。为了避免用户数据因设备掉线无法正常获取，必须对存储数据进行冗余存储。但如果仅对数据进行多备处理，根据乡农定理，存储的效率太低，因此引入纠删码技术。

纠删码技术在应用于云存储时,首先将用户文件分成 X+1 个大小相等且为 k 的倍数的数据段(不足的用 0 补齐),然后对每一个数据段作纠删码编码,在存放编码后得到的数据块 Di 与校验块 Dj 时,按下标分别存放到不同的文件分片中,例如文件数据段 0 的数据块 D0 存放在分片 0 中,D1 存放在分片 1 中,数据段 1 的数据块 D0 存放在分片 0 中,D1 存放在分片 1 中,依次类推。通过分片机制得到的文件分片每一个都是由文件不同部分的数据块和校验块组成的，分片中文件信息是分散的,即单个文件分片不会泄漏用户数据信息，这就保证了即使包括存储节点提供商在内的第三方非法取得单个节点上存储的分片,也无法获得用户文件内容,云存储中数据的隐私性得到可靠保障。

同时,由范德蒙德矩阵性质可知，在 n=k+m 个分片中，只要有 k 个分片能够正常使用,系统就能完全恢复用户的原始文件。这就意味着,即使某些分片被恶意删改,或者是系统中单个或多个存储节点失效时,用户数据也不会丢失。这一特点提高了云存储系统的容错性和冗余性，为数据的可靠性和完整性提供了保障。此外,应用 RS 纠删码在恢复用户文件时,最少只需要连接 k 个下载节点。连接的下载节点越少下载速度越快,下载延时越短。应用该算法的优点在于出现网络丢包或错误时,下载节点不需要采用重传机制,只需要重新选择其他节点完成下载任务。

4.8 人脸识别技术

- 人脸比对，

  指计算待识别的人脸与目标人脸相似程度，分析两张脸是否属于一个人的技术人脸比对专注一致性的认定，属于人脸识别中的 1：1

SPoC 科技的算法基于不同人脸结构特征与大量样本的学习，获得人脸模型对应的概率模型，通过匹配人脸的特征值，从而实现确认和识别过程，进而进行人脸解锁、面部识别通过后支付等行为

- 活体防伪技术

活体防伪，指运用算法手段判断摄像头前的用户是否为真人，防止他人利用高清照片、
视频、面具等方式仿冒目标人脸的技术
SPoC 的活体防伪技术不需要额外设备与复杂操作，是在线远程身份核查服务的
重要组成部分,可以满足金融等高安全性要求场景提供真人身份验证

4.9 超级算力技术

以超级计算为核心的计算科学与区块链、大数据和人工智能等信息技术的深度融合创新，推动技术应用于实体产业，将成为经济新旧动能转换的重要手段，SPoC 应用硅谷技术可以把散布在世界网络上的闲置算力进行整合管理,聚集，为超高性能的运算服务能力。

4.10 爱回收

开设垃圾币回收板块，通过人工智能算法进行数据抓取分析，实时开通兑换通道。可以兑换相应比例的 SPoC，清除垃圾币，改善数据环境，让数据更加轻便。

4.11.核心优势

综上所述，SPoC 具备以下核心优势：

- 高吞吐：通过改善 SPoC 的 TPS 实现，结合分片及侧链技术，目标 TPS 可达千万级别；
- 大容量：通过改善 SPoC 的底层网络文件系统实现，结合加密去重技术，理论可以提供无限存储空间；
- 高可靠：通过改善 SPoC 的区块链网络结构，结合超级节点和边缘节点双重分层共识，构建可靠可行的价值体系，确保整个网络稳定运行；
- 多样性：通过改善 SPoC 的智能合约实现机制以及任务调度模型，结合边缘计算网格，使得得智能合约适应大数据计算的应用场景；
- 高兼容：智能合约编写规范兼容市面主流公链，结合多重合约虚拟机机制，使得智能合约跨约跨链兼容，降低开发者的入门门槛；
- 低成本：通过优化 SPoC 经济模型，结合多重激励机制，实现消费体系和生产体系的良性循环，提供具有其他中心化设计和竞品所无法比拟的运行成本。
- 高安全：基于深度学习能力的人脸识别技术，提供人脸检测与属性分析、人脸 1：1 对比、人脸搜索、活体检测等能力。灵活应用于金融，，数据安全可控。

5、5G 实现技术核心

5.1 低时延传输与交换技术

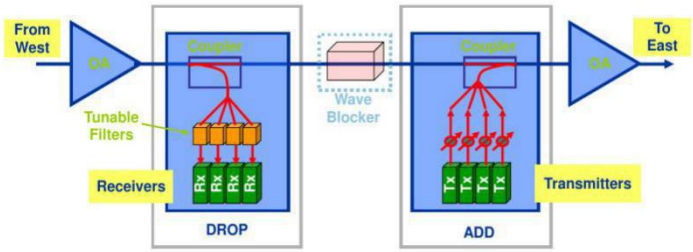
超低时延是 5G 业务相对 4G 非常重要的一个性能提升，对承载网提出苛刻的要求。毋庸置疑，基于 ROADM 的光层一跳直达是实现超低时延的最佳首选，但是只适用于波长级的大颗粒度传输与交换。而对于波长级别以下的中小颗粒度，如 1G/2.5G/10G/25G 等，主要还是通过优化 SPoC 映射、封装效率来降低时延。

5.1.1 ROADM

全光组网调度技术

SPoC 通过光层 ROADM 设备实现网络节点之间的光层直通，免去了中间不必要的光电-光转换，可以大幅降低时延。

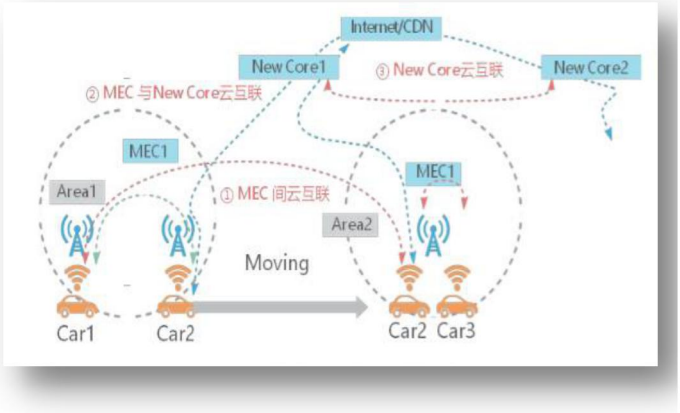
在技术实现上，基于 WSS（Wavelength Selective Switching，波长选择开关）技术 ROADM 已经成为业界，如下图所示，这是一个典型 CDC-ROADM（Colorless，Directionless & Contentionless ROADM，波长无关、方向无关、无阻塞 RODAM）的技术实现方式，基于 1xNWSS 以及 MCS（Multi-cast Switching，多路广播开关）器件，通过各类 WSS、耦合器、Splitter 等组件支持最大 20 个维度方向上的任意信道上下波。



随着 ROADM 技术的持续演进，下一代 ROADM 将朝着更高维度、简化运维的方向发展，基于 MCS 技术的 WSS 由于分光比太大，需要采用光放大器阵列进行补偿，其未来演进受到限制，尤其是难以向更高维度发展。MxNWSS 技术是一个重要的发展方向，相对于 MCS，其优势包括：

（1） MxNWSS 具有波长选择性，能够大幅降低分光损耗，减少光放大器需求，从而降低功耗，提高可靠性，能够支持更多的维度方向（例如 32 维）；

（2） MxNWSS 具有更紧凑的结构，有利于设备小型化



当网络逐渐走向全光架构，波长数目大幅增长，需要对全网光层实施有效管理、监测和追踪，是在全光网中最重要的技术。通过给光信道分配波长标签，可以在网络中的关键节点设置监测点，提取标签信息，由此获取每一个波长在网络中的传输路线、业务信息与状态，提高波长规划、管理的效率。

5.1.2 超低时延 SPoC

传送技术

目前商用 SPoC 设备单点时延一般在 10us~20us 之间，主要原因是为了覆盖多样化的业务场景（比如承载多种业务、多种颗粒度），添加了很多非必要的映射、封装步骤，造成了时延大幅上升。随着时延要求越来越高，未来在某些时延极其苛刻场景下，针对特定场景需求进行优化，超低时延的 SPoC 设备单节点时延可以达到 1us 量级。具体可以通过以下 3 个思路对现有产品进行优化：

（1） 针对特定场景，优化封装时隙目前 SPoC 采用的是 1.25G 时隙，以传送一个 25Gbps 的业务流为例，需要先分解成 20 个不同时隙来传输，再将这 20 个时隙提取恢复原始业务，这个分解提取的过程需要花费不少时延（~5us）。如果将时隙增大到 5Gbps，这样就可以简化解复用流程，能够有效降低时延（~1.2us），并且节省芯片内缓存资源。

（2） 简化映射封装路线常规 SPoC 中，以太业务的映射方式需要经过 GFP（Generic Framing Procedure，通用成帧规程）封装与 Buffer 中间环节，再装载到 ODU flex 容器，而在 OTU 线路侧，需要时钟滤波、Buffer、串并转换，整体时延因引入 Buffer 和多层映射封装而增大。新一代的 Cell 映射方式基于业务容量要求做严格速率调度，映射过程采用固定容器进行封装，可以跳过 GFP 封装、Buffer、串并转换等过程，降低时延。

（3） 简化 ODU 映射复用路径 SPoC 同时支持单级复

用和多级复用，理论上每增加一级复用，时延将增加 512ns。因此在组网是采用单级复用可以有效降低时延，如针对 GE 业务，多级复用（GE->ODU0->ODU2->ODU3->ODU4->OTU4）的时延约为 4.5us，而单级复用（GE->ODU0->ODU4->OTU4）的时延约为 2.2us。值得注意的是，在实际项目中，在追求极致时延特性的时候，也应当权衡适用性、功耗、体积、芯片可获得性、可靠性等其他因素，比如针对特定场景进行优化，可能就会导致应用场景受限。总之，随着未来芯片架构、工艺技术进一步提升，SPoC 设备可以通过多种渠道实现超低时延，逐步向理论极限逼近，同时更好地平衡其他性能参数。

5.2 高智能的端到端灵活调度技术

5G 时代，能够灵活调配网络资源应对突发流量是 5G 网络关键特征要求。对于网络的灵活带宽特性，依据承载硬件系统的逻辑管道容量与传输业务大小的匹配度，分为两种情况：

（1） 逻辑管道大于传输业务颗粒度，则单个逻辑管道承载多颗粒度业务，通过 ODUflex 技术实现传输带宽灵活配置和调整，以提高传输效率；

（2） 逻辑管道小于传输业务颗粒度，则需要考虑多端口绑定及带宽分配，如 FlexO 技术。此外，对于网络端到端的管理和控制，进行高效的网络部署和灵活的资源动态分配，完成业务快速发放，则需要利用软件定义网络（SDN）等新型集中式智能管控技术来实现。

5.2.1 ODUflex

灵活带宽调整技术

传统 ODUk 按照一定标准容量大小进行封装，受到容量标准的限制，容易出现某些较小颗粒的业务不得不用更大的标准管道容量进行封装，造成网络资源浪费。ODUflex，即灵活速率的 ODU，能够灵活调整通道带宽，调整范围为 1.25G~100G，其特点有：

（1）高效承载。提供灵活可变的速率适应机制，用户可根据业务大小，灵活配置容器容量，保证带宽的高效利用，降低每比特传输成本。

(2)兼容性强。适配视频、存储、数据等各种业务类型，并兼容未来 IP 业务的传送需求。

由于网络边缘接入业务将会非常复杂，如 5G、物联网、专线等，业务也具有临时性，因此还需要管道能够根据实际业务带宽大小，进行无损调节，这就要求支持 ITU-T 的 G.HAO（HitlessAdjustmentofODUflex，ODUflex 的无损伤调整）协议，该协议支持根据接入业务速率大小，动态的为其分配 N 个时隙，然后再映射到高阶 ODU 管道中，如果接入业务速率发生变化，通过 G.HAO 协议，网管控制源宿之间所有站点都会相应调整分配时隙个数，从而调整 ODUflex 的大小，保证业务无损调节。

针对 5G 承载，ODUflex 是应对 5G 网络切片的有效承载手段，通过不同的 ODUflex 实现不同 5G 切片网络在承载网上的隔离。

5.2.2FlexO

灵活互联接口技术

光层 FlexGrid 技术的进步，客户业务灵活性适配的发展，催生了 SPoC 层进一步灵活适应光层和业务适配层的发展，业界提出了 FlexO 技术。灵活的线路接口受限于实际的光模块速率，同时域间短距接口应用需要低成本方案，FlexO 应运而生。

FlexO 接口可以重用支持 OTU4 的以太网灰光模块，实现 N*100G 短距互联接口，使得不同设备商能够通过该接口互联互通。FlexO 提供一种灵活 SPoC 的短距互联接口，称作 FlexOGroup，用于承载 OTUCn，通过绑定 N*100GFlexO 接口实现，其中每路 100GFlexO 接口速率等同于 OTU4 的标准速率。

5.3 总结

SPoC 对于网络灵活调度极高，可借助 ODUflex、FlexO、ROADM/OXC（OpticalCrossConnection，全光交叉）等带宽灵活调度和调整技术，并通过引入 SDN 实现端到端的网络综合管控，实现网络资源的最优配置和管道

的最大利用效率，完成快速业务发放。

SPoC 标准完善，产业成熟，可以满足 5G 承载的提出的大带宽、低时延、高精度时钟、高可靠等多数需求，在此基础上通过技术演进补足短板，是实现 5G 高效承载的一条风险和成本俱佳的技术演进路线。

为了满足 5G 前传低成本和低时延的需求，需要对 SPoC 技术进行简化，包括减少复用层级、简化开销、使用更大的支路时隙（TS）等。同时，为了满足中传/回传在灵活组网方面的需求，需要考虑在增强 OTN 分组处理能力的基础上，增强路由转发功能。

6、应用场景

在 4G 时代，数据通常以接入层、汇聚层、核心层接入，业务数据在核心网集中处理，这种中心化工作方式难以满足 5G 应用场景对于低时延、大带宽和多连接的要求。5G 时代，针对不同的业务场景，业务将在不同节点分布式处理；以去中心化的工作方式提高效率和可靠性。随着分布式 AI 的崛起，5G 边缘网络平台将承载更多的算力和数据流量。

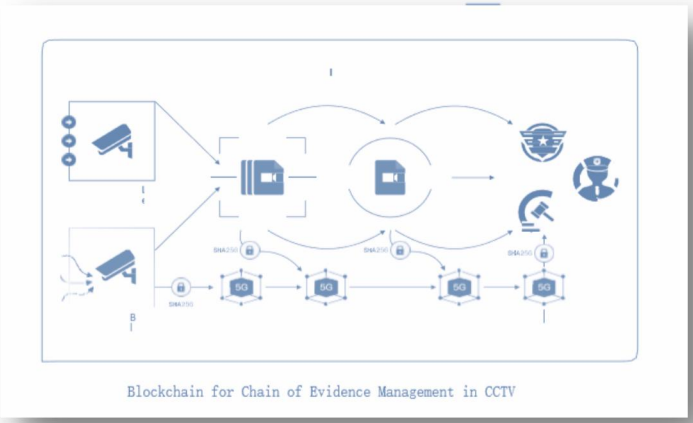
6.1 视频流场景

4G 技术促进了手机视频的普及。曾经有文字、静态相片的地方，现在有摄像头、视频博客、YouTube 频道、Facebook 直播、Snapchat 和 TikTok 等各种传播渠道。现在，5G 技术为超高清视频提供了基础。随着 5G 的普及，实时视频流在移动应用和社交媒体上将变得更加流行。

SPoC 支持 5G 架构下的视频流上链，SPoC 将视频内容分块转换为哈希值，存储在 SPoC 网络上，支持视频索引变量、储存变量置换，采用基于内容索引的方式，能够实现视频流的上链和智能合约操作，实现海量视频和图片的智能化解析。

SPoC 能够支持 5G 架构的以下视频场景：

- 支持摄像头多场景应用，例如可以对视频上的人脸进行 100 多个关键点的分析，生成每一个人脸的性别、年龄、服饰等详细信息。
- 将信息存储在 SPoC 网络上，利用区块链提供精准、高效的图像分析。
- 支持各种视频直播节目应用，提供去中心化视频版权保护，打破现有的应用中心化版权运作，真正保护原创直播视频的版权收益，并可以提供点对点的价值交换。
- 激励更多的终端贡献视频存储空间，通过通证激励机制盘活闲置视频存储资源。



6.2 车联网和无人机

5G 技术支持设备与设备之间的直接通讯，构建 D2D（DevicetoDevice)网络,因而各类物联网将迅速普及，首当其冲的便是“杀手级”应用——车联网领域。SPoC 在大数据管理、安全性、透明性和点对点交易方面具有独到优势，使得在车联网的自动驾驶、无人驾驶等领域设备协作成为可能。

SPoC 可用于整个汽车价值链，从供应链管理、汽车硬件制造到自动化驾驶，以及车辆生命周期数据跟踪，继而为自动驾驶提供数据，也能创造成本节约和优化运营流程。通过 PoT 模块将车辆数据接入链上后，如果车辆发生事故，未来 SPoC 能够保证数据及时采集，基于实时传输的物联网数据，完成保险赔付、二手车交易等金融场景使用。在车联网应用场景中，SPoC 支持自主身份，即将一个独特的身份标识存储于 SPoC 上，构成唯一的身份标识。另外，借助设备的可编程逻辑（智能合约) 控制器机制，可以利用区块链为芯片提供加密接口，从而在去中心化的环境下，保证系统的安全性。

6.3 软件定义广域网和网络附加存储 (SD-WAN+NAS)

SD-WAN（SoftwareDefinedWAN，即软件定义广域网）是当前企业和企业之间、企业和分支机构以及家庭应用的流行网络解决方案。根据咨询机构 Gartner 的预测，到 2019 年底，将有 30%的企业采用 SD-WAN 专线。5G 的发布将进一步简化网络连接策略，比如为企业间的视频会议提供高可靠性。

在 5G 架构下，企业级、家庭级用户可以通过 SD-WAN+NAS（NetworkAttachedStorage，即网络附加存储）的方式，利用超融合技术一起提供服务。SD-WAN 在应用层实现 5G 数据流的加密和流向控制，NAS 接入 SPoC 网络，可以实现存储的共享和备份。

在 SD-WAN+NAS 的应用场景中，SPoC 将提供高度的隐私性、点对点的交易，简化了信任构建，为高度自治、敏捷和简化的应用铺平了道路。SPoC 具备安全且固有的容错性，使用公钥加密和时间戳来验证每个记录或操作。利用 SPoC 的智能合约，通过公共分类账验证产品或交易的真实性，并减少监管和审计相关风险，同时在

双方建立了可信机制。

6.4 无线 Mesh 产品

无线 Mesh 是应用于 5G 网络连续广域覆盖和超密集组网场景中重要的无线组网技术，能够构建快速、高效的基站间无线传输网络，提高基站间的协调能力和效率，降低基站间进行数据传输与信令交互的时延。

有激励机制的无线 Mesh 被以太坊创始人 Vitalik 认为是区块链应用的最佳领域之一。基于通证的激励，借助物联网终端，SPoC 可以配合自组织，形成一个具有灵活性、去中心化、分布式、能够自我修复的无线 Mesh 网络，提供比互联网更高的速度和宽带，并且它通常是免费的，以便更加快捷方便、低耗能地为社交、娱乐、商业服务。

6.5 边缘计算

伴随着智能终端的发展，边缘计算的兴起，大量实时的需要交互的计算将在边缘节点完成。边缘计算的核心理念就是将数据的存储、传输、计算和安全交给边缘节点来处理，SPoC 网络恰好符合边缘计算架构，可以充分利用节点本身所具备的计算能力，就近完成物联网设备计算存储的对接需求，提升物联网感知-计算-响应这一过程的时效性。在物联网应用中存在大量需要低延时响应的使用场景，当云计算在这些领域一筹莫展时，SPoC 的边缘计算方案是一个新的解决途径。

7、经济模型

7.1 价值体系

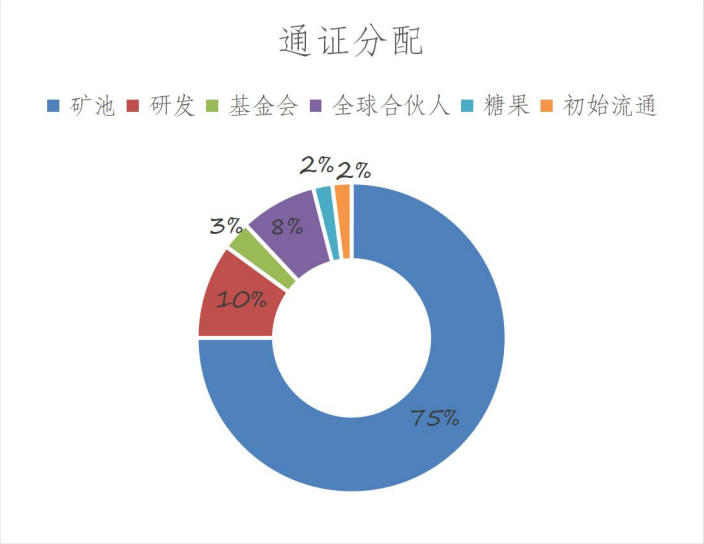
作为面向 5G 应用场景的公链，SPoC 的主要目标是支持 5G 复杂应用场景下的区块链应用，因而 SPoC 的通证将扮演非常重要的角色。**它体现了 SPoC 的下列价值主线:**

- **价值载体：**每一个应用场景接入或直接使用一定量的 SPoC，或定义自己的通证，并与 SPoC 进行一定比率的兑换。随着应用场景的逐渐丰富，SPoC 使用和消耗越来越多，SPoC 的价值也越来大。
- **交易属性：**与 EOS 类似，SPoC 上的每笔交易都无需要支付交易费用，其上的 DAPP 应用也需要使用 SPoC 抵押和购买资源，SPoC 支持智能合约，合约上的 SPoC 将通过交易进行原子级别的交易交互。
- **激励机制：**通过积极的激励计划，SPoC 激励人们主动提供系统验证交易，创造区块，利用济手段产生积极的反馈可以促进系统的不断发展。通证将作为奖励，激励社区持续为系统做出贡献。

7.2 通证分配

SPoC作为算力币，主要用来收益分红，体现币价。其波动性满足玩家的投资需求。

SPoC 基于 ERC-20 代币的标准发行量为5亿，永不增发。



通证分配	百分比	数量
发行总量	100%	5 亿
矿池	75%	3.75 亿
研发	10%	5000 万
基金会	3%	1500 万
全球合伙人	8%	4000 万
糖果	2%	1000 万
市场流通	2%	1000 万

8、发展规划（IPFS 联盟）

8.1 时间规划

2017 年 9 月　项目立项

2017 年 9 月　组建团队

2018 年 1 月 第一版钱包及第一款云矿机开发

2018 年 2 月 云矿场使用测试版上线以太坊，引爆社区

2018 年 8 月 项目基金会成立

2018 年 12 月 第三款游戏进行上线波场，一周内吸引 20 万海外粉丝注册。

2019 年 2 月 实体矿机项目规划

2019 年 5 月 研发实体项目，开启代码测试

8.2 未来规划

2019 年 9 月　代币发行、私募、上线交易所

2019 年 9 月 钱包正式上线，正式打通云矿场，云矿机

2019 年 11 月 实体矿机接入，起步实体矿场

2019 年 11 月 节点计划正式启动

2019 年 12 月 主网上线测试

2020 年 1 月　主网正式上线、塞班岛年会、登录全球前十大交易所

2020 年 2 月　完善矿场生态成立去中心化基金

2020 年 3 月　落地文字存储场景

2020 年 4 月　落地视频存储场景

2020 年 5 月 启动股权计划、落地

2020 年 6 月 开启收购计划收购多家矿场，矿机开发公司准备登录纳斯达克

8.2 矿机业务

8.2.1 云矿机上线

团队历时数月倾力打造的云矿机即将全网发布，挖矿静态收益、推广动态激励、动力奖池三项收益可累计享受，让全球参与用户收益最大化。预计在今年下半年 SPoC 主网上线时根据具体条件兑换实体矿机。参与用户可通过 SPoC 官网下载，进行挖矿。

8.2.2 云矿石上线

SPoC 矿石系统是一种众包模式的云计算方案。它汇集闲散储存空间,通过云计算的方式进行最优化的实时部署,帮助各大内容站解决存储不足等问题，真正实现共享

资源，收益最大化。

8.2.3 实体矿机

降低挖矿门槛,实现绿色节能的新型矿业体系，设计之初加入了一个抵押机制,用户可以将加密货币借给需要的矿工获取收益，它能够利用家庭的闲置资源，以及设备内的存储空间，来为项目存储碎片化的数据，提供分布式存储的能力。在稳定公链网络、提升交易速度的同时，矿工还可以通过挖矿设备为项目方提供稳定的宽带资源和存储能力，矿工的收益结构也更加多元化，挖矿收益也更高

8.2.4 实体矿场

PoC 共识机制，容量证明绿色节能，低功耗（25 瓦）低噪音无热量。POC 硬盘矿机拒绝了传统的垄断形式，无需全球寻找丰水电费，任何城市都能搭建矿场，都能轻松参与挖矿，挖矿减少了电量的损耗将大大的提高回本周期。

用户矿机托管，收费，质押分红。与此同时实体矿场不仅可以接入 SPoC 项目，也接入以 PoC 机制为主的多币种进行收益最大化。

9、管理团队、投资机构和合作白名

9.1 核心团队

Jay

是硅谷连续创业者，领导过数个创业项 目，在区块链技术和加密货币领域有4年的研究经验。在此之前曾任职于美国私募基金与投行，完成过数个上亿美元项目的投资和并购。

Allan

全栈工程师，拥有超过10年的开发经验。谷歌8 年的工作经验，领导过多个谷歌项目。此外在硅谷数个创业公司担任技术合伙人。Allan在区块链领域有着非常丰富的开发经验，开发过数个极受欢迎的Dapp。

Sunny

拥有超过 6 年的软件开发和网站开发经验。曾参与多项软件系统设计、游戏软件开发 、机器学习模型建立。Sunny曾任职于facebook区块链小组。

Lee

拥有超过8年的网页和移动端全栈开发经验，曾任数个硅谷科技公司的tech leader。 在此之前他还有机器视觉和图像处理领域的 研发经验。他拥有丰富的Dapp 和智能合约开发经验。Lee毕业于CMU,曾任职于Uber。

Tuo

拥有超过3年的后端软件服务开发 和架构设计经验，曾在美国热门Startup任职 软件工程师。在此之前他还有移动端app和 物联网硬件产品的开发经验。Tuo曾任职于谷歌。

Nick

亚太地区运营负责人，精通中，韩，日三国语言。有超过8年的市场运营和推广的经验。曾任职于多个公链项目的市场负责人。

Jessica

北美及欧洲地区运营总负责人。拥有 8 年以上的

市场运营与媒体公关经验 。曾是一名首席记者与公关，与腾讯、优酷 等多家媒体 深度合作;拥有多年虚拟货币以 及区块链项目个人投资经验。Jessica负责项目在欧美的市场运营，市场战略以及公共关系。

9.2 顾问团队和投资机构

团队拥有来自全国各地知名机构的行业顶尖人才：

Charles

早期的区块链传道者，专注于超高速交易和图表分析，欧洲加 密社区的建设者和意见领袖。

Lam

5年平面设计经验，3年UI/UX设计经验，擅长界面和动效设计。曾多个参与智能家居，AR以及 区块链产品设计。

Clarence

新加坡资深律师，在区块链及虚拟货币领域有着十分丰富的经验。服务对象主要为当地的国际银行、基金会、基金经理、大型房地产开发商和业主，也包括一些初创公司。

9.3 合作白名单

IPFS

星际文件系统 IPFS（InterPlanetary File System）是一个面向全球的、点对点的分布式版本文件系统，目标是为了补充（甚至是取代）目前统治互联网的超文本传输协议（HTTP），将所有具有相同文件系统的计算设备连接在一起。原理用基于内容的地址替代基于域名的地址，也就是用户寻找的不是某个地址而是储存在某个地方的内容，不需要验证发送者的身份，而只需要验证内容的哈希，通过这样可以让网页的速度更快、更安全、更健壮、更持久。

BHD

基于Proof Of Capacity 的新型加密货币 ，BHD采用升级版的cPOC挖矿， 称之为Conditioned Proof Of Capacity，拥有完美的经济模型和共识算法 ，是用硬盘作为共识的参与者，降低了加密货币对电力资源的消耗 ，挖矿降低了参与门槛，让其生产方式更趋向去中心化方式，更加安全可靠 ，相对POW 挖矿， cPOC

挖矿更加绿色节能，低功耗，低噪音，无热量，抗ASIC化降低了共识信用成本，增强了共识强度、广度和共识结构的安全性

IPFS&Filenet（FN）

IPFS&Filenet 是构建在 IPFS 之上的一个激励层，以奖励矿工共享自己的存储资源和网络资源。Filenet 同时是一个令牌，它运行在分发证明机制上，是一种基于 IPFS 提供内容共享的超级云系统，致力于存储和分发有价值的内容

YottaChain

YottaChain 是由中国十大青年科学家王东临带队打造的区块链存储公链，YottaChain 通过连接全球分散的存储资源，打造一个规模浩瀚的星际存储池，能确保每个人的数据主权，比现有中心化存储具有压倒性优势（可靠性提升万倍、成本降低数倍，并具备抗 DDoS 和容灾等特性）。YottaChain 掌握区块链存储核心科技，拥有 200 多项国内外专利技术，其核心 TruPrivacy 技术是全球唯一能实现加密后去重的技术，并荣获全球专利，从而改变存储行业格局。

Galaxy Network

GN 将打造新一代雾 CDN，触及数以万计的智能设备，使其成为网络节点。GN 作为 POC 共识机制的以太坊，搭载智能合约支持其他类 POC 项目快速完成代币发行，同时也将利用成熟硬盘挖矿技术，协助 GN 侧链快速建立自己的 POC 矿业生态。雾 CDN 更加去中心化，相对于云的集合状态，雾的状态是离散型状态，数据分布式存储于边缘设备而非中心化服务器之中，多(弱)中心化 CDN 加速，比如光猫，路由器，桌面型矿机，NAS，电脑，pad，手机等等，没有场地限制，没有宽带要求，只需稳定在线。结合存储数据和扩展性对于雾 CDN 的作用相当重要，通过区块链技术以及 POC 共识能够真正使雾 CDN 落地。

10、免责申明和风险提示

本声明不涉及与证券招标以及承担 SPoC 经营性的相关风险，不涉及任何在司法管制内的受管制产品，本文件是项目阐述的概念性文件。白皮书并非出售或者征集招标与 SPoC 产品及其相关公司的股份、证券或其他受管制产品。

根据本文件不能作为招股说明书或其他任何形式的标准化合约文件，也并不是 构成任何司法管辖区内的证券或其他任何受管制产品的劝告或征集的投资建议。本文件不能成为任何销售、订阅或邀请其他人去购买和订阅任何证券,以及基于此基础上形式的联系、合约或承诺。本白皮书并没有经过任何国家或地区的司法监管机构审查。不作为参与投资的建议：在本文件中所呈现的任何信息或者分析，都不构成任何参与代币投资决定的建议，并且不会做出任何具有倾向性的具体推荐。您必须听取一切有必要的专业建议，比如税务和会计梳理相关事务。不能构成任何声明和保证：本文件用于说明币游链项目所提出的 SPoC，但 SPoC 基金会明确表示：

（1）对于本文件中描述的任何内容的准确性或完整性，或者以其他方式发布的、与项目相关的内容，不给予任何声明和保证；

（2）在没有前提条件的情况下，不能对任何具有前瞻性、概念性陈述的成就或合理性内容给予任何声明和保证；

（3）本文件中的任何内容，不作为任何对未来的承诺或陈述的依据；

（4）不承担任何因白皮书的相关人员或其他方面造成的任何损失；

（5）在无法免除的法律责任范围内，仅限于所适用法律所允 许的最大限度。不是任何人都可以参与项目：SPoC 建设并不是任何人都可以参与，参与者可能需要 完成一系列的步骤，其中包括提供表明身份的信息和文件。非授权公司与该项目无关： 除了SPoC基金会，使用其他任何公司或者机构的名称商标，并不说明任何一方与之有关联或认可，仅供说明相关内容之用；

（6）依照部分国家和地区的监管政策，SPoC 公募与私募阶段均需要严格的 SPoC 机制，不针对包括中国、美国、新加坡等国家和地区的投资人开展相关活动。