

PCS

白

皮

书

beta 1.0

一个轻量级去中心化区块链应用开发平台

摘要	3
第一部分 PCS 设计理念和创新	4
1.1 区块链诞生的意义	4
1.2 为什么设计 PCS	5
1.2.1 打造一个轻量级的区块链开发系统	5
1.2.2 现阶段区块链技术痛点	6
1.3 PCS 的主要创新	7
1.3.1 PCS 人性化的区块链编程操作	7
1.3.2 PCS 的共通性和兼容性设计	8
1.3.3 PCS 提升底层公链的可拓展性	8
1.3.4 PCS 支持秒级处理速度	9
1.3.5 用户免费使用网络资源	9
第二部分 PCS 实现方案	10
2.1 PCS 公链	10
2.2 共识机制	10
2.3 技术优势	11
2.3.1 去中心化机制保证系统安全	11
2.3.2 弱审核机制，自由发行通证	11
2.3.3 七层架构模型	12
2.4 账户	12
2.5 虚拟机独立架构机制	13
2.6 身份和隐私	13
第三部分 PCS 应用	14
3.1 去中心化应用	14
3.2 使用侧链支持跨链资产交易及分红	14
3.3 多个行业的支持	14
3.4 社区福利应用	15
第四部分：PCS 资产发行	15

摘要

PCS 是诞生于数字货币区块链 3.0 时代的多元化的区块链生态系统， 它以一个轻量级的区块链开发系统呈现， 旨在打造一个可以堪比 Microsoft 这样的世界级开发平台， 它将颠覆比特币和以太坊、 乃至以及现阶段所有区块链项目的运行规则， 成为每一个人都可以触手可及的区块链编程系统。

在 PCS 系统中， 可以通过价值传输协议 (Value Transfer Protocol) 来实现点对点的价值转移， 并根据此协议， 构建一个面向个人的区块链编程系统， 同时构建一个支持多个行业的 (金融、 物联网、 供应链、 社交游戏等) 去中心化的应用开发平台 (DAPP Platform) 。

运行在 PCS 区块链上的不同形态的、 异构的区块链资产可以通过该区块链生态系统进行登记、 交换、 存储、 以及基于之上更复杂的交互操作。 PCS 希望通过不断突破区块链技术的应用边界和技术边界， 使普通互联网用户能感受到区块链技术的价值。

PCS 通过领先的设计理念和创新的设计思路来实现， 具备支持秒级高频交易、 去中心化机制保证系统安全、 弱审核机制， 自由发行通证、 人性化的设计， 易于上手等技术优势。 并通过 Identity， Oracle 和 Data feeds 的引入， 在合规性方面， 符合不同行业的监管需求。 PCS 的共识机制采用了委托权益证明机制 (Delegated Proof of Stake)， 避免了工作量证明 (Proof of Power) 的资源浪费， 系统也更快更安全， 为企业级应用奠定了基础。

另外在脚本和虚拟机方面， 在 PCS 的测试网络中， 我们将兼容 EVM， 后期通过标记不同的虚拟机类型， 可以支持更多的虚拟机， 包括 LLVM 和 Lua 以及 EVM2.0. 以及 为 VM 开发的更严格的编程语言。

最后， 面向移动端策略 (Go Mobile) 也是 PCS 特别重视的一个战略， 在 PCS 的生态系统中， 我们将会与第三方开发者， 一起从技术架构支持提供移动端的服务，

包括：移动端钱包、移动端 DAPP 应用、移动端智能合约服务。我们也鼓励第三方的开发者，加入我们，一起开发区块链的移动端服务，共同推动区块链技术的落地。

第一部分 PCS 设计理念和创新

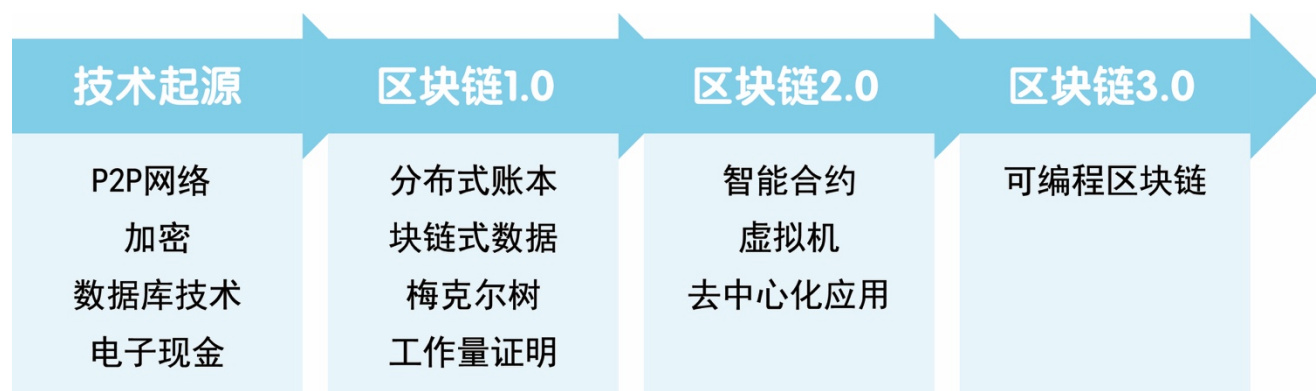
1.1 区块链诞生的意义

在 2009 年 1 月 3 号，比特币的创始区块被挖出，并在第 170 个区块发生了第一笔比特币的转账交易，从此开启了比特币网络作为一种点对点的价值交换网络蓬勃发展的时代，虽然中间经历了各种危机，但是比特币网络的价值从零开始，到今天已经成为一个价值约 1100 亿美金的点对点支付网络。

区块链技术给数字经济时代带来了巨变的曙光。

区块链的意义在于可以构建一个更加可靠的互联网系统，其去中心化、可追溯性、公开透明等特性可以从根本上解决价值交换与转移中存在的欺诈现象。进一步的研究发现，区块链技术具备一种“降低成本”的强大能力，能简化流程，降低一些不必要的交易成本及制度性成本。

这种能力应用于许多社会领域中，对于改善当前低迷的经济环境更有现实意义。越来越多的人相信，随着区块链技术的普及，数字经济将会更加真实可信，经济社会由此变得更加公正和透明。



1.2 为什么设计 PCS

1.2.1 打造一个轻量级的区块链开发系统

自从 2009 年比特币代码开源以来，区块链和数字货币被公众接受的程度越来越高，无数的开发者和社区人员一起参与和见证了区块链技术的快速发展。它已被大量的应用于行业的各种创新实践中，并同时创造了服务和商务运转的新方式。

区块链技术的发展可分为三个阶段：1.0 时代的代表是比特币，2.0 时代的代表是以太坊智能合约，而当下最热门的区块链项目之一 EOS 是被公认的区块链 3.0 时代的代表，探索着区块链应用领域的发展。相对于 IT 界数十年来的领导者 IBM 和 Microsoft 来说，EOS 相当于 IBM。IBM 是国际商用电器公司，在整个计算机和软件行业的发展过程中，取得了瞩目的成就，但它的发展依然不及家喻户晓的 Microsoft，为什么呢？

Microsoft 的定义与 IBM 完全不一样，从品牌的命名就可见一斑，IBM 是面向企业级的商业计算机解决方案，而 Microsoft 微型计算机，则是面向个人用户的计算机解决方案。定位的一不一样，造就了两个公司的成就不一样，微软把计算机和可视化的操作系统带给了每个人，极大的提升了整个社会的效率，同时微软也成为了最伟大的计算机软件公司。

今天，有了面向企业级别的区块链商业解决方案 EOS，同样也还会有面向个人的区块链商业解决方案，这就是“Personal Chain Operation System”，个人区块链操作系统 PCS。

所谓个人区块链操作系统，并不意味着只针对个人用户，而是要通过区块链技术形成一个轻量级的区块链服务，让 DAPP 开发走向个体，让每一个普通的用户都可以享受到区块链应用。

1.2.2 现阶段区块链技术痛点

A . 对共识机制的挑战

对于区块链技术中的共识算法现在已经提出了多种共识机制，最常见的如 PoW、PoS 系统。但这些共识机制是否能实现并保障真正的安全，需要更严格的证明和时间的考验。

区块链中采用的非对称加密算法可能会随着数学、密码学和计算技术的发展而变的越来越脆弱。以现在超级计算机的算力为例，产生比特币 SHA256 哈希算法的一个哈希碰撞大约需要 2^{48} 年，但随着今后量子计算机等新计算技术的发展，未来技术中对于非对称加密算法可能具有一定的破解性。其次，在比特币的机制下，私钥是存储在用户的本地终端中，如果用户的私钥被偷窃，依旧会对用户的资金造成严重损失。区块链技术上的私钥是否容易窃取的问题仍待进一步的探索与解决。

B . 网络吞吐量小

正如我们看到的，在去中心的设计下，所有节点都在计算、存储各分布式账本的数据，每次计算所需时间较长，交易吞吐量相当有限(1MB)，例如比特币的底层设计仅支持每秒 7 笔交易。这样的网络吞吐量目前无法支撑更多区块链的商业化应用。

C . 不同区块链间兼容性弱

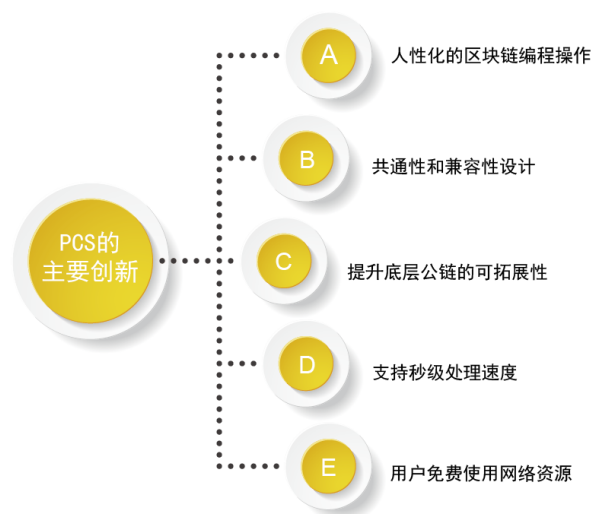
不同区块链之间存在着兼容性的问题，例如基于 UTXO 模型的比特币生态和基于 Account 模型的以太坊生态很难有兼容性。区块链的兼容性主要考察的是区块链系统、智能合约和数据层三个方面的因素，需要处理底层多种关系型和非关系型的数据，实现起来会比较复杂，需要很多兼容设计。

PCS 出现目的是解决现有的区块链应用性能低、安全性差、开发难度高以及过度依赖手续费的问题。PCS 将创建一个对开发者友好的区块链底层平台，类似区块链的操作系统，性能强大，可以同时支持多个应用程序同时运行，可支持多种变成语言；通过并行链和 DPOS 的方式解决了延迟和数据吞吐量的难题；并广泛引入如下特性：基于角色的权限管理、用于界面开发的 WEB 工具包、自描述接口、自描述数据库体系、还有一个声明式许可方案，从而更好完成 PCS 的超越区块链愿景。

1.3 PCS 的主要创新

1.3.1 PCS 人性化的区块链编程操作

微软带来全新的 PC 机操作体验，让所有人利己脱离简单枯燥的字符串，使用更加简单的鼠标来操作 PC 机。而 PCS 将带来全新的区块链编程体验，它有点类似于微软的 windows 平台，通过创建一个对开发者友好的区块链底层平台，支持多个应用同时运行，为开发 dAPP 提供底层的模板。让所有没有编程经验的基础的人，也能编写出属于自己的区块链 DAPP，让 DAPP 开发走向个体。



1.3.2 PCS 的共通性和兼容性设计

PCS 的设计哲学中，对共通性和兼容性的考虑非常充分。在整个数字货币领域，我们知道基于 UTXO 模型的比特币生态和基于 Account 模型的以太坊生态很难有兼容性，随着数字货币的发展，目前已经有接近 2000 种数字货币在流通，而且每天都有大量的新币种在发行，这就要求基础公链具备更强的包容性。

PCS 的设计可以兼容比特币网络和以太坊网络，一方面为以后借力比特币的 BIP 协议，提供了技术上的可能性。而 Ethereum 第一次将智能合约的概念从理论变成实际，从而拓展了区块链技术的边界，其 EVM 是目前为止唯一 一个经过测试的智能合约虚拟机，因此保持和 EVM 的兼容性，就显得非常重要，因此 PCS 的虚拟机将保持和 EVM 的兼容性，所有在以太坊平台上面开发的智能合约，也可以在 PCS 平台上面运行。

软件的向下兼容性也是一个非常重要的问题，使用旧版本创建的文件和智能合约，将能持续在新版本上面运行，而不用用户强制升级，这将会给用户带来很多便利。因为智能合约的特殊性和一次性部署，如果不能实现向下兼容性，将会给已经执行过的智能合约带来很大问题，也造成后期软件无法迭代和升级，也会出现 EVM2.0 和 EVM1.0 无法兼容的问题，这也是区块链系统软件设计者需要注意的问题。

1.3.3 PCS 提升底层公链的可拓展性

作为一个去中心化的操作系统，当出现分歧时能否达成共识，在避免硬分叉的前提下保持迭代，将成为一个至关重要的问题。

在公链的运行中，底层的代码出现 bug 是无法避免的，但频繁出现 bug 会丧失用户对其的信任度。PCS 公链从整体架构的设计上解决了这个问题，当系统出错的时候，能够根据可读性意图来区分这个错误是否确实是 bug，并且来判断社区的修复是

否正确。例如当系统遭到攻击时，其中的节点将会迅速采取行动冻结黑客账户，然后通过投票采取有效的处理方式，避免了因无法共识而出现的硬分叉问题。

1.3.4 PCS 支持秒级处理速度

以太坊以及目前大部分的区块链应用最让人诟病的一点就是“慢”和“拥堵”，特别是在交易量堆积的时候，目前比特币实际应用中仅能支持大约每秒 7 次的转账，以太坊也仅能支持每秒数十次转账。如何在安全的前提下实现高速处理是区块链底层公链突破的重点。

PCS 采用了 DPOS（股份授权证明）共识算法机制，在有限制的测试条件下已经实现了每秒上万次的交易量。后续，PCS 将使用并发技术来继续扩展其网络性能，有望实现每秒数百万次的交易处理能力。届时将解决底层公链的速率和拓展性问题，将可同时支持数千个商业级的分布式应用程序（DAPP）在其平台上运行。

1.3.5 用户免费使用网络资源

不管是比特币还是以太币，在过去都做了很好的尝试，都有手续费，而 PCS 的用户不必为了使用平台而付出费用。这样可以免费使用的平台自然可能会得到更多的关注。有了足够的用户规模，开发者和企业可以创建对应的盈利模式。

第二部分 PCS 实施方案

2.1 PCS 公链

PCS 公链是一个支持多行业的去中心化区块链应用开发平台，通过完善的设计，将区块链技术的优势以更加灵活便捷的方式带给不同行业的应用者和普通互联网用户。

PCS 通过共通性和兼容性创新、提升底层公链的可拓展性、支持秒级处理速度等技术优势，采用委托权益证明机制（Delegated Proof of Stake）的共识机制，避免了工作量证明（Proof of Power）的资源浪费和权益证明机制（Proof of Stake）的中心化趋向，系统也更快更安全，为企业级应用奠定了基础。

PCS 的目标是：通过持续性的区块链技术研发和创新，为企业用户、普通用户搭建一个开放、透明、安全和多元化的生态系统。

2.2 共识机制

PCS 的共识机制采用了委托权益证明机制（Delegated Proof of Stake），避免了工作量证明（Proof of Power）的资源浪费，系统也更快更安全，为企业级应用奠定了基础。根据 DPOS 共识机制，全网持有代币的人可以通过投票系统来选择区块生产者，一旦当选任何人都可以参与区块的生产。

PCS 里预计每 3 秒生产一个区块。任何时刻，只有一个生产者被授权产生区块。如果在某个时间内没有成功出块，则跳过该块。

PCS 架构中区块产生是以 21 个区块为一个周期。在每个出块周期开始时，21 个区块生产者会被投票选出。前 20 名出块者首选自动选出，第 21 个出块者按所得投票

数目对应概率选出。所选择的生产者会根据从块时间导出的伪随机数进行混合。以便保证出块者之间的连接尽量平衡。

如果出块者错过了一个块，并且在最近 24 小时内没有产生任何块，则这个出块者将被删除。这确保了网络的顺利运行。

在正常情况下，DPOS 块链不会经历任何叉，因为块生产者合作生产区块而不是竞争。如果有区块分叉，共识将自动切换到最长的链条。具有更多生产者的区块链长度将比具有较少生产者的区块链增长速度更快。此外，没有块生产者应该同时在两个区块链分叉上生产块。如果一个块生产者发现这么做了，就可能被投票出局。

2.3 技术优势

2.3.1 去中心化机制保证系统安全

PCS 是一个网络节点分布在全球的“公司”，意味着 PCS 不会倒闭，PCS 少只需要 3 台联网的电脑就能自动运行。PCS 所有业务都由网络自动运行及智能合约完成，和比特币一样是一个全自动无人值守的系统。

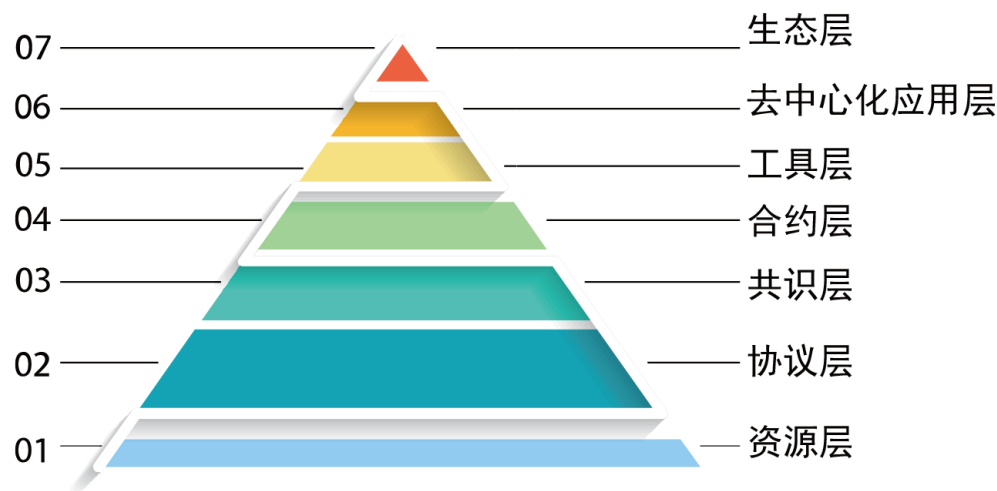
2.3.2 弱审核机制，自由编写智能合约

因为 PCS 是一个纯粹地去中心化系统，所以采取弱审核机制。用户可以自由使用 PCS 的任何功能，完全没有限制。同时允许个人或企业在 PCS 系统内自由编写和发行自己的智能合约，并且通过智能合约构建自己的通证积分体系。最主要的是 PCS 的智能合约发行功能是通过可视化界面操作的，即使没有代码编写的技能，也能编写出自己想到的合约，这也是 PCS 向微软学习的一大进步，把编写代码的工作界面化可视化。PCS 将会是区块链金融的基础设施，致力于和传统的互联网和非互联网企业相结合，

创新区块链国民生产和生活的每个行业，比如零售行业、餐饮行业、服务行业、文化艺术产业等等。





2.3.3 七层架构模型

PCS 作为一个区块链应用开发平台，为整个区块链技术生态提供了完备的发展体系和架构，从资源层、协议层、共识层、合约层、工具层、去中心化应用层到生态层等七个层次完善了一个生态布局。



2.4 账户

PCS 允许使用唯一的长度为 2-32 个字符的可读的名称来实现对账户的引用，和现有账户体系一样简单，账户具备多层级角色管理，并为用户提供了一种在密钥被盗时恢复其帐户控制的方法，确保账户安全。

 账户管理	 密匙管理	 权限管理	 风控审计
账户注册 账户登录 账户注销 不相关性	密匙生成 密匙关联 密匙保险箱 密匙签名链	权限分级 权限控制	用户关联 审计控制 风控管理

2.5 虚拟机独立架构机制

在合约层 PCS 通过开放 API 接口来使虚拟机与 PCS 进行集成，并且脚本语言和虚拟机的实现将独立于 PCS 操作系统技术，任何开发语言或虚拟机只要有适当的、性能足够的沙箱都可以通过 API 与 PCS 集成在一起。目前 PCS 的设计将支持 Web 组件和类以太虚拟机（EVM）。由于虚拟机与 PCS 的分离，使得开发人员可以选择自己熟练的编程语言进行智能合约的开发，可使 PCS 上的应用开发更加灵活，从而大大降低了区块链技术的使用门槛。

2.6 身份和隐私

PCS 系统将通过智能合约管理 PCS 平台上的用户。PCS 系统将提供可选的身份识别模块，Identity 是区块链系统可以对接金融系统的前提条件。在 PCS 系统中，我们将区分 Identity 客户和非 Identity 客户。PCS 系统开发者将计划开发基于相应的 Identity 智能合约代码，并把代码开源给第三方。通过第三方征信机构的引入，在 PCS 系统中，通过 Identity 智能合约验证的客户将会拥有更多的优先级。

关于隐私，因为 PCS 系统兼容 UTXO 模型，将通过加密传输协议，给 PCS 系统中的交易提供更多的隐私保护。

第三部分 PCS 应用

3.1 去中心化应用

DAPP 是运行在分布式网络上，参与者信息被安全存储、隐私得到很好保护，通过 PCS 公链可以实现网络节点去中心化操作的应用程序，它结合了前端界面与智能合约，前端用户可以选择各种命令，智能合约则支持实现应用功能与区块链交互。

PCS 将不同的 DAPP 想法产品化，使普通互联网用户可以真正感受到区块链技术带来的价值。例如去中心化的社交、去中心化的存储和去中心化的域名服务、去中心化的计算服务等，通过激励机制的引入，将更深层次利用共享经济的理念，改变现有的 APP 市场和商业模式。在这样的模型之下，仅需做好商业模型设计和用户体验，区块链团队即可开发出基于区块链的应用程序，也就大大降低区块链的准入门槛。

随着移动互联网和区块链技术的发展，开发者可以在移动端进行更多 DAPP 应用的开发和落地，让更多用户可以享受 PCS 的红利。

3.2 使用侧链支持跨链资产交易及分红

作为一个去中心化的底层公链，在 PCS 上可以建立更多的侧链，而不同的侧链构成了整个 PCS 生态系统，在这个生态系统内所有的资产都可以通过区块链技术实现交易及分红。

3.3 多个行业的支持

在 PCS 系统中，可以通过价值传输协议（Value Transfer Protocol）来实现点对点的价值转移，并根据此协议，构建一个支持多个行业的（金融、物联网、供应链、

社交游戏等）去中心化的应用开发平台（DAPP Platform）。这样一个平台的搭建可以实现对更复杂商业逻辑的支持。

3.4 社区福利应用

用户还可以选择 3 个社区福利应用，也称为智能合约。这些智能合约将根据每个应用程序从 Token 持有者收到的选票比例来收取 Token。经选举的应用程序或智能合约可以由新当选的应用程序或 Token 持有人的智能合约所替代。



第四部分：PCS 资产发行

PCS 链上的 Token 即为 PCS 币，是 PCS 链对于打包交易者以及系统参与节点分发的一种特殊的 Token，采用 DPOS 机制，鼓励更多矿工参与到其生态中。共发行 PCSX PCS 币的价值：

- A. 资产发行
- B. 资产交易的手续费

C. 收益权资产的分红

D. 链上资产交换

