享云链
LinkChain

打造全球第一商用公链

白皮书

www.lianxiangcloud.com

目录

摘要

享云链旨在为共享计算、高隐私要求的自由交易场景提供一个高性能的、安全的区块链基础设施。

为满足这一定位，享云链设计了高性能、强一致性的共识机制，引入能够隐藏交易双方地址和金额的隐私保护机制；为保证链上商业和金融的广泛应用场景具备现实可行性，享云链从区块链账户层面引入信用评分机制、多资产账户模型等创新设计，使得链上链下之间的信任传递成为可能。

链克作为享云链的原生数字通证，除作为自由交易场景的媒介，还承载了规模庞大、前景广阔的共享计算生态。为实现取代以亚马逊云为代表的传统云计算服务的愿景，链克会通过享云链继续作为激励广大用户分享闲置网络资源、存储资源的工作量证明而存在；同时，项目方会将共享计算生态的商业价值持续投入链克体系，构建可持续生态。

1.背景

2008 年比特币项目的出现，在十余年的发展过程中，区块链技术逐渐引起了科研工作者、开发者、企业和政府机构的广泛关注。区块链技术由于具备天然的去中心化、不可篡改、抗抵赖等特性，已经成为了一个人们一直在追寻的可信协议，并且在分布式计算和各类云服务领域有着天然优势。

2018 年 8 月，腾讯云服务器丢失初创公司清博数控数年数据。2019 年 4 月，网络安全公司 UpGuard 的研究人员在亚马逊云云计算服务器上可公开访问的地方发现上亿 Facebook 用户的个人信息记录 (存于亚马逊数据库中)。

另一方面，互联网发展至今，用户数据到底属于谁这个问题一直把用户本身排除在外。腾讯系与头条新产品，在微信 /QQ 昵称、头像等用户数据的适用范围上的争执；网络游戏更换服务商时用户数据是归属于运营商还是开发商的争议等等，提供中心化服务的企业从未意识到这些数据理应属于用户。正由于中心化服务，用户无法真正拥有自己的数据，用户数据成为中心化服务提供商手里的一笔巨大财富，而用户却无法从中分得任何利益。

5G 时代已渐行渐近，人类社会与互联网的紧密度还将被更大限度的深化。未来几年内全球每天所产生的数据量和对算力的需求量都将会呈指数级的爆发式增长。企业存储数据的成本与对安全的要求越来越高，数据安全与隐私问题备受公众关注，集中式处理模型越来越不能适应人们的需求。但传统云计算商业模式对于云服务速度受限、设备成本高、学习成本高、故障容错低、可辐射的企业规模受限，以及数据安全与隐私皆受到挑战等问题，无法给出有效的解决方案，其运作模式已经跟不上时代的发展，问题日益凸显。

这些问题并非不可解决，但背后都代表着巨大的成本投入，4G 时代的成本问题已经十分突出，而在 5G 时代这一矛盾还将以几何倍数放大。雪上加霜的是，摩尔定律的失效导致社会计算成本无法相应降低，导致传统的云服务模式乃至互联网商业逻辑面对着越来越高的成本、越来越难以保障的稳定性、越来越严苛的安全环境，一筹莫展。

我们认为，区块链技术将为互联网乃至整个世界构造一个崭新的未来。在这个未来的世界中，数据不再被中心化节点垄断，隐私保护将从最底层的逻辑得到保障，从根本上避免中心化节点滥用数据，并把用户数据的所有权还给用户。而共享计算将有效解决摩尔定律失效所带来的成本问题，显著降低全社会的计算成本，推动商业模式质变，加速新时代的到来。

区块链与共享计算的结合为互联网行业带来了生机，区块链所具有的系统自治性、数据可追溯确权、信息不可篡改等核心优势刚好弥补了纯分布式计算的缺陷，二者的结合对传统集中式云服务行业的痛点一击即中。这将让人们从信息互联网进入到价值互联网时代，为人类带来去中介化的全新的社会组织架构和商业模式，从而改变我们现有的生活方式。区块链可以有效地解决中心化模式中存在数据作假空间、高度依赖单一组织等痛点，从而构建一个去中心的自治生态。

然而现有区块链技术仍然存在一系列的问题，阻碍了区块链技术的广泛应用。这些问题包括性能问题、隐私保护、链下到链上的信任问题等等。已经存在一些区块链项目在致力于解决其中的一些问题，例如以太坊尝试通过分片技术使区块链具有可扩展性，得到性能提升；zcash、MONERO 等项目在探索链上交易的隐私保护方案。

但事实上，仅有部分问题得到解决，并不能完全支持区块链技术在更广泛的商业场景下孕育成功应用。人们期望出现一个更完整的解决方案。

2.目标

为构建一个计算与数据都高度去中心化的、低成本的、充分保护隐私的、可信任的互联网世界的未来，享云链作为区块链基础设施，需要具备以下特性：

隐私保护

资产的隐私保护不仅有利于保障个人安全，也是自由市场能有效运作的必要条件。因此链上交易双方需要能够隐藏账户地址和交易金额，并且保证交易数据无关联性和不可追溯性。

多种资产的交互和流转

在大面积的商业和金融服务中，存在多种不同资产的交易，要求链上能够提供资产高速流转、可以快速引入新资产并能与现有资产无缝交易，并且在需要隐私保护的前提下，实现高吞吐量的高效资产交易。

高性能

典型的商业和金融场景拥有数量庞大的用户群体和频繁的交易请求，一个能够以低时延、高吞吐的处理大量请求的技术平台是至关重要的。

低成本

通过共享计算生态构造一种广泛分布的可持续化的资源共享模式，以 Token 奖励用户的方式提供低成本、去中心化的计算资源，服务于至少 90% 的互联网产品，构成能够取代诸如亚马逊云、Google Cloud 等传统云服务商的商业生态。

链下到链上的信任传递

商业实体通过链下的优质的商品或服务积累的信誉，需要能在链上得到延续；在链下的金融场景中，涉及大量的基于信用评分的服务场景，需要在链上有对应的基础设施支持。

长期信用体系建设

健康、积极、公平的竞争环境可以使人类社会得以发展并繁荣昌盛。享云链致力于在自治生态中建立一个公平竞争环境，尽可能地减少各种虚假信息和恶意行为带来的噪声。为此，在享云链生态中，另一个价值尺度——信任值，会在社区的发展过程中逐渐加入、完善。通过信任值体系，享云链将为其上的所有数据、信息、用户行为赋予一个可靠的、有重大参考意义的值，解决海量互联网信息的可信度难以验证、互联网用户之间难以信任的问题，从而极大降低社会事务运行成本。

在本白皮书中，我们将介绍享云链的关键技术方案：
在第 5 章，我们将介绍共识机制。
在第 6 章，我们将介绍享云链的账户模型和资产管理模型，展示了享云链多资产管理的能力。
在第 7 章，我们将介绍隐私保护方案，展示享云链和链克在高速、灵活的匿名交易领域的技术优势。
在第 8 章，我们将介绍智能合约的双虚拟机方案，以支持多种智能合约编程语言。
在第 9 章，我们将详细介绍节点选举与社区治理机制。
在第 11 章，我们将介绍享云链长期建设的愿景。

3.Token-链克

链克 LinkToken，是少有的由中国企业在全球发行的应用通证（utility token）。发行已近 2 年，始终屹立不倒、稳定发展。而以链克 LinkToken 为奖励的玩客云是中国最畅销的智能硬件产品之一，发售时在市场上供不应求，曾一度出现 5-10 倍溢价购机的情况，受到超过 3500 万个用户的喜爱和认可。

自 2017 年 10 月上线以来，链克作为工作量证明，对分享闲置带宽资源和存储资源的用户进行激励的模式，为共享计算的生态积累了大量的用户。目前已经有超过 150 万台智能硬件参与到这一模式中，构成了一个 30T 带宽、1500PB 存储空间，服务于数十家互联网企业的强健生态。

社会价值高速增长正相关的链克商业生态

2015 年共享计算刚起步的时候，单台设备的上行带宽是 2M；2017 年玩客云发布的时候单台上行带宽是 15M。进入 2019 年这一数字增长到了 25-30M，这意味着单台设备可以产生的价值，也就是单位链克所代表的价值，在 3-4 年里提升了 20 倍。而 5G 时代带宽将突破 100M，甚至进入 1000M 时代，单台设备产生的价值还会持续翻倍。与之相匹配的，基于链克的共享计算为全社会节约的闲置资源规模也是成比例扩大的。这种低成本的优质资源，还将通过参与其中的企业孕育出更大规模的商业价值。

5G 时代除了玩客云外，还会有大量的创新硬件设备加入由链克构建的共享计算生态。2019 年在 CES 上，接驳闲置手机的玩客云 mini 获得了 CES 官方 Two Picks 大奖，而智能电视、盒子、音箱等长期在线设备都会逐步被纳入链克生态。由此可见链克用户将是边缘计算最大规模的应用者和受益者。

链克迁移到享云链后，将保持 15 亿总量不变，同时继续承担共享计算生态下工作量证明的功能，在资源共享、节省能源、降低全社会成本等方面继续发挥价值。而在享云链的社区自治体系的构建中，链克还会作为开发者奖励、出块节点奖励、管理机构成员奖励、投票资格等等，从多层面支持生态建设与社区自治。

背靠千亿美元规模云计算市场的链克价值体系

2018 年全球云计算产业规模为 2720 亿美元，权威机构预测在 2023 年这一数字将增长到 6233 亿美元。云计算毫无疑问是未来数年间增速最快的领域之一，而链克与共享计算生态的价值，也将在这一领域得到最大程度的放大。

我们认为，共享计算的本质就是互联网运行成本极大降低、数据隐私充分保障、数据的可靠性一眼可辩。这一切均将通过链克构造的共享计算生态来最终实现。基于这一理念，链克经过两年实践，积累了大量的用户和商业场景，并获得了众多一流互联网企业的支持。通过实践证明，共享计算将是传统云计算模式在面对诸多问题无计可施时，眼前可选择的最优解。

在未来，基于链克的共享计算生态，在商业变现方面会通过云存储、边缘计算、网络加速、内容分发等各类服务实现业务模式的立体化，在更为广阔的落地场景施展拳脚，进而实现取代传统云服务的愿景。届时，无论是计算能力、存储空间、隐私保护，还是其他功能，均将可以通过由链克构建的服务体系来实现，将共享计算的红利分享给各行各业。最终，也将源自各个产业的商业价值，回流进链克体系。

作为中国知名度最高的 Token，我们相信在链克转入享云链后，这一生态将得到更大规模的发展，释放前所未有的巨大能量。

链克当前应用生态

1. 线上兑换平台

项目方设立的链克商城已经有近 400 家企业商户入驻，商品覆盖涵盖日用百货、餐厨用品、手机数码、家用电器、教育阅读、视频会员等十余个品类，可兑换商品种类近 2000 种，且商户与商品仍在持续的拓展中，即便有源源不断的商户申请入驻，但链克商城将保持严格的审核制度，致力于为链克用户提供更多更好的可兑换商品，以保障用户的最佳体验。

另一方面，线上兑换平台 / 活动，也是共享计算生态中，享受到低成本红利的企业，将商业价值重新投入到链克体系，让整个共享计算生态健壮成长的渠道。

2. 新零售项目

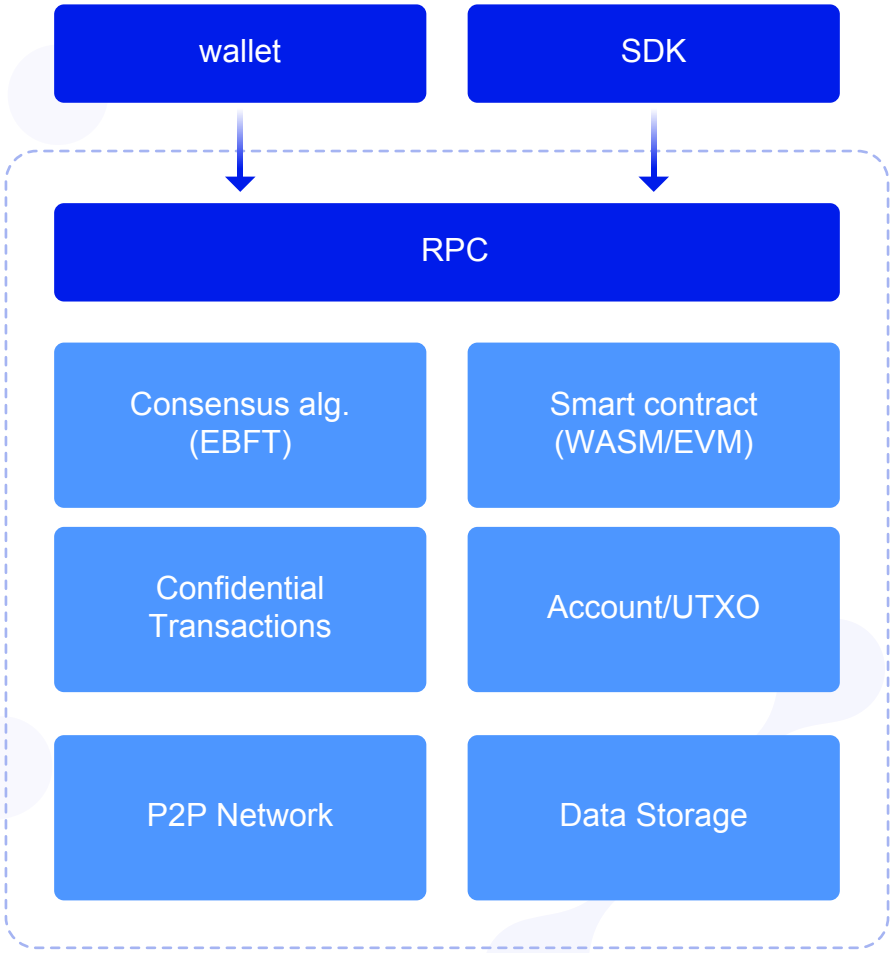
基于享云链运行的超有惠项目中，用户消费获得超积分后，可用超积分直接抵扣货款，是一项具备刚性兑付特征的通兑积分服务。超积分的转账会收取 10% 的链克作为手续费，增强了链克的需求量。目前超有惠的商业模式和产品功能已得到验证，加盟门店数超过 600 家，还将在全中国范围内不断扩大 B 端与 C 端用户群体。

3. 其他应用

目前已经有包括宠物养成、棋牌在内的多款游戏，以及云服务管理软件运转在享云链上，未来项目方也将大力发展各类链上应用。

回望过去，链克的知名度享誉中国乃至全世界，正是链克的可用性与稀缺性奠定了享云链生态的基础；展望未来，链克将会在生态中承担更多的角色，而这个自治的共建生态也将为链克赋予更大的价值。

4.技术架构



享云链技术架构图

享云链包含钱包应用、Dapps SDK、RPC 接口层、智能合约、隐私保护、共识算法、P2P 网络、账户和资产管理、数据存储等模块。

5.EBFT共识机制

享云链设计了一种周期性地自动更换验证人节点的拜占庭共识算法，实现了高吞吐、低延迟及强一致性的共识机制，我们称这个算法为 EBFT(Elective BFT) 算法。其中的 E(Elective) 表示验证人节点的上任是通过定期竞选实现的，并且验证人节点在任期的表现会影响其下次竞选的结果。

验证人节点的准入条件

在 EBFT 共识机制中，能够参与共识算法的节点被称为验证人节点，所有符合准入条件的节点将组成一个验证人节点池，共识算法将在节点池中按周期选择验证人节点。一个节点要进入验证人节点池，需要同时满足以下几个条件：

1. 提供符合一定标准的 IT 资源（满足服务器、带宽、安全规范、运维等条件）；
2. 提交一定数量的链克作为押金，为获取更高的出块概率，可提供超额押金；
3. 需要进行公开选举，排名靠前的节点才可以进入验证人节点池，并获得参与共识的机会。

享云链根据上述的准入条件构建节点池，这个节点池的节点数量原则上没有限制，规模可以非常庞大。但由于共识效率、单一节点的收益和节点数量三者之间并不是一个正相关关系，项目方将会依据享云链的发展情况对节点数量进行调整。节点池在初期将先以 15-35 个节点的规模运转。

验证人节点更换

享云链定期（通常为 1321 个区块）自动运行一次验证人竞选算法，从节点池选取一定数量的节点（通常为 22 个节点）替换掉当前在任的节点作为本轮的验证人节点。竞选算法按节点服务质量、押金数额和随机因素这 3 个条件进行综合评估，以保证具有以下特性：

1. 屏蔽掉恶意节点；降低不稳定的节点（例如经常超时不出块的节点）被选中的概率。
2. 诚实节点中，押金数额越高的节点被选中作为验证人节点的概率越大。
3. 随机因素保证押金数额较低的诚实节点也能以较低的概率被选中作为验证人节点。
4. 每次验证人变更需要超过 2/3 节点的共识，记录到区块中。

验证人节点选举出来后，在随后的在任期间，这些验证人节点之间再通过 EBFT 共识算法来对区块提议进行确认。

EBFT 算法

享云链的 EBFT 算法是自 PBFT(Practical Byzantine Fault Tolerance) 算法改进而来，这些改进包括：

1. 简化状态机 (例如去掉 View Changed 等状态，超时后直接进入下一轮区块提议流程)，减少消息种类，使其更适用于区块链的共识场景。
2. 节点使用自己的数字签名进行提议或投票，以便算法能通过其公钥追溯恶意节点。
3. 算法对恶意节点和不稳定的节点进行惩罚：恶意节点的押金会被销毁并失去验证人节点资格，这将大幅增加节点实施不当行为的成本。提议区块超时的节点将被降低后续被选中作为验证人节点的概率，长期稳定出块的节点则会增加被选中作为验证人节点的概率，提升了系统的稳定性。

EBFT 算法是强一致性的共识算法，每次出块需要超过 2/3 节点的两轮投票，能容忍最多 f=(N-1)/3 个拜占庭节点（N 为验证人节点数量）；诚实节点不会重复提议同一高度的区块，对同一个高度的两个区块也不会重复投票，这样就避免了软分叉的情况；得益于强一致性保证，享云链能够具备极高的交易吞吐量，每隔 1-3 秒内就能确认一个区块，也就是说，享云链的交易能在 1-3 秒得到确认。

可扩展性

当数据量或交易量越过单链能支持的上限时，享云链通过使用多链架构、Layer 2 扩展方案等机制得到无限的可扩展性。

停顿恢复机制

如果当前验证人集合中超过 1/3 的节点出现崩溃或拜占庭错误，系统的出块流程将陷入停顿。这时候需要启动恢复机制。

系统陷入停顿一段时间后（比如 10 分钟），网络上所有节点都可以感知到，因为停顿时所有节点都收不到新的确认区块。这时由当前可用的验证人中的提议者构造一个特殊区块，称为恢复区块（recover block），这个恢复区块内容包含执行竞选算法得到的新的验证人列表，然后向网络上的其它备用节点广播这个区块，其他节点收到恢复区块后，验证区块合法性并检查是否确实陷入停顿状态（长时间没有接收到新的区块），再对新的验证人列表进行 2 轮投票确认，经过全体在线节点的 2/3 确认后，所有节点更新自己保存的验证人列表; 被选中的验证人则可组成新的验证人集合，恢复出块流程。若新列表中的验证节点也存在超过 1/3 的节点没有响应而无法出块，则将无响应节点排除后再竞选相应数量的验证人，直到系统恢复正常出块。

经过两轮 2/3 确认的恢复机制是可行的，因为它可被证明仍然是拜占庭安全的。尽管由于需要在庞大的节点集合中达成共识而可能缓慢而昂贵（大量的消息广播），但对于去中心化系统中极少发生的系统停顿事件，自动化的恢复机制将非常重要，即使需要昂贵的通信开销也是可以接受的。

为了尽可能避免进入停顿状态，当发现某个验证人节点连续 3 次超时没有提议区块时，则经过共识后从节点池选择节点加入验证人集合，同时将这个没有响应的节点从验证人列表中删除掉。

6.账户模型和资产模型

目前为止，区块链存在两种账户模型：来源于比特币的 UTXO 账户模型和以以太坊为代表的 Account 账户模型。这两种账户模型各有优势: UTXO 是无状态的，更有利于并发处理和实现隐私保护; Account 模型拥有全局状态，交易执行效率高，成本更低，并且更有利于实现图灵完备的智能合约支持。

享云链同时支持 UTXO 和 Account 两种账户模型；并且，无论是 UTXO 还是 Account 账户，用户都能管理多个种类的数字资产；其中每种资产都通过资产类型来区分，由于 Token 资产都是由智能合约发行的，或通过智能合约接收的来自其他公链的数字资产（例如比特币或以太币），因此享云链的资产类型实际上是一个合约地址。

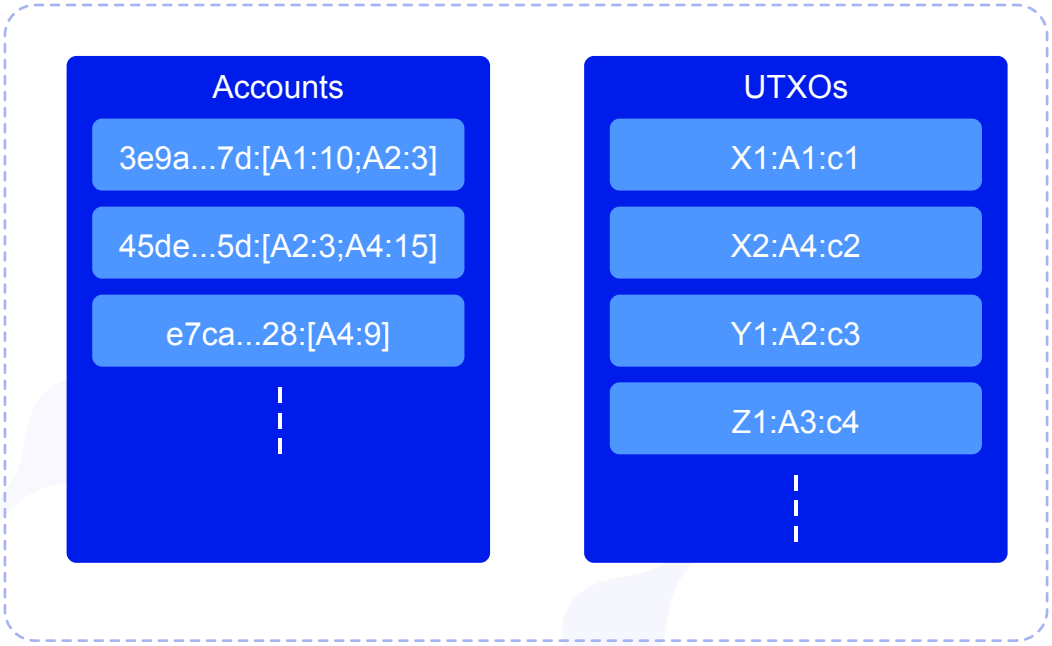


图:链上账户模型

如上图所示为链上账户模型的示例，链上有 Account 和 UTXO 两类账户：

1. 每个 Account 账户都有一个资产列表，记录当前账户下拥有的资产类型和对应的余额，例如，Accounts 条目 45de…5a: [A2:3; A4:15] 表示地址为“45de…5a”的账户中，资产（Asset）A2 的余额为 3，资产 A4 的余额为 15；
2. 每个 UTXO 都有一个“资产类型”字段，例如 UTXOs 条目 X2: A4: c1，此 UTXO 所有者为 X2（X2 为一次性隐私地址），资产类型 A4 的未花费输出为 c1。在链上，c1 是密文，隐私保护技术中称为金额承诺，只有此 UTXO 的拥有者能用其私钥解密后看到实际金额。

现在，若用户 Alice 的 Account 地址为 45de…5a，隐私地址为 X，X 的一次性地址分别为 X1 和 X2，则 Alice 的钱包将显示其拥有的资产列表：

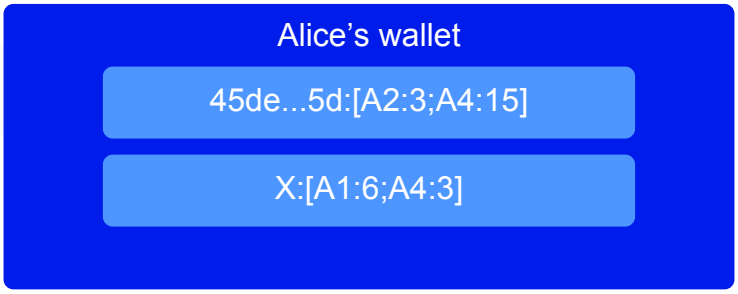


图:Alice的钱包

图中，Alice 的钱包显示其 Account 地址 45de…5a 有资产 A2 余额 3，A4 余额 15；隐私地址 X 有资产 A1 余额 6，A4 余额 3。由钱包私钥将金额承诺解密后，显示为实际金额。

享云链的多资产账户模型赋予普通 token 资产以第一类资产的能力，让 Token 资产能像原生数字资产那样自由流转，并能与任意的智能合约进行更复杂的交互操作；用户的钱包能显示两个账户模型下的所有资产余额，并且能通过发送交易将资产在两种账户模型之间互相转移。

得益于对两类账户和多资产模型的支持，享云链能提供完整的隐私保护方案和去中心化交易服务。

7.隐私保护

在传统的银行业和商业中，隐私保护是最重要的方面，因为隐私保护不仅有利于保障个人安全，也是市场能进行自由竞争的必要条件。

然而，在比特币和以太坊为代表的区块链系统中，链上的所有交易数据和账户数据对所有节点或用户都是公开的、可追溯的，任何人都可以查看任意账户的余额、追溯所有的历史交易数据。这样，某个用户只要公开其账户地址（为了能与他人进行交易，这是不可避免的），他人就能从链上看到他的所有账户信息和交易记录，而这些信息通常属于个人隐私或商业机密，为了保障个人安全或竞争优势，这些信息在现实世界中是不希望被泄漏的。区块链的这个薄弱之处与传统的银行业和商业准则有巨大的差异，导致大部分的金融和商业活动都无法在区块链上开展。

比特币上有用户开发了混币的方案来规避这个缺点，但这种方案存在中心化的第三方的缺点；Zcash 项目利用零知识证明实现隐私保护，但这种知识证明要求每笔交易添加约 30kb 的额外数据量，以致此方案也难以被用户接受；门罗币（Monero）项目使用环签名和 Bulletproofs 实现地址隐藏和金额隐藏，减少了交易数据量，是一个较为优秀的解决方案，但门罗币无法支持智能合约，并且吞吐量和交易验证速度仍然低下，难以大规模使用。

享云链的隐私保护方案的初步版本基于环签名方案和 Bulletproofs 技术来实现交易双方的地址隐藏和金额隐藏，并从共识算法、多链架构、并行性、硬件加速等方面改进交易验证性能，提升用户体验。并且考虑到公开交易也存在大量的应用场景，享云链的隐私保护特性对用户来说是个可选项，用户发起交易时可自行决定是否需要进行隐私保护。

地址隐藏原理

享云链隐私交易的地址隐藏使用可链接环签名方案。
每个用户 U_i 都有一组公私钥对（x_i, x_iG），其中 x_i 为私钥， $P_i = x_iG$ 为公钥，
此外，每一个公钥还有一个绑定的标签 Tag_i. 用户 U_0 签名时，他从网络上找其它 $n-1$ 个用户，记为 $U_1, U_2, \cdots, U_{n-1}$ ，将包括自己在内的 n 个用户的 UTXO 公钥装进合 $L = \{P_0, P_1, \cdots, P_{n-1}\}$ ，然后运行环签名方案，并在签名时出示 Tag。

验证者可以验证环签名的合法性，但是无法确定集合中 $L = \{P_0, P_1, \cdots, P_{n-1}\}$ 哪个公钥对应的私钥拥有者是真正的签名人，从而隐藏了签名人的信息，另外检查签名 Tag 是否被使用过，从而可以检验双花。

金额隐藏原理

享云链隐私交易的金额隐藏使用 Bulletproofs 方案。
通过非交互零知识证明协议，给定金额的绑定值 $\mathrm{Com} = xG + aH$ ，证明金额 $a \in [0,2^d - 1]$ 。
Bulletproofs 的证明体系主要基于离散对数的 Perdesen Commitment $C(x,a) = g^x h^a$ ，
证明体系的建立主要分为以下几步：

1. 给出新的对数尺寸内积证据（argument）；
2. 给出基于新构造内积证据的零知识区间证明系统；
3. 给出区间证明的聚合方法；
4. 给出基于任意运算电路的零知识证明系统。

隐私交易的 UTXO 结构

用户的所有隐私交易均通过 UTXO 的账户模型实现。如果想要进行隐私交易的用户只在 Account 账户中有余额，那么他可以先将 Account 账户的金额转换成 UTXO 形式，然后再发起隐私交易。

享云链的每一笔隐私保护的 UTXO 的数据主体是由以下几部分组成：

- UTXO 公钥：UTXO 的公钥全网公开，私钥由 UTXO 所有者掌握。
- 金额绑定承诺：金额为显式数字 a（不隐私）或者承诺 $\mathrm{Com} = xG + aH$（隐私，x 为混淆元素）。
- 金额合法证明：当前 UTXO 的金额承诺的 $\mathrm{Com} = xG + aH$ 满足 $a \in [0,2^d - 1]$ 区间证明 π 。
- UTXO 索引信息：包括环签名签发信息、区块信息等。

隐私交易的执行流程

当 Alice 向 Bob 发起隐私交易时，其用户钱包客户端执行以下流程：

1. 寻找混淆 UTXO；
2. 计算新的 UTXO 金额承诺及金额的合法性证明；
3. 通过公钥加密新 UTXO 的金额与混淆元素；
4. 协商新 UTXO 公钥（只有接收者可以算出私钥）；
5. 用可链接环签名签发交易。

交易请求广播到链上，验证人节点打包交易时，执行以下流程：

1. 验证旧的 UTXO 合法性；
2. 检验是否双花；
3. 验证环签名的合法性；
4. 验证新 UTXO 的金额合法性区间证明。

区块确认后，Bob 的钱包将执行以下步骤以接收新的 UTXO：

1. 根据新 UTXO 公钥，计算新 UTXO 私钥；
2. 解密新 UTXO 的金额和混淆元素；
3. 验证新 UTXO 承诺的正确性；
4. 使用钱包保存新 UTXO。

8.智能合约及虚拟机

享云链支持 WASM 和 EVM 两种主流的图灵完备的虚拟机，用户可以用 C/C++、solidity 等常用编程语言开发智能合约。

享云链的智能合约具有全局状态，其地址是 Account 地址；用户可以从 Account 或 UTXO 地址发送指定额度的隐私资产到合约地址；同样地，智能合约也能将指定额度的资产发送给 Account 地址或 UTXO 隐私地址。

在享云链上，通过智能合约发行的 Token 资产能通过一个普通交易的形式发送到链下的 UTXO 地址或 Account 地址上，被发送的 Token 资产将能被转换为等额的未花费的 UTXO 或 Account 账户余额增量，Token 资产的类型被设置为 Token 发行合约的地址。

9.节点选举

节点的稳定记账与出块对区块链系统的运行至关重要。享云链采取固定数量出块节点和备选节点协同工作的方式。

节点的稳定运转和出块质量将对整个生态产生主动影响，进入节点池的节点，无论是否处于出块状态，都需要保持服务器在线来保障出块的稳定与高速。

作为回报，节点出块时对应的手续费全部为出块节点所有，同时项目方还会对节点池内全部验证人节点（不包含恶节点）所能获得的奖励总额提供基础保障。由于存在销毁链克的机制可能导致链克的流通量不足，享云链的生态发展也可能需要补充链克参与流通，未来如出现递补链克的情况，节点池也将获得相应的链克用于奖励验证人节点，以保障出块速度和稳定性。

除社区会员拥有的权益外，节点还拥有重大事件的提议权与特殊事件的投票权。但如若出块节点在最高容忍时间内不出块、或有欺骗、勾结和选择性不参与行为的，一旦确定会被立即淘汰，并在本轮的未参与出块的节点中抽取替补。拖慢享云链运行效率，多次服务器不在线等行为，会剥夺本轮出块节点资格。

对于有作恶行为的节点，将加大惩罚力度，不仅立即剥夺验证人节点资格，还会采用销毁锁仓链克，并将其加入黑名单等惩罚方式。激励机制与惩罚机制的设计皆是为了保障体系中所有成员的利益与维持生态健康发展的驱动力。

节点选举与投票规则

只需要配置符合标准的服务器、质押足额链克的会员就可以成为节点候选人。

所有链克用户都拥有为节点候选人投票的权利，投票的效力与投票人的所持链克数相关，最终选出得票最高的相应数量的节点。在投票的规则中，拥有玩客云的成员不仅可以用链克投票，也可以用玩客云投票，一台绑定了链克口袋地址的玩客云所代表的具体票数，请参见每次竞选的规则详情。

由于享云链是一个动态发展的生态，每次进行节点选举时的环境均会有所变化。每次选举的具体规则，都可能依据当时的情况有所不同，请以项目官方网站公开的当期竞选与投票规则相关内容为准。

在首次节点选举中，为了保证享云链顺利切换至节点选举模式、安全运转度过转换期，会分段进行多轮招募，每轮招募少量节点，与项目方的节点一起构成节点池，并以这个节点池运行一段时期。

首次招募形成的节点池在运转一段时间，确保享云链的稳定、安全、高速运转后，将重新进行节点竞选，项目方的节点将与其他节点一视同仁地进行竞选，不再拥有直接进入节点池的特权。

进入节点池的节点，将会从锁仓链克数量、持续出块质量与随机种子的角度被衡量，按固定任期选出当前的出块节点。其中，锁仓越多的用户被抽中的概率越大，随机种子可以保锁仓链克较低的节点能够占到一定的出块比例。

关于首次节点竞选的细则等内容，请参见享云链官方网站后续公开的竞选详情。

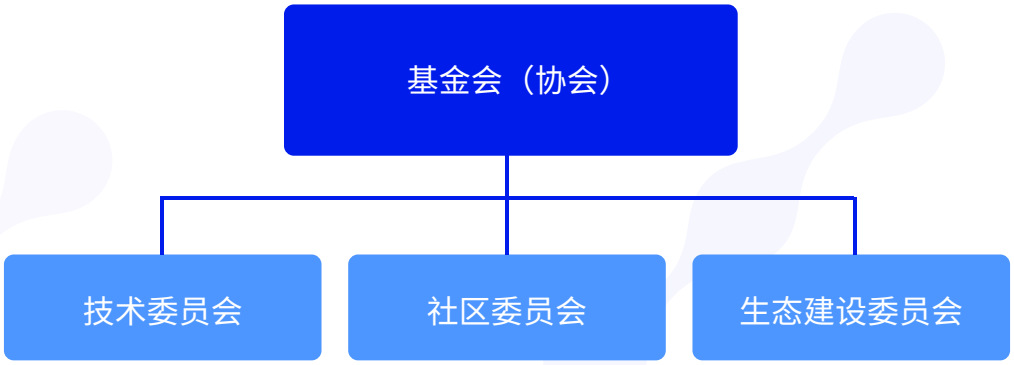
10.社区治理

在区块链的世界里，不仅要有第一生产力的技术，相应的价值尺度，还要具有使之自进化的管理体系。在享云链的自治体系中，承担主网搭建、技术升级和激励社区的项目方未来将会以基金会或协会的方式存在。而推动技术发展与生态繁荣的 DAPP 开发者与保障享云链运转的验证人节点将作为特殊角色，充分发挥技术生产力对区块链发展的重要作用。与此同时，广大链克用户也都可以成为社区的一员，甚至是作为社区管理机构的成员之一，在社区治理中贡献力量，成为建设享云链生态的一份子。

社区管理机构将会各司其职，协同发展，为保障生态建设与社区运转做出卓越贡献，维护体系中生产关系与生产力的良性协同发展。链克将会承担符合享云链共识机制的激励形式，成为生产力与生产关系相互促进的粘合剂。

管理机构职责与分工

为了推进生态建设的繁荣，维护社区秩序的稳定，保障自制体系的正常运转与资产处置的公正公开，体系内设立了以下组织架构：



基金会（协会）：作为项目方承担长期规划与重大事件仲裁职能；
向节点、开发者等为享云链生态做出贡献的人 / 团体提供奖励。
技术委员会：主要在协助推动享云链、各类 DAPP 的技术优化、技术建设和技术进步；
社区委员会：负责社区的日常管理、运营工作，保障社区的活跃度和有序运转；
生态建设委员会：负责生态建设相关的各项提案与落地，引导生态健康发展。

社区建设与发展

社区共建需要全体成员的参与，在自治系统中，不同的社区成员身份对应了不同社区建设参与权。投票决议将会是社区共建中的重要内容，类别大致为社区治理投票、选举投票与考评投票三种，不同的投票事项将由不同的决议人掌握，让整个社区在充满博弈的环境中蓬勃发展。

在体系设计中，参加管理机构的成员将通过日常工作获得链克激励。每位合格的委员会成员将会获得基金会按照一定的比例分配的链克资产。而为享云链做出贡献的人或者团体，无论是开发、宣传还是投资，社区均会对贡献度进行评判，与之匹配合理的奖励。

我们认为不存在可以应对享云链发展过程中一切问题的完备制度，享云链社区必然是不断发展的，需要由内自外的自我更新。因此，我们认为由基金会、验证人节点和三大委员会构成的享云链社区类似于现实社会中的立法机构，是可以不断进行自我完善的组织。

由于三类委员会的职能分工差异，首期成员的诞生方式、成员构成的更迭、机构规模的扩张与缩减方式等也各有不同。委员会运作机制的规则和管理职能细则，以及社区的各项规章制度，将在首次社区选举开启前公开。

此后在社区不断发展的过程中，发起决议事项的范围，各职能的分工等等，都会通过社区三个委员会在实践中，与节点、开发者、项目方一起不断讨论，不断发起新的议题，不断完善各项规则，基金会（协会）作为项目方，也会以投票者的身份加入其中，以民主的方式让享云链生态在不断变化发展的过程中，日趋合理、完善。

11.未来愿景——为基于区块链的所有信息的可信度赋值

基于享云链的高性能共识算法、隐私保护方案以及多资产账户模型，未来将引入衡量用户贡献的价值尺度与行为可信度的综合指标——信任值，使得享云链能在去中心化组织、商业、金融和公益等场景中更加切实践行，让基于区块链的一切行为、信息、数据的可信程度、价值高低有一个具备广泛共识的可参考指标。

包括验证人节点在内的每个用户（即享云链生态下的每一个地址）将被赋予一定的信用分(Credit Value)，此信用分用于衡量一个用户（无论此地址是普通人、节点或是某个企业）在系统中的可信度，信用评分越高，可信度越高。

享云链的信用值是由链下和链上相结合而产生的，是一个具有更高形式的制度设计的机器信任系统，这样的系统有着更高的生产力和经济活力。

例如在未来享云链共识算法改进中，信任被定义为一种能大幅降低系统的熵的机制。信任某个节点就是乐观地降低这个节点对系统的不确定性影响的预估。信用值越高的节点，其不确定性就越低，因此由高信用值的节点组成的系统将更加有秩序和高效率。

在未来信用值体系开始运作时，享云链将为此设计一套基于信用评分的共识算法，它综合了链上及链下的信用积累机制、经济学因素、密码学以及 BFT 容错算法，实现了低延迟、高吞吐、强一致性的共识机制，并且能在算法上识别并排除恶意节点或不能持续稳定工作的节点，提升了系统的稳定性，也鼓励了用户提供稳定可靠的验证人节点。我们称这个算法为 PoCredit-EBFT 算法。

而在去中心化社区中，只要存在明确的目标，我们就仍然需要有组织来承担协调机制：为了达成某个目标而组织人员、实施计划，这个过程中需要对所有权、架构、运作、奖励和惩罚制定一定的规范和评价、仲裁机制。享云链的去中心化社区未来也将被纳入信任值体系，通过有效的信用评分体系，衡量社区成员的声誉或可信度，从而大幅提高社区运行过程的公信力，以此为基础才能构建一个能健康地自我发展进化的去中心化社区。

另外，信用值及其评分系统在基于区块链的大量商业和金融场景中也将发挥巨大作用。如果没有信用体系，而只有狭义上的区块链，即使它的数据是经过共识的、不可篡改的、去中心化的、抗抵赖的、权限对等的，也无法在两个陌生人之间在进行交易之前就建立信任，因为信任能否达成跟交易双方在链下的实际情况及其在交易历史中的表现相关。

经济学研究认为信任的成本才是经济活动最大的成本，而企业组织之所以会出现的原因，正是为了能达成批量和长期的信任关系，降低内部交易成本以实现盈利；一个企业的规模会不断扩大，直到在企业内执行某项交易的成本大于在公司外执行该项交易的成本。信用值体系的引入有助力于隐私保护，并将链上交易的成本大幅降低，因此去中心化的组织、商业和金融应用将变得更加可行。

引入信用值体系后，链下和链上通过信用体系连接形成的互相促进的系统：用户通过链下的商品、服务、社区贡献、公益捐赠等行为提升信用评分，获得声誉和信任；基于信用评分的搜索排名将降低用户的搜索成本，从而享受链上的优质服务；这将使用户能降低交易成本，获得更多的利益；从而促进用户改进链下的商品或服务，或更多地贡献社区，或避免不当行为，以获得更高的信用评分。

信任值的功能主要有以下几个方面：

1. 搭建信用评分系统，使得生态内的商业模式以低成本高效率运转，促进匿名交易，在安全、可信的基础上保护隐私。
2. 利用信用体系可以降低搜索、签约、协调成本的特点，开拓去中心化自治组织或社区服务组织。
3. 开展去中心化金融服务，社区成员可以通过价值体系做价值验证、贷款、投融资及风险管理。
4. 评判组织、个人的可靠性，以及由其发起的项目、由其发布的信息的可靠性。

从微观的角度，信任值体系可以降低商业成本、提升商业效率；从宏观的角度，信任值体系可以为基于区块链的一切行为、数据和信息的可信度赋值，提供一个可靠的参考，从而降低求证互联网信息可靠性的成本，让每个人都可以简单、直接、准确的判断海量互联网数据中的某一条信息是否可信。

12.结论

享云链采用高性能的共识机制和隐私保护方案，支持多资产账户模型，并且通过信用评分体系，享云链系统已经将信任植入了软件协议里，并将它部署到整个网络中，为创新组织、商业和金融服务产业带来了一个新的公共设施。

在享云链上，任何用户都能够构建各类产业服务，持续维护信任且又可以保障隐私，以此为基础形成一个有效的自由竞争市场。因此，享云链有能力在包括去中心化自治组织、交易所、金融、商业服务以及公益项目等人们一直在设想的广泛应用场景中落地实用。

由于链克以及其背后的共享计算生态的存在，项目方还将以多种形式，把企业为获取以链克为激励单位的计算资源所付出的成本，源源不断地投入到享云链的生态当中，与其他应用场景一起，不断提升享云链的生态价值。

13.路线图

我们认为区块链技术与享云链，将给世界提供一个前所未有的可能性，进而创造一个崭新的未来。为了实现这一愿景，我们将要对享云链进行至少五次重大升级。且基于对探索未来无限可能性的期冀，我们将这五次升级分别以五位伟大的航海家来命名。

郑和升级

2019 年 9 月开启测试，预计 9 月内正式升级上线。支持 UTXO 账户模型和 Account 账户模型，业内首个同时支持 UTXO 和 Account 模型的主链；隐私链克功能上线，支持隐私 UTXO 交易；支持 EVM 与 WASM 双虚拟机。

在这个版本的享云链上，开发者可以发行非隐私 Token，可以开发基于合约的去中心化交易所，支持非隐私 Token 跟隐私链克的去中心化交易。虽然暂时只支持链克作为隐私 Token，但已经为隐私 Token 发行及去中心化交易打下坚实基础，具备支持去中心化交易所的能力。

另一方面，在 2019 年 9 月完成升级时，验证人节点轮换的共识算法、验证人节点与节点池正式上线运转。

享云链将依据节点竞选结果，把共识交给验证人节点和节点池来运作，享云链正式进入共建时代。

克里斯托弗·哥伦布升级

2019 年年底上线，原生支持单账户多币种，支持合约发行隐私 Token，每个享云链上发行的 Token 都可以转换为隐私的 UTXO。

享云链将为所有享云链上的 Token 提供隐私交易的基础服务，可以让链克以外的 Token 也具备隐私交易的能力。开发者能够开发合约发行自己的隐私 Token，并可通过合约进行隐私 Token 间、隐私 Token 和链克间的去中心化交易。

达·伽马升级

预计 2020 年 Q1 上线，实现跨链通信，项目方会先挑选 1-2 个非享云链 Token，例如比特币、以太坊或者 EOS 等，将其跨链到享云链上，为生态建立样例，同时欢迎开发者自己实现其他 Token 跨链，真正实现为所有 Token 提供隐私交易环境，为所有 Token 提供去中心化交易服务。

斐迪南·麦哲伦升级

预计 2020 年 Q2 上线，实现链的性能可扩展性，通过多链或者多 layer 的方式实现，为未来各类应用的并发量激增打好基础。

詹姆斯·库克升级

预计 2020 年 Q4 上线，实现基于信用评分的共识机制，社区自治与共建也将进入信用时代。为互联网信息和每个享云链用户（地址）的信任赋值，开启建设互联网信用时代。

引用

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System: https://bitcoin.org/bitcoin.pdf

[2] BitcoinWiki. Proof of stake. https://en.bitcoin.it/wiki/Proof_of_Stake

[3] Ethereum: https://github.com/ethereum/wiki/wiki/White-Paper

[4] Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems. 1982, 4 (3): 382–401. doi:10.1145/357172.357176

[5] Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance and Proactive Recovery. ACM Transactions on Computer Systems (Association for Computing Machinery). 2002, 20 (4): 398–461. doi:10.1145/571637.571640: http://pmg.csail.mit.edu/papers/osdi99.pdf

[6] MONERO RESEARCH LABS: RING CONFIDENTIAL TRANSACTIONS: https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2015/1098&version=20151217:200440&file=1098.pdf

[7] Zerocoin Electric Coin Company. ZCash: All coins arecreated equal, 2017. https://z.cash.

[8] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nickolai Zeldovich: Algorand: Scaling Byzantine Agreements for Cryptocurrencies: https://people.csail.mit.edu/nickolai/papers/gilad-algorand.pdf

[9] Ethan Buchman, Jae Kwon and Zarko Milosevic: The latest gossip on BFT consensus: https://arxiv.org/pdf/1807.04938

[10] Ethan Buchman: Tendermint: Byzantine Fault Tolerance in the Age of Blockchains: https://allquantor.at/blockchainbib/pdf/buchman2016tendermint.pdf

[11] Nicolas van Saberhagen: CryptoNote v2.0: https://cryptonote.org/whitepaper.pdf

[12] bulletproofs: https://crypto.stanford.edu/bulletproofs/

[13] Benedikt Bunz, Jonathan Bootle, Dan Boneh Andrew Poelstra, Pieter Wuille, and Greg Maxwell: Bulletproofs: Short Proofs for Confidential Transactions and More: https://eprint.iacr.org/2017/1066.pdf