

Portaldot White Paper



高性能全球区块链应用网络服务系统

Version 1.3

POT Foundation 版权所有

前 言

2013 年，区块链技术因为比特币的全面火爆而风靡全球。从以比特币老牌数字货币为代表的区块链 1.0 到具有智能合约功能的公共区块链平台以太坊，区块链进入 2.0 时代，再到现在的区块链 3.0 时代，必定是与实体经济深度融合。全球区块链产业未来社区化将进一步加速，包括区块链技术发展带来的新的商业模式和生产关系变革，全球各国区块链监管政策的进一步细化与完善，将影响数字资产投资用户在区块链上的投资选择，有线下实体产业做支撑的区块链项目和应用场景落地的项目将被用户热爱。

近两年，国内外经济发展环境、条件、要求均在不断变化，以贸易战为代表的国际关系事件使实体经济增长面临压力。一方面是贷款增速和总额的数据统计激增，一方面却是实体商家融资难的呼声。当前，各银行在执行落实国家金融扶持政策时，出于自身金融风险等因素考虑，仍然设置了较为严格的放贷门槛，导致缺少抵押物、经营风险较大的实体商家不仅难以从银行获得贷款，更难通过企业债券、股票等方式直接融资，实体商家融资难、融资贵问题仍未得到根本解决。

POT 公链是由 Portaldot Foundation（简称 POT 基金）投资研发，基金会主要经营范围：区块链网络技术研发，数字资产管理。

Portaldot Foundation 从 18 年立项研发，汇聚了来自全球顶级的极客技术人才，包括中国大陆知名的区块链技术开发团队，一起参与 POT 的开发。在这个过程中基金会也致力于 POT 生态的扶持与建设，支持了包括电商平台、通证餐饮、竞游联盟平台等第三方平台的开发孵化，帮助实体产业进行数字经济发展。

目 录

前 言.....	I
一、 项目背景.....	1
1 全球区块链行业现状.....	1
1.1 产业生态初步形成.....	4
1.2 产业链条脉络逐渐明晰.....	5
2 全球区块链发展趋势.....	5
2.1 区块链发展前景.....	6
2.2 区块链技术赋能实体.....	8
2.3 区块链+大数据.....	9
3 POT 的发展契机.....	10
二、 项目介绍.....	11
1 POT 定位.....	11
2 项目核心优势.....	11
2.1 团队优势.....	11
2.2 POT 解决传统商家痛点.....	12
2.3 实体商家的一站式服务平台.....	12
3 POT 通证计划.....	12
三、 应用列举.....	15
1 跨境支付.....	15
2 社交电商.....	15
2.1 链哆哆电商平台.....	16
3 多边贸易融资.....	17
4 移动通信应用.....	17
四、 技术策略.....	18
1 概述.....	18
2 架构设计总揽.....	19
3 核心层设计.....	20
3.1 共识插座.....	20
3.2 P2P 网络.....	20
3.3 交易池.....	20
3.4 存储.....	23
3.5 RPC (Remote Procedure Call) 接口.....	24
4 功能层设计.....	25
4.1 共识机制.....	25
4.2 智能合约.....	31
4.3 账户体系.....	33
4.4 资产管理.....	34
5 优势.....	35
5.1 无分叉升级.....	35
5.2 高度可扩展.....	35
5.3 异构多链.....	36
五、 基金会.....	36
1 基金会介绍.....	36
2 组织委员单位.....	37
六、 合作伙伴.....	38
七、 发展历程.....	39
八、 风险提示.....	40
九、 免责声明.....	41

一、项目背景

1 全球区块链行业现状

2018 年，全球区块链融资市场规模快速增长，其中亚太市场将扮演重要角色，驱动全球市场发展，特别是得益于中国、印度以及东南亚国家的快速增长。北美过去几年有着不可忽视的市场地位，预计未来仍然将保持稳定发展，特别是美国，美国的变化将对全球区块链融资的发展产生重要影响。就目前的形式来看，全球变化较快且不可预测，未来区块链融资行业发展将充满更多变数。

欧洲引领全球区块链行业

在自身开源文化推动下，欧洲在各个方面均引领了世界区块链行业的发展，不论个人还是企业机构都积极参与到区块链项目中。调查显示，欧洲区块链创业公司主要集中在伦敦、阿姆斯特丹、巴塞罗那、柏林和瑞士 Cryptovalley 等地。

美国区块链产业发展滞后

据 OBLIFetlier VentBLIFERes 统计，尽管世界上四分之一的区块链公司来自美国，但这些公司都仅仅专注于比特币等加密货币领域，只有极少一部分公司涉猎区块链在非货币领域的应用，在医疗、保险、能源、供应链等国家正在着力开发的垂直领域里，美国的区块链行业发展已经明显落后于其他国家。作为世界金融中心的美国在区块链创新领域的表现可谓让人大跌眼镜。有专家认为，美国这种“滞后”与

企业创新能力无关，主要是受到了监管体制的限制。美国两家知名的区块链公司 Kraken 和 Coinbase 均坐落在湾区，但都是以比特币等加密货币作为主要业务的。

美国社交网络巨头 Facebook 在 2019 年 6 月 18 日发布了加密货币项目 Libra 白皮书，一石激起千层浪。很快引发各国监管层的关注，各界开始热议——Libra 是否另谋货币体系？会否冲击国际货币体系？应否纳入央行监管框架等等。

Facebook 在其最新季度报告中提醒投资者，尽管该公司预计将在 2020 年推出数字货币 Libra，但有许多因素可能使之提前夭折。Facebook 表示，自该项目于 6 月宣布以来，它认识到了来自立法者和监管机构的阻力的重要性。

以太坊带动加拿大区块链产业发展

相比于美国，以太坊的出现使得加拿大的区块链产业散发出了"青春活力"。目前，加拿大国内存在着一个庞大的区块链创业社区，汇集了包括以太坊概念提出者 Vitalik Buterin 在内的一大批区块链领域人才，此外，区块链领域的两位重要奠基者 William Mougayar 和 Don Tapscott 也均来自加拿大。与美国证券交易委员会（SEC）的无所作为不同，针对区块链创业公司和其他金融科技公司，加拿大证券管理委员会（CSA）日前主动地推出了新的 "Fintech" 沙箱计划，以促进国内区块链行业的发展。

中国中央银行发声 深圳成为数字货币试验田

2017 年 1 月，中国央行正式成立数字货币研究所，旨在研究区块链和数字货币发展。随后在 2018 年 9 月，央行数字货币研究所在深圳成立了“深圳金融科技有限公司”。根据国家知识产权局数据库，央行数字货币研究所已经申请了 71 项专利，专利主要与数字货币相关。深圳俨然已经成为数字货币发展的热土。今年 7 月 4 日，中国人民银行深圳市中心支行与国家税务总局深圳市税务局举办《战略合作框架协议》签署暨税务备案表业务上链启动仪式，此时距离央行贸金平台试运行发布正好 10 个月。目前，央行贸金平台已实现供应链应收账款多级融资、跨境融资、国际贸易账款监管、对外支付税务备案表等业务上链。其中，深圳全市 28 家银行 483 家网点税务备案业务上链运行正常，对外付汇业务量已超 300 亿人民币。

区块链技术在央行贸金平台上的应用探索，为深圳发展数字货币提供了技术支撑和经验参考。深圳在通信、互联网、区块链等方面具备较好的技术基础，对数字货币的研究能起到技术支撑的作用。“数字货币不仅仅是发币，还需要很多边缘技术的支撑，而深圳有好的技术生态环境。”数字货币的便捷性主要体现在移动支付，还有跨境支付和结算，Facebook 的数字货币 Libra 要实现的一个主要目标就是跨境支付。而深圳的移动支付普及度高，在跨境方面也具备优势，毗邻港澳，开放的程度高，尤其是前海也在试点跨境支付和结算，具有对接国际金融市场的优势。

全球区块链产业目前处于高速发展阶段，创业者和资本不断涌

入，企业数量快速增加。区块链应用加快落地，助推传统产业高质量发展，加快产业转型升级。利用区块链技术为实体经济“降成本”、“提效率”，助推传统产业规范发展。此外，区块链技术正在衍生为新业态，成为经济发展的新动能。区块链技术正在推动新一轮的商业模式变革，成为打造诚信社会体系的重要支撑。与此同时，全球区块链企业积极从产业高度定位区块链技术，政策体系和监管框架逐步发展完善。

1.1 产业生态初步形成

未来三年将是传统行业与区块链更紧密融合的时期，随着区块链开始改变市场结构，企业将会关注到商业的变革，带有智能合约技术的新生态系统会被整合到在现有行业中，新型的商业模式和监管服务模式将会涌现，社会企业数量将会大大增加。跨链技术将实现不同区块链之间，甚至区块链和传统 IT 系统之间的价值流转。结合区块链技术目前的发展速度和现有技术、市场、监管体系的成熟程度，可以预见区块链生态在三年之内将实现广泛落地，与具体产业场景深度相结合，创造出新模式，切实推动实体经济转型升级、提质增效。区块链技术在实体经济中广泛落地为实体产业“换道超车”直接实现“可信数字化”提供了机遇。利用区块链技术，结合物联网和工业互联网的进一步推广和普及，大量交易将由线下转向链上，企业的管理系统和机器设备的联网率也将显著提升，物理空间的实物资产也会被更广泛地映射到网络空间，数字资产将成为企业资产的重要组成部分，实

体产业的商业模式也将实现前所未有的深度变革，这将极大地加快全球数字化进程，为数字建设提供有力支撑。

1.2 产业链条脉络逐渐明晰

目前，全球区块链产业链条已经形成，从上游的硬件制造、平台服务、安全服务，到下游的产业技术应用服务，到保障产业发展的行业投融资、媒体、人才服务，各领域的公司已经基本完备，协同有序，共同推动产业不断前行。从区块链产业细分领域新成立公司分布状况来看，截至 2018 年 3 月底，区块链领域的行业应用类公司数量最多，其中为金融行业应用服务的公司数量达到 286 家，为实体经济应用服务公司数量达到 309 家。此外，区块链解决方案、底层平台、区块链媒体及社区领域的相关公司数量均在 140 家以上。

2 全球区块链发展趋势

全球区块链产业未来社区化将进一步加速。包括区块链技术发展带来的新的商业模式和生产关系变革；全球各国区块链监管政策的进一步细化与完善，将影响数字资产投资用户在区块链上的投资选择，有线下实体产业做支撑的区块链项目和应用场景落地的项目将被用户热爱。

随着对区块链技术认识的提高，区块链技术潜在的应用场景及应用市场不断被发掘，区块链已经不再是普通意义的技术应用，而涉及到了国家核心竞争力与国家安全。此前，IBM 区块链发展报告就指

出，全球 9 成的政府正在规划区块链投资，并将在 2018 年前进入实质投资阶段。

2.1 区块链发展前景

随着中本聪的第一批比特币被挖出来，区块链 1.0 时代也开启了，可以简单理解为区块链 1.0 时代和比特币、莱特币这些老牌数字货币为代表的时期。1.0 时代做的不多，但是把区块链带入到了现实社会中，这就足够了。

最有名的莫过于九年前，一位名叫 Laszlo Hanyecz 的程序员用 1 万枚比特币购买了两个披萨。这被广泛认为是用比特币进行的首笔交易，也是币圈经久不衰的笑话之一，很多币友将这一天称为“比特币披萨日”。但是从另一个角度来说，这次的行为将电脑中挖的那些虚拟货币与现实中的实物联系起来，这是具有里程碑意义的，因此是无价的。

在 1.0 时代，人们过多关注的只是建立在区块链技术上的那些虚拟货币，关注它们值多少钱，怎么挖，怎么买，怎么卖。不过时间久了，自然会有更多的人去关注技术本身，随后就是引发一场新的革命——区块链 2.0 时代。

区块链 2.0 时代是以以太坊、瑞波币为代表的智能合约或理解为“可编程金融”，是对金融领域的使用场景和流程进行梳理、优化的应用。

区块链 2.0 时代是智能合约开发和应用的时期。智能合约是一种可以自动化执行的简单交易。举一个简单的例子，我跟你打一个赌，

如果明天下雨，算我赢，如果明天没下雨，就是你赢了。然后我们在打赌的时候就把钱放进一个智能合约控制的账户内，第二天过去了，赌博的结果出来了以后，智能合约就可以根据收到的指令自动判断输赢，并进行转账。这个过程是高效，透明的执行过程，不需要公正等第三方介入。也就是说，有了智能合约以后，打赌就没办法赖账了。

在区块链 2.0 时代中最著名的莫过于具有智能合约功能的公共区块链平台以太坊了，也可以说是以太坊掀起了区块链 2.0 革命的浪潮。以太坊为了解决比特币的扩展性不足的问题而生，事实证明也确实如此，大量的 token 基于以太坊发行，疯狂之下，成功地将 ETH 推上了全球加密数字货币市值排行榜的第二名。但区块链的 2.0 技术只能达到每秒 70 至 80 次交易次数，这也成为其快速发展的制约性因素。于是，这就需要将眼光放到未来的 3.0 时代。

区块链 3.0 时代是区块链技术在社会领域下的应用场景实现，将区块链技术拓展到金融领域之外，为各种行业提供去中心化解决方案的“可编程社会”。

在区块链 1.0 和区块链 2.0 的时代里，区块链只是小范围影响并致富了一批人，因其局限在货币、金融的行业中。而区块链 3.0 将会赋予我们一个更大更广阔的世界。未来的区块链 3.0 可能不止一个链一个币，是生态、多链构成的网络，类似于操作系统或类似于电脑全球的一个巨大的电脑的操作系统。

所以区块链的 3.0 时代，区块链的价值将远远超越货币、支付和金融这些经济领域，它将利用其优势重塑人类社会的方方面面，从根本上改变信任机制，促进全社会向前发展。这是一场没有硝烟的革命，

那我们要做的是，加速它，迎接它，拥抱它，最后改变这个世界。

2.2 区块链技术赋能实体

区块链 1.0 时代主要是以比特币为代表的数字币阶段，更多的是起到一种分布式记账的作用；2.0 时代则是以以太坊为代表的智能合约阶段，利用去中心化的虚拟机来处理点对点的交易；而 3.0 时代则是区块链技术全面应用的时期。

区块链进入 3.0 时期，将着力赋能实体经济，应用场景非常广泛，可以深入应用到社会管理、文化娱乐、金融服务、医疗健康、IP 版权、教育、物联网、通信等各个领域。而区块链最相匹配的领域，是与共享经济的结合，可以快速启动和激活共享经济。“共享经济的前提是规模效应，没有规模就没法共享。”通过区块链技术进行共享，企业能将用户手中闲散的资源利用起来，无需投入大量资金购买资源，这就解决了企业在共享经济中资源原始积累的问题。

除此之外，区块链还可以解决共享经济中存在的公平性问题，即公平地获得资源和公平地获得回报。“在区块链应用的共享经济领域，所谓‘大数据杀熟’的情况很难存在。”“大数据杀熟”是指面对同样的产品和服务，老顾客或者购买频次较高的顾客比新顾客或购买频次较低的顾客花的钱更多。在区块链上，可以看到每一笔交易的信息和数据，企业难以利用信息的不透明性去“杀熟”，从而保障消费者

的权益。目前，中国正在由区块链 2.0 时代，迈入 3.0 时代，这无疑将更好地赋能实体经济。

2.3 区块链+大数据

在大数据上使用区块链技术，可以保证我们上链的数据是不会被篡改的。在实际的生活当中，也会降低人们之间的信任成本，因为大多数时候，我们为了相信一个人，不得不去做很多的工作，为的就是能让合作更加的高效。

假设有一个平台可以把我们过往的一些交易数据呈现出来，而且这些交易数据都是基于某种共识机制，大家都对这个机制信任，那么，这无形中就会节约很多交易成本。其次，区块链数据的不可篡改就注定了人们在数据上链之前会格外注意自己数据的真实性，因为一旦默认了自己数据造假，未来在区块链的世界里，作为个人必将也是很难生存。

因为一切数据都是透明公开的（需要验证），那么数据也就意味着无法删除、无法修改，你的数据就是在给你自己的人格品牌背书。所以，区块链和大数据的结合一定程度上会避免未来人们对数据造假所造成恶劣结果的一种忽视。随着大数据的发展，未来数据过度集中化的现象也会得到遏制，也就是像上面所说的数据孤岛、数据过度集中，数据隐私泄露等问题都会得到一定程度的改善。

3 POT 的发展契机

随着区块链 3.0 时代的到来，区块链技术将实现在社会各个领域的应用，促进行业的发展和新兴技术的发展。区块链只是一项技术，本身并不神秘。然而区块链作为一种颠覆性技术，有望打造“价值互联网”，推动整个经济体系实现技术变革、组织变革和效率变革，为构建现代化经济体系作出重要贡献，因此引起了社会各界的广泛关注。商盟的出现致力于解决传统实体商家的痛点，对实体经济发展困难带来实质性的改变，应用价值是不可预估的。

区块链嵌入实体商家联盟，打造去中心化的 POT 生态经济，从资金和技术方面支持实体经济发展，从而打破行业垄断壁垒，让更多的公众享受到技术革命带来的环境以及财富上的成果。一切商业的正常展开需以可持续发展为前提，POT 将区块链经济与商业经济深度融合，从技术、理念上支持商业经济的发展，以商业经济为基础辐射全产业链。同时，POT+区块链两个具有无限潜力的双链组合给致力于项目研发、实体商家的创业者、志愿者一个财富增值的契机，同时将驱动整个商业链的发展。

二、项目介绍

1 POT 定位

Portaldot，英文缩写 POT，以下简称 POT。POT 是由 Portaldot Foundation（POT 基金）投资研发的一条国际化的基础公有链，发起之初 POT 基金就与英国知名的区块链以及互联网科技公司达成战略合作，进行技术开发。POT 的打造很快引起了全球各行各业实体商家的关注和加盟，并自发组成了商家联盟联合会，商盟会成员都在商盟会内组织管理委员会进行自治共管服务于会员以及整个 POT 的推广。

POT 是在区块链、大数据等前沿技术与实体产业深度融合的背景下综合性解决传统实体商家经济发展困难、金融门槛高、企业资金瓶颈等一些全球经济存在的困境与人工难以解决的问题为基础，英国方面结合基金会强大的资金、资源优势，打造了贯穿全球商业生态经济产业链的区块链应用平台。

2 项目核心优势

2.1 团队优势

POT 技术团队是一支来自英国的成熟技术团队。团队大部分成员于 2015 年便已进入区块链领域，均来自于全球知名互联网巨头企业的高级开发人员，有着丰富的系统设计经验，并对以太坊及比特币等开源系统有着深入的研究，擅长多语言计算机编程，曾为国际著名金融机构和公用事业公司等提供区块链技术支持。同时，优秀的技术团队自带光芒，项目发展吸引了欧洲众多资本方的青睐，为团队的发展提供了强有力的资金支撑。

2.2 POT 解决传统商家痛点

区块链可以打通各行业之间的壁垒，所有数据在区块链上可查、可溯源、不可篡改，数据真实可靠，使各行业之间相互联通，努力在区块链上将各行业联通起来，之后我们将把我们的技术应用到更多的行业中去，在区块链上形成商家资源整合、生态产业联盟。

POT 的设计充分考虑了商家资源的合理利用以及实体经济发展困难等问题，使得传统实体商家的发展能与区块链技术有效结合。区块链技术的嵌入，不再是单纯地生态的理念，更是商业、经济的深度整合。POT 致力于解决传统实体金融门槛高、实体经济发展困难等痛点，帮助实体经济更好地发展。

2.3 实体商家的一站式服务平台

POT 打造了全新的商业模式——一站式商业联盟平台。POT 将区块链经济与实体经济深度融合，从技术、理念上支持实体商家的经济发展，为用户提供开发以区块链底层技术公链为基础的商业生态圈，为链上企业、项目提供包括顶层设计、技术支持、资源整合、线上平台等专属企业项目孵化服务，并会根据用户需求持续开发和更新。

3 POT 通证计划

为了让更多的志愿者以及实体商家能够参与到 POT 的打造中来，也为了 POT 问世前的知名度打造，商盟会成员共同商讨实行 POT 计划：打造区块链商家商城，汇集各行业实体商家的资源和优势进行整合，并结合区块链技术进行游戏、挖矿等为商城引流，让消费者能够在日常的消费中参与到 POT 的推广和未来 POT 项目实现的红利。同

时也能让商家在投资和推广中能够得到资源的整合以及可持续的发展。

POT 是 Portaldot 的原生 Token，是 Portaldot 生态内的唯一通证，总发行量 30 亿枚，永不增发。主要用于 POT 生态建设、Defi 与治理、社区激励、网络 搭建、运行和支付等用途。

(1) 预挖 9 亿枚

基金会 1 亿枚，占比 3.33%：3000 万枚用于早期融资、基金会搭建与空投；7000 万枚用于市场调度（分 4 年线性释放）；

商业融资储备 3 亿枚，占比 10%（分 4 年线性释放）；

生态扶持计划 5 亿枚，占比 16.67%：其中 1 亿枚用于金融生态打造，即理财挖矿、DEFI、NFT 等；剩余 4 亿枚分 4 年线性释放，用于生态建设、社区治理、奖励、后期融资等。

(2) NPOS 节点服务器挖矿 21 亿枚

计划 20 年挖完，每 4 年减半，出块速度 1 分钟，例如第一个 4 年每区块产 515.539843865POT，主网区块高度 2102400 左右第一次产量减半。

(3) 节点服务器质押

挖矿奖励根据总质押量和通胀率决定，奖励产生后每个验证者池根据各自的 Era Points 按比例分配。最低质押量 5000POT/台，最高质押量 30000POT/台，最高质押率 80%。具体奖励公式如下：

验证人奖励： $R_{PE_PVP} * C + R_{PE_PVP} * (1 - C) * (S_V / TS_VP)$

提名人奖励：假设为第 i 个提名人，则奖励为 $R_{PE_PVP} * (1 - C) * (S_{N_i} /$

TS_VP)

角色解释:

验证人 (Validator): 运行全节点并质押一定 token 成为验证人, 负责网络维护, 并获得一定比例的回报。

提名人 (Nominator): 无需运行全节点, 质押一定 token 给验证人并获得一定数量的回报。

验证人池: $1 \times \text{验证人} + N \times \text{提名人}$ 组成一个验证人池

验证人集: 若干个验证人池组成

参数对照:

Slot: 出块时间

Era: 若干个 slot 形成一个 era, 每个 era 结束则重新选举验证人集, 用 E_Y 表示一年有多少个 Era

Era Points: 根据验证人的出块量、对于平行链的有效性声明等叠加, 每个验证人的 Era Points 占比用 E_P 表示;

每 Era 总奖励 = 年通胀率 * 总质押量 / E_Y , 用 T_R_PE 表示;

每 Era 每个验证人池奖励 = $T_R_PE * E_P$, 下文中用 R_PE_PVP 表示;

验证人池中各个人的奖励分配: 扣去佣金后根据每个人的质押量按比例分配

佣金率: 用 C 表示;

验证人池总质押量: 用 TS_VP 表示;

验证人质押量: 用 S_V 表示;

提名人质押量: 假设有 x 个提名人, 则各个提名人的质押量可表示为 S_N_1 、 S_N_2 、...、 S_N_x 。

三、应用列举

1 跨境支付

在跨境贸易业务中，往往存在手续复杂繁琐、时效性差、软条款等方面的问题。以 **Swift** 为例，需要到柜台填资料，一般两到三个工作日到账，有时单笔交易的耗时可能也要长达数日，除手续费外还收取电报费。以中国银行为例，收取汇款金额的 $1/1000$ (最低 50 元人民币)，此外还需要收取电讯费 150 元手续费。同时交易中仍存在大量的纸质文件，不仅效率低而且存在遗失及信任风险，现在普遍采用的制度如：信用证结算、托收结算、银行保证函等也都存在各类缺陷的问题，给跨境贸易带来不便。

POT 利用区块链技术覆盖各企业数据，可以打破国际贸易局限，解决跨境支付问题。由于它具有高可靠性、简化流程、交易可追踪、节约成本、减少错误以及改善数据质量等特质，使其具备重构金融业基础架构的潜力。能够解决支付与结算的痛点，通过区块链技术，实现资金转移，在跨国收付款人之间建立直接交互，简化处理流程，实现实时结算，提高交易效率，降低业务成本，

POT 将现有商业体系的基础制度和交易规则固化在底层协议中，推动底层逻辑的标准化和自动化、高层业务应用的分布化，提高效率后，上述手续可能会被精简到数个小时以内,进而对现有商业体系的制度基础和参与者关系产生颠覆性影响。

2 社交电商

在大宗商品交易中，存在着效率低下、内幕交易、信息不安全、

商业欺诈、监管空白、仓单重复质押、信息不透明等等行为，极大地制约了大宗商品贸易的发展。

POT 商城采用分布式系统框架，系统可以完全代替传统的纸质单据，通过自动化数据匹配的方式，使文件数据处理的效率提升数倍。通过加密技术，共享买卖双方的交易信息并实时监控和记录，防止数据篡改和丢失，在保护关键信息的同时提高交易信息的透明度，使监管部门减少监管成本提高监管水平。

2.1 链哆哆电商平台



链哆哆以社交电商为依托，以区块链技术为保障，以五大体系为发展规划，以技术驱动、脱虚向实为指导思想，致力于解决中小企业的供销问题、解决实体商家的经营问题。

链哆哆电商平台是 POT 基金会投资孵化电商平台，链哆哆 1.0 已于 2020 年 7 月 1 日正式发布，平台采用区块链技术，以不同于现有传统电商平台的分布式电商思维，将电商与区块链相结合，以区块链溯源体系，通证奖励系统，直播间带货等多角度，促进平台的快速发展并取得优秀成绩：电商平台上线首月营业额即突破 100 万；注册会员 5000 人，VIP 会员突破 2300 人；入驻商家突破百家。

3 多边贸易融资

在供货商、进货商、银行等贸易融资参与主体间建立联盟链，通过区块链记录贸易主体资质、多频次交易、商品流转等信息，使贸易双方及银行间公开透明安全地共享真实可信的信息。针对供应链中的大型企业，银行可以借此丰富融资风控模型，减少线下人工采集和确认信息真实性的工作量，开展动产评估下的融资服务。有融资困难的供应链上下游中小企业，可基于区块链提供的主体资质认证、与大型企业的多频次交易信息认证获得信用背书，缓解融资难题。

4 移动通信应用

电信行业是一个典型的需要多方共同决策、上下游产业链协同合作业务极其繁杂的行业，彼此之间的信任以及沟通的效率在一定程度上影响了整个行业的服务水平。POT 的去中心化、多方共识的特点完美契合了电信行业的业务需求，并且区块链信息防篡改的特性，保证了沟通信息的真实性和准确性。除此之外，在 POT 搭建的应用平台上，用户可以将智能手机作为通讯节点，为用户提供节点奖励，奖励的代币又可以用于电信行业消费服务如话费、流量的支付，刺激代币的流通，推动 Dapp 在社区的使用和 POT 生态圈的发展。

四、技术策略

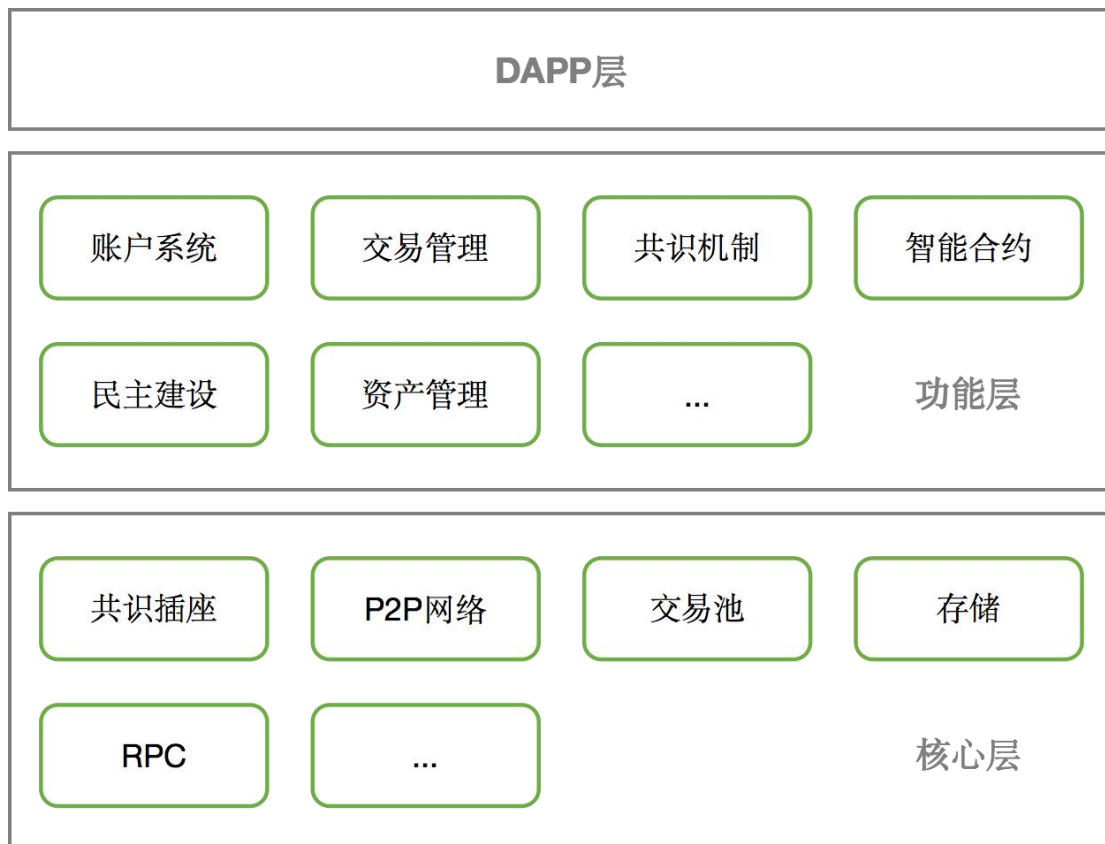
1 概述

Portaldot Network 是 Portaldot 庞大生态的基石。

Portaldot Network 作为新一代的区块链协议，它将专门构建区块链的整个网络结合在一起，以支持它们大规模、无缝隙的协同工作。

Portaldot Network 允许在任何类型的区块链之间发送任何类型的数据，因而它解锁了大量真实世界的应用场景，通过将来自多个专用区块链的最佳功能组合在一起，它为新的去中心化市场铺平道路，为各种去中心化应用程序提供更公平的服务支持。

2 架构设计总揽



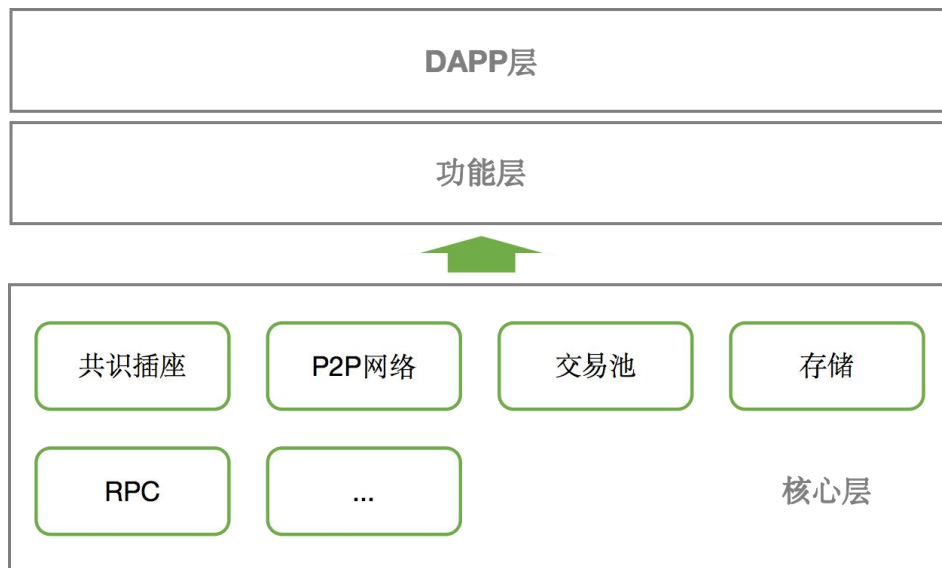
Portaldot Network 在设计时充分遵循

- 模块化
- 低耦合
- 高并发
- 安全性

的设计原则，系统整体可分为核心层、功能层、DAPP 层三大层次。

- **核心层:** 为 Portaldot Network 提供区块链网络的核心基础功能，包括共识插座、P2P 网络、交易池、存储支持、RPC 接口等。
- **功能层:** 为 Portaldot Network 定义区块链网络的业务逻辑。我们可以把功能层看作是区块链网络中的“状态转换函数”，它定义了用于表示区块链网络状态的存储项，同时也定义了允许用户对该状态进行更改的函数。
- **DAPP 层:** 基于 Portaldot Network 开发的去中心化应用生态，由于针对大量真实场景的支持，可以预见将会有包括物联网（IoT）、金融、治理、身份管理等多种应用出现在我们的生态中。

3 核心层设计



3.1 共识插座

共识机制是允许区块链网络参与者就区块链状态达成一致的一种逻辑。共识插座提供共识机制底层逻辑，为未来可能的共识升级提供支持。

3.2 P2P 网络

允许客户端与其他网络参与者进行通信的功能。Portaldot Network 使用基于 Rust 的 libp2p 库来实现此功能。

3.3 交易池

交易池包含所有在网络广播的，已被本地节点接收和验证的，所有已签名和未签名的交易。

3.3.1 有效性检查

交易池检查交易是否有效，比如：

- 检查交易索引 (nonce) 是否正确
- 检查帐户是否有足够的资金来支付相关费用
- 检查签名是否有效
- 交易池还定期检查池内现有交易的有效性，如果发现无效或过期的普通交易，该交易将被交易池删除。

3.3.2 交易排序

如果交易是有效的，交易队列会将交易分为两组：

- 就绪队列 - 包含所有可放到新的待处理区块中的交易。
- 未来队列 - 包含所有可能在未来变成有效的交易。 例如一个过高的索引(nonce)值的交易，此交易将在此队列中等待，直到之前的交易上传至区块链上。

3.3.3 交易依赖关系

ValidTransaction 结构体定义了 requires 和 provides 参数来构建交易的依赖关系。再加上 priority 参数，这个依赖设计允许交易池生成有效的交易线性顺序。

所有具签名交易都需要包含一个交易索引 (nonce)，该索引值在每次进行新的交易时都会递增 1，例如，新账户的第一笔交易将

是 $\text{nonce} = 0$ ，第二笔交易将是 $\text{nonce} = 1$ 。

交易体包括一个 `provides` 标签，其值为

$\text{Provides} = \text{Encode}(\text{sender} + \text{nonce})$

和 `requires` 标签，其值为

$\text{Requires} = \text{Encode}(\text{sender} + (\text{nonce} - 1))$ if $\text{nonce} > 1$

如果 $\text{nonce}=0$ ，则交易不需要其他信息。因此，来自单一发送人的所有交易都将形成一个顺序，并被包括其中。

3.3.4 交易优先级

`ValidTransaction` 中的 `TransactionPriority` 结构体决定了就绪队列中的交易顺序。当某个节点成为下一个区块生成者时，它将在下一个区块把交易按优先级别从高到低排序，直到达到区块的重量或长度限制。

`priority` 定义了当一个交易可解锁多个依赖交易时，所应有的线性排序。例如，如果我们有多个交易的依赖性得到满足，那么我们会使用 `priority` 来选择它们的处理顺序。例如：

1. 如果我們从不同的发送者那里收到 2 个交易，我们通过 `priority` 来确定哪个交易更为重要，并优先把它打包进区块中。
2. 如果我們从同一个发送方收到 2 个相同 `nonce` 的交易，那么只会会有一个交易会被打包到链上。

我們使用 `priority` 来选择 `fee` 较高的交易，并把它储存到交易池中。

3.3.5 交易生命周期

交易生命周期可以遵循两条路径：

- 由本地节点生成的区块：

- (1) 我们的节点会监听网络上的交易。

- (2) 每一笔交易都要经过验证，而有效的交易会被放入交易池。

交易池负责对交易进行排序，并返回可被纳入区块的交易。在就绪队列中的交易将被用来打包到区块内。

- (3) 交易会被执行，而状态变化会存在本地内存中。来自就绪队列的交易也会在网络上传播给其他节点。我们将使用准区块的排序来处理，因为排在队列前面的交易具有更高的优先级，也更有可能在下一个区块中成功被执行。

- (4) 构建好的区块会被发布到网络上。而网络上其他所有节点都会接收并执行该区块。

- (5) 交易在区块生成时不会从就绪队列中被删除，仅在区块导入时才被删除。

- 从网络接收的区块：该区块被执行后，整个区块要么成功，要么失败。

3.4 存储

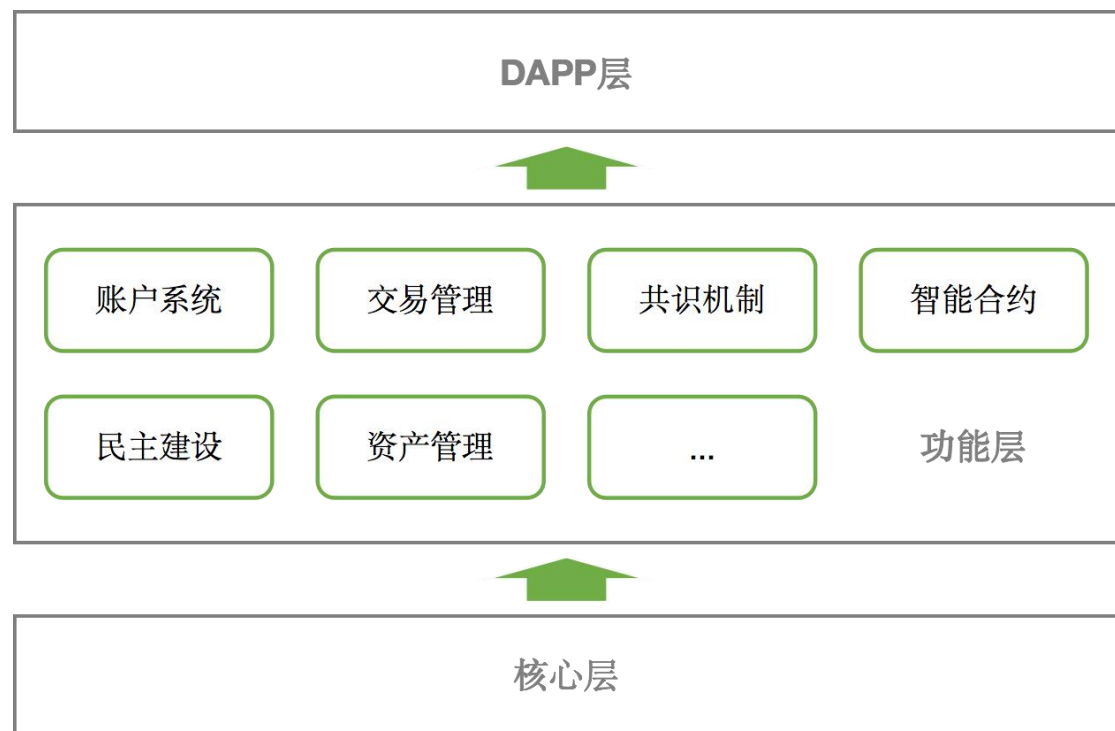
用来存储区块链网络中不断增长的状态数据。区块链网络使参与者可以就存储状态达成无需信任的共识。Portaldot Network 使用了

基于 RocksDB 的高效 key-value 存储机制。

3.5 RPC (Remote Procedure Call) 接口

允许区块链用户与网络交互的功能。Portaldot Network 提供 HTTP 和 WebSocket RPC 服务。

4 功能层设计



4.1 共识机制

4.1.1 概述

共识是一种在共享状态上达成协议的方法。为了使区块链的状态继续建立并向前进，网络中的所有节点必须达成一致共识。通过这种方式，去中心网络中的节点可以保持彼此同步。在区块链上如果去中心化网络节点没有共识，就无法确保由其他节点共享的状态是真实的。共识旨在参与者之间提供状态的客观事实，每个参与者对网络都有自己的主观观点。这些节点间进行通信的过程并达成协议使能够构建新区块。

4.1.2 概念定义

Slot: 槽，代表区块生成时间。

Epoch: 时期，固定长度的 Slot 集合，每个时期内区块生产相关的随机性参数将重新定义。

Era: 时代，固定长度的 Epoch 集合，每个时代结束都将重新选举验证者。

VRF: 可验证随机函数，根据私钥生成，任何人可以通过公钥来证明。

4.1.3 角色

●**验证人(Validator):** 每个 Era 结束后，系统会选择出一个验证人集，他们在接下来的 Era 内，将在高度敏感的协议中扮演关键角色，比如区块的生产和最终验证。他们的工作要求很高，因为他们需要运行成本高昂的操作，确保高通信响应能力，并建立长期的可靠性声誉。他们还必须将自己的 Token 进行质押作为良好行为的保证，当他们偏离协议时，这个质押就会被惩罚掉。相反，当他们按规则行事时，他们会得到奖励。任何完成任务的节点都可以公开地成为候选的验证节点。但是，由于操作上的原因，最终只能选择有限的验证人。

●**提名人(Nominator):** 提名人公布了一份他信任的候选人名单，并把一定数量的 Token 进行质押来支持他们。如果这些候选人中的一些人被选为验证人，他将根据根据质押的数量占比来得到相应的利益回报。与验证人不同的是，提名人没有数量的限制。只要提名人去选择，

并且只支持具有良好安全实践的候选验证人，那他的风险就很低，并且有持续的收入来源。

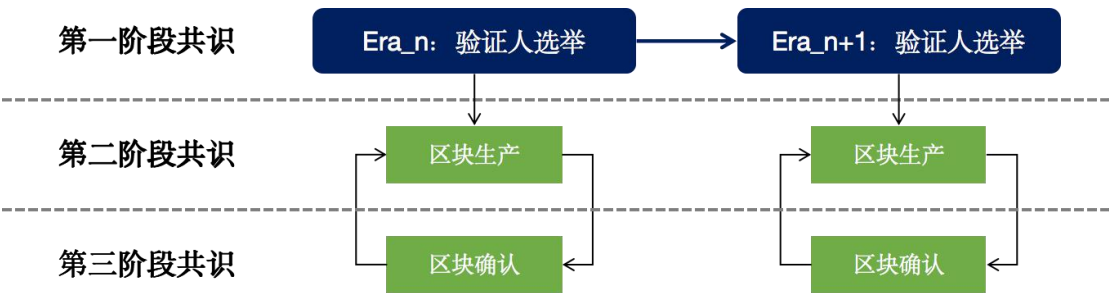
4.1.4 Portaldot Network 的共识机制

在 Portaldot Network 中，我们使用的并非传统的单一型共识，而是混合型共识，完整的共识工作过程分为三个阶段：

第一阶段：选举验证人集；

第二阶段：验证人生产区块；

第三阶段：验证人进行区块确认，形成整个系统的最终确定性。



4.1.5 基于 NPoS 的验证人选举

Portaldot Network 的验证人集是一个有限大小的集合，数量可以为数百或数千，这个数字最终将由治理决定，但它将独立于网络中的用户数量，从而确保可扩展性。与其他基于 PoS 的根据验证人的质押数量来衡量投票比重的项目不同，Portaldot Network 在共识协议中给被选出的验证人同等的投票权，同时系统允许无限数量的提名人参与，他们通过投入更多价值来帮助维持整个系统高水平的安全性。

根据参与者的偏好，在每个 Era 开始时选出一组新的验证人为这

个 Era 服务。每个人都可以选择成为验证人候选人或提名人，每个候选人都设定他意向的质押投入及佣金。反过来，每个提名人都会发布一份包含她信任的候选人名单并进行质押。一个验证人与所有支持他的提名人将组成一个验证人池，并且质押数与投票数对等，对于某个验证人池我们定义

$PoolStake_n$ 代表下标为n的验证人池得到的所有投票数

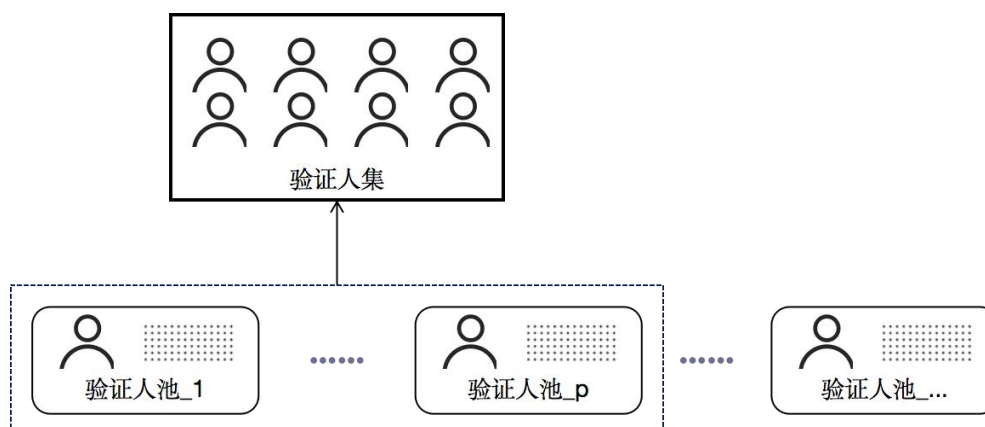
v_n 代表验证人池对应的验证人的自我投票数

$\sum_{k=1}^j n_k$ 代表验证人池中所有提名者的投票总和

则每个验证人池得到的总投票数为：

$$PoolStake_n = v_n + \sum_{k=1}^j n_k$$

假设验证人集大小设定为 p ，我们把这些信息将输入到选举协议中以选出支持最多的 p 个候选人作为这个 Era 的验证人。



提名人与他们提名的验证人分享奖励或惩罚。因此，在生态中提名者在被视作一种监督者，他们将根据验证者的质押水平、佣金、过去的表现和安全实践等参数来确定是否进行支持。系统允许选出拥有大量总股份的验证者，从而有助于将验证者选举过程变成公平性选举

而非独裁型统治。我们认定在任何时刻系统中都存在一定量的质押，这使得任何组织干扰选举过程都将非常困难，因为它需要大量的质押或足够高的声誉来获得提名人的支持，这种攻击的成本昂贵，而且可能会失去他所有的质押和声誉。

4.1.6 基于 VRF 的区块生产

Portaldot Network 使用基于 Slot 的区块生成机制，并使用 VRF PRNG 随机执行插槽分配。在每个 Slot 上，所有授权机构都会使用 VRF 函数生成一个新的随机数，如果该随机数小于给定的阈值（与它们的权重/质押成正比），则它们有权产生一个块。VRF 函数产生的证明将由其他对等节点用来验证区块声明的合法性。

该引擎还负责收集链上的熵，该熵将用于指定 VRF PRNG 的种子。在一个 Epoch 内，我们将使用相同的验证者集，因区块生成而产生的所有 VRF 输出将被收集在链上随机池中。提前一个 Epoch 宣布 Epoch 参数，即在编号 N 的 Epoch 结束时，链上宣布 N + 2 的 Epoch 参数（随机数，权重等）。

由于 Slot 分配是随机的，因此有可能将一个 Slot 分配给多个验证者，在这种情况下，我们将拥有一个临时分叉，也有可能一个 Slot 并没有分配给任何验证器，在这种情况下，不会产生任何块。这种情况下出块时间不确定。我们设定一个参数

$$c(0 \leq c \leq 1)$$

则一个 Slot 中验证人为空的概率为

$$1 - c$$

因而该参数的选择会影响与最大可容忍网络延迟有关的协议的安全性。

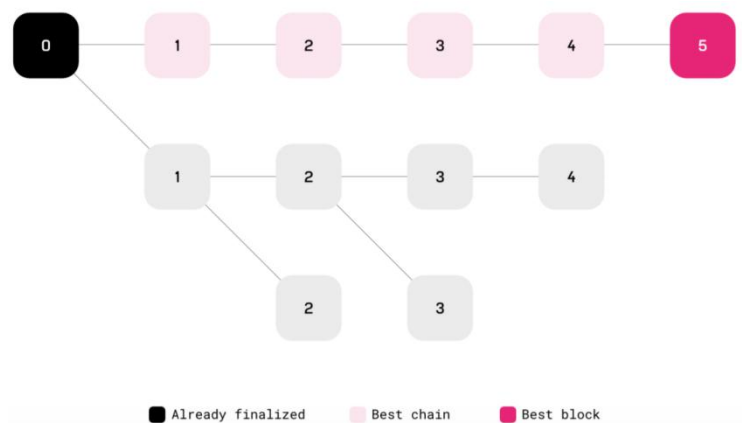
除了上述基于 VRF 的 Slot 分配（我们将其称为主 Slot）之外，本机制还支持确定性的辅助 Slot 分配。当运行验证者节点时，主 Slot 优先级大于辅助 Slot，验证者节点首先尝试声明主 Slot，然后回退并尝试声明辅助 Slot。辅助 Slot 分配是通过在索引处选择权限来完成的：

$$\text{blake2}_{256}(\text{randomness}_{\text{epoch}} + \text{number}_{\text{slot}}) \bmod \text{len}_{\text{authority}}$$

辅助 Slot 支持 SecondaryPlain 或 SecondaryVRF 变体，与 SecondaryPlain 变体相比，SecondaryVRF 变体生成附加的 VRF 输出。

4.1.7 基于 BFT 的区块确认

在 Portaldot Network 中只要 2/3 的节点是诚实的，并且可以在异步设置中处理 1/5 的拜占庭节点，它就可以作为同步的网络模型中的一部分运行，最终确定性证明系统使用最长链规则进行投票。



与其他区块链系统相比而言，一个明显的区别是，即使在长期的网络分区或其他网络故障之后，GRANDPA 还是在链上达成协议，而不是在区块上达成协议，从而大大加快了最终性确定的过程。换句话说，一旦超过 2/3 的验证者证明包含某个块的链，则导致该块的所有块都会立即完成。

4.2 智能合约

Portaldot Network 提供了部署和执行基于 WebAssembly 的智能合约的功能。

4.2.1 智能合约语言 ink!

ink! 是一个基于 Rust 的 eDSL，专用于编写区块链网络中 Wasm 智能合约的语言，它的设计宗旨是正确性、简洁性、和高效性。

4.2.1 智能合约开发

传统的智能合约平台允许用户在核心区块链逻辑之上发布额外的逻辑。由于任何人（包括恶意参与者和缺乏经验的开发者）都可以发布智能合约逻辑，这些公共智能合约平台上内建了许多刻意设计的安全防护手段。以下是一些例子：

- **Fees:** 确保合约开发者因执行智能合约而被占用的计算和存储资源付费，这样出块节点的资源就不会被他们滥用。

- 沙箱：一个合约无法直接修改核心区块链存储或其他合约的存储。它的作用是限制合约只能修改自己所拥有的状态，且只能向其它合约或状态函数发起外部调用。
- 状态租赁：合约会因为占用了区块链的空间而需要为其付费。这确保人们不会从“免费、无限的存储”中获利。
- 回滚：合约可能有导致逻辑错误的情况。我们对合约开发者开发能力的期望很低，因此我们增加了额外的开销，以支持在交易失败时回滚整个交易。这样，在出错时不会更改任何状态。

这些不同的开销使得智能合约运行得更慢、更昂贵，但是合约开发的“目标受众”与状态开发者的不同。合约可以让你的社区在你的状态逻辑上扩展和开发，无需处理各种令人发疯的提案、状态升级等等。它甚至可以作为未来的状态变更的测试基础，将你的网络隔离于日后可能发生因成长产生的痛楚或错误。总而言之，Portaldot Network 智能合约：

- 对网络来说是天生安全的。
- 通过经济激励来防止滥用。
- 通过额外的计算开销来支持错误处理。
- 开发门槛更低。
- 通过试验场使得社区快速互动以创建新的逻辑。

4.3 账户体系

Portaldot Network 使用多组公钥/私钥对来表示网络的参与者。密钥对代表一个账户，并可以控制资金，类似于其他区块链中的普通账户，根据参与者的不同角色，账户密钥可分化出 Stash 密钥、Controller 密钥和会话密钥三个不同抽象：

4.3.1 Stash 密钥

Stash 密钥是定义 Stash 账户的公私钥对。这个账户就像一个“储蓄账户”，你不应该用它进行频繁的交易。因此，应以最安全的方式来处理其私钥，例如在安全层或用安全硬件来加以保护。

由于 Stash 密钥以离线方式进行保存，它指定了一个 Controller 账户来根据 Stash 账户资金的权重来做出与支付无关的决定。它还可以指定一个代理账户来代表它在治理中进行投票。

4.3.2 Controller 密钥

Controller 密钥是定义 Controller 账户的公私钥对。在 NPOS 模型中，Controller 密钥会代表某个账户进行验证或提名。

Controller 密钥被用于支付偏好设置，例如提名奖励的目的地址，如果是验证人，可用它设置会话密钥。Controller 账户只需要支付交易费用，所以它只需要最少量的资金。

Controller 密钥不能用来从 Stash 账户中支出资金。然而，Controller 账户的行为可能会导致惩罚，因此仍应妥善保管。

4.3.3 会话密钥

会话密钥是验证者用来签署和共识相关消息的"热密钥"。不应该将它们作为控制资金的账户密钥，应只应用于其指定用途。它们可以定期更改；更改的方式是，你的 **Controller** 账户只需通过对会话公钥进行签名创建一个证书，并通过外部交易的形式广播该证书就可以了。

为创建会话密钥，验证人的操作者必须证明其拥有一个密钥能够代表其 **Stash** 帐户(质押)和提名人。为此，他们使用自己的 **Controller** 密钥对该密钥签名，从而创建证书。然后，他们在链上发布一笔包含该会话证书的交易，来告知区块链该会话密钥代表了他们的 **Controller** 密钥。

4.4 资产管理

一般而言，资产系统提供具有固定供应量的可替代资产管理功能，包括资产发行、资产转账、资产冻结、资产销毁等。**Portaldot Network** 中的资产系统旨在实现以下目的：

- 以经过许可的方式发行新的可替代资产类资产，并支付一定数量保证金。
- 允许帐户持有这些资产，而无需存在链上的其他任何东西。
- 在帐户之间移动资产。
- 更新资产的总供给。

- 允许具有特殊特权的帐户进行管理活动，包括冻结帐户余额和铸造/销毁资产。

5 优势

5.1 无分叉升级

如今，我们已经习惯了应用程序的频繁更新。开发人员在设计错误导致问题之前修复它们，并且随着更好的解决方案添加新功能。与所有应用程序一样，区块链需要支持升级才能与时俱进。然而，升级区块链要比升级普通应用程序困难得多，升级传统区块链将导致分叉网络，而有争议的硬分叉还可能会分裂一个社区。

Portaldot Network 彻底改变了这一过程，使区块链能够在无需分叉链的情况下进行升级，这是通过透明的链上治理实现的。有了这个特性，Portaldot Network 使项目能够保持敏捷，适应并随着技术的发展而发展。它还大大降低了有争议的硬分叉带来的相关风险，对许多组织来说，硬分叉是很严重的事情。

5.2 高度可扩展

一条区块链不足以支持去中心化应用的繁华未来，早期区块链有限的吞吐量和缺乏专门的功能层使得它们在许多实际场景中无法扩展。

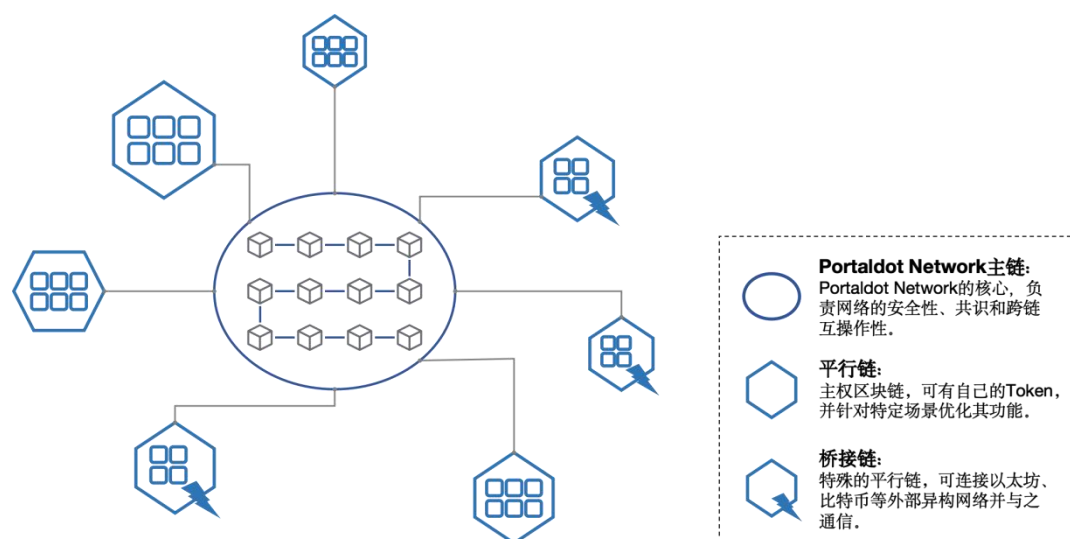
通过将多个专用链桥接到一个分片网络中，Portaldot Network 允许并行处理多个交易。此系统消除了以前逐个处理交易的网络出现

的瓶颈。Portaldot Network 将能够在未来通过嵌套中继链进一步扩展，这将增加可以添加到网络中的分片数量。

5.3 异构多链

Portaldot Network 将异构区块链分片组成的网络称为平行链。这些链连接到 Portaldot Network 主链并由其提供安全，它们还可以通过桥与外部网络连接。这意味着它将多个链连接在一个网络中，允许它们并行处理交易，并在链之间交换数据，同时提供安全保障。

由于 Portaldot Network 独特的异构分片模型，网络中的每个链可以针对特定的场景进行优化，而不是被迫适应一刀切的模型。



五、基金会

1 基金会介绍

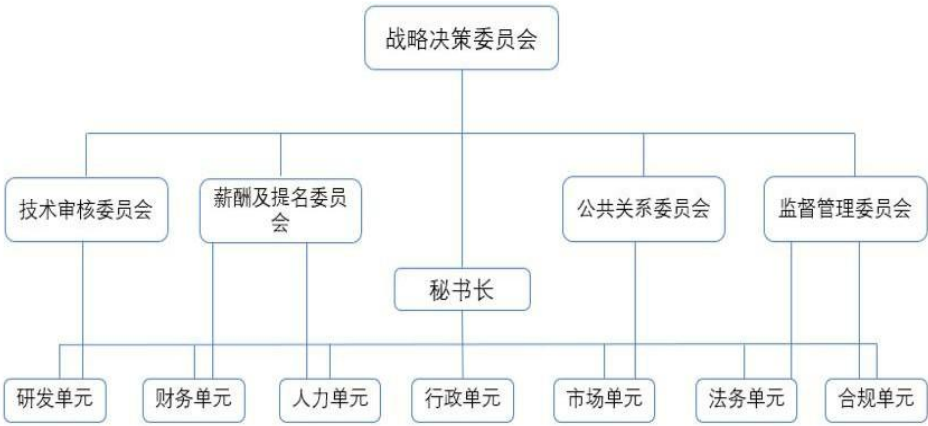
POT 基金会（以下简称“基金会”）是在英国成立的非营利性实

体。POT 基金会将作为 POT 的倡导实体，致力于 POT 的开发建设和治理透明度倡导及推进工作， 促进开源生态社区的安全、和谐发展。POT 团队委托具有公信力的第三方机构，协助团队在英国设立实体，并代为维护实体架构的日常运营与报告事务。而随着志愿加入 POT 共建 POT 的成员不断涌现，商业联盟联合会成员的不断发展壮大，基金会遴选适当的商盟会参与成员加入基金会职能委员会，共同参与实际的管理与决策。成员从商盟会中产生，在职能上受基金会监管。

基金会根据项目开发的可持续性、战略制定的有效性、管理有效性、风险管控及项目的高效运营。基金会在治理结构方面坚持五大原则：中心化治理与分布式架构的融合；职能委员会与职能单元共存；风险导向的治理原则；技术与商业并存；透明与监督的原则。

2 组织委员单位

POT 基金会组织结构提出专业组织委员会与职能部门相结合的方式，对日常工作和特殊事项予以应对。以下详细介绍基金会各职能委员会以及主要职能部门的职责。基金会的设立参考传统实体的运营，将设立各项职能委员会，包括战略决策委员会、技术审核委员会、薪酬及提名委员会及公共关系委员会等组成。基金会组织架构包括（如下图）：



六、合作伙伴



哈希资本是一家全球领先的国际化风险投资及资产管理机构。业务涵盖风险投资，咨询研究以及资产管理。哈希资本关注科技领域的每一步创新及其所带来的商业变革。投资领域包括人工智能，大数据，区块链等前沿科技。



GSC 致力于为零售客户及金融机构提供广泛的金融衍生产品交易服务，主要包括外汇，金属，能源，股指，股票，农产品等 CFD 产品。致力以优质的客户服务，领先的平台技术，极具竞争力的交易条件，满足环球投资者的不同需要。



Portaldot Club 即 Portaldot 国际俱乐部，是由参与 Portaldot 网络的各方自主组成的治理社区集合，包括各大社区、生态方、开发者、节点、矿工组织、基金方等。Portaldot Club 是 Portaldot Network 的重要合作伙伴，在 Portaldot 布道、生态节点搭建、社区治理和持续性发展方面起到重要作用。

七、发展历程

2018 年 8 月，核心团队提出 Portaldot Network 及技术路线

2019 年 1 月，Portaldot 基金会成立并召开极客研讨会议

2019 年 5 月，Portaldot 团队加入顶级底层架构师

2019 年 9 月，Portaldot 基金会与多国区块链技术团队达成合作

2019 年 11 月，Portaldot 基金会得到欧洲某财团资金支持

2020 年 10 月，Portaldot 基金会支持社交电商生态建设完成

2020 年 12 月，Portaldot 资产管理系统上线

2021 年 1 月，Portaldot 国际俱乐部成立

2021 年 4 月，Portaldot POA 测试网上线

2021 年 5 月，Portaldot POS 测试网上线

2021 年 6 月，Portaldot Network 1.0 上线

2021 年 7 月，Portaldot 生态计划

2022 年 6 月，Portaldot Network 2.0 上线

2022 年 7 月，Portaldot 大航海计划

八、风险提示

政策性风险：目前各个国家对于区块链项目以及各个板块的监管政策尚不同，存在一定的因政策原因而造成参与者损失的可能性；市场风险中，若数字资产市场整体价值被高估，那么投资风险将加大，参与者可能会期望互换项目的增长过高，但这些高期望可能无法实现。

团队内风险：POT 汇聚了一支活力与实力兼备的人才队伍，吸引到了区块链领域的资深从业者、具有丰富经验的技术开发人员等。在今后的发展中，不排除有核心人员离开、团队内部发生冲突而导致项目整体受到负面影响的可能性。

团队间风险：当前区块链技术领域团队、项目众多，竞争十分激烈，存在较强的市场竞争和项目运营压力。项目是否能在诸多优秀项目中突围，受到广泛认可，既与自身团队能力、愿景规划等方面挂钩，也受到市场上诸多竞争者乃至寡头的影响，其间存在面临恶性竞争的可能。

项目技术风险：首先，本项目基于密码学算法所构建，密码学的迅速发展也势必带来潜在的被破解风险；其次，区块链、分布式账本、去中心化、不同意篡改等技术支撑着核心业务发展，生态公链团队不能完全保证技术的落地；再次项目更新调整过程中，可能会发现有漏洞存在，可通过发布补丁的方式进行弥补，但不能保证漏洞所致影响的程度。

安全风险：在安全性方面，单个支持者的金额很小，但总人数众多，这也为项目的安全保障提出了高要求。电子代币具有匿名性、难

以追溯性等特点，易被犯罪分子所利用，或受到黑客攻击，或可能涉及到非法资产转移等犯罪行为。

九、免责声明

本文档仅作为传达信息之用，文档内容仅供参考，不构成在 POT 及其相关公司中出售股票或证券的任何投资买卖建议、教唆或邀约。此类邀约必须通过机密备忘录的形式进行，且须符合相关的证券法律和其他法律。本文档内容不得被解释为强迫参与互换。任何与本白皮书相关的行为均不得视为参与互换，包括要求获取本白皮书的副本或向他人分享本白皮书。参与互换则代表参与者已达到年龄标准，具备完整的民事行为能力，与 POT 签订的合同是真实有效的。所有参与者均为自愿签订合同，并在签订合同之前对 POT 进行了清晰必要的了解。POT 团队将不断进行合理尝试，确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新，包括但不限于平台机制、代币及其机制、代币分配情况。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。请参与者务必及时获取最新版白皮书，并根据更新内容及时调整自己的决策。