区块链

Web3.0 时代：开放、隐私、共建

在分布式技术（区块链）的助力下，Web3.0 将从开放、隐私和共建三个角度去颠覆 Web2.0 互联网，打造一个由用户社区主导的去中心化世界，重构互联网流量价值范式。

Web2.0 时代，以互联网巨头为核心，形成多个生态圈，核心互联网公司对数据、价值和网络效应具有垄断性，生态之间存在着强大的隔阂界限。互联网世界最重要争夺的资源便是流量入口（用户注意力和资金流）。这一切在 Web3.0 时代将发生深刻的变化：Web3.0 世界将充分开放化，用户在其中的行为将不受生态隔离的限制，甚至可以认为，用户可以（基于基础逻辑）自由畅游在 Web3 世界；用户数据隐私将通过加密算法和分布式存储等手段得到充分保护；Web3 世界，内容和应用将由用户创造和主导，充分实现用户共建、共治，共享平台的价值。

Web3.0 的主要特点是开放、隐私和共建。开放性体现在：

1）用户在某个互联网应用“领域”中的准入充分自由、门槛低；

2）用户行为不受第三方限制、互联网应用打破原有的所谓生态内、生态间的界限，应用之间具有高度的组合性和复合性；合成资产、NFT 等组合下，甚至可以在非许可、无交割的前提下将传统世界财富融合进入 Web3.0。

3）另外，Web3.0 内部基于不同基础设施的应用之间可以被“跨链”协议解决互联互通。

隐私体现在：数据所有权归用户所有，价值转移不需要第三方授权。

共建体现在：用户在 Web2.0 互联网应用中的内容创造是多方面受限的（受平台审核限制、跨平台限制），在社区治理方面的限制更甚，因此也就限制了用户在创作者经济共享方面的价值捕获。Web3.0 将打破这些限制，同时区块链的代币激励机制将内容经济的价值有效地反馈给创作者。共建、共享的另一个方面是共治，即 DAO。

新的流量范式。Web3.0 将不是单纯争夺用户注意力和资金流入口，由于协议的复合型、用户登录的开放性等特点，协议的调用次数往往更重要。同时，Sandbox、Roblox、我的世界的兴起，让市场看到了从 2D 到 3D 的升维，除了更立体的展示效果，还会有更多的社交空间。

关于落地形态。Web3.0 充满了想象力，其最终的落地形态现在并不能清晰判断。但其趋势已然出现苗头。在向 Web3.0 演进过程中，有很多 Web 2.0 和 Web 3.0 混合形态的产品出现。典型代表是 Opensea 和 Metamask 钱包。

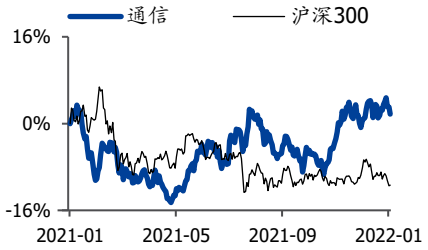
浏览器还是 APP？现存的 Web 3.0 应用，在 PC 和手机主要以 web 浏览器方式访问。不同于 Web 2.0 时代厂商喜欢开发独立的移动端 App 和 PC 客户端，Web 3.0 也许将打破这一现象。App 和客户端对于用户行为数据收集可能更为方便、也方便核心厂商对生态应用的管理，这一点在注重隐私和开发的 Web 3.0 时代将改变。

另外，本文对 Web 3.0 时代的监管也做了一些探讨和设想。1）稳定币——首当其冲，纳入传统监管框架；2）隐私性——底层 KYC，应用层实现可控适度匿名；3）DAO 治理——探讨阶段，传统监管介入。

风险提示：区块链商业模式落地不及预期；监管政策的不确定性。

增持（维持）

行业走势



作者

分析师宋嘉吉
执业证书编号：S0680519010002
邮箱：songjiaji@gszq.com
分析师任鹤义
执业证书编号：S0680519040002
邮箱：renheyi@gszq.com

相关研究

1、《通信：重视通信+基建产业链投资机会》2022-01-09
2、《区块链：数字人民币 App 上线，新电子支付体系显露真容》2022-01-04
3、《通信：2021 通信行业十大关键词》2022-01-03

内容目录

1. 核心观点 3
2. Web3.0 从何而来，又将何去？ 3
2.1. Web1.0 到 Web3.0：互联网经历了什么 3
2.2 . Web3.0 生态已现雏形 5
3. Web3 的标签：开放、隐私和共建的世界 5
3.1. 开放：Web3.0 打破生态界限 5
3.1.1 ENS（Ethereum Name Service）：去中心化的身份验证和域名系统 6
3.1.2. MASK Network：通向 Web3.0 的开放大门 7
3.1.3 Polkdot：连接 Web3.0 内鸿沟的桥 8
3.2. 隐私：数据所有权和价值的转移 9
3.2.1. Horizen：保护隐私前提下的开发平台 10
3.2.2 NuCypher：Web3.0 的分布式密钥管理系统 11
3.3. DAO：共建、共治和共享价值的网络世界 12
3.3.1 Mirror：完全由用户主导的内容创作平台 12
3.3.2 Gitcoin：代码与资源的共享共治平台 13
3.4. 元宇宙：Web3 推动"现实世界"与"虚拟世界"的融合 15
4. 向 Web3.0 流量价值新范式的演进 17
5. Web3.0 时代的监管思考 20
风险提示 21

图表目录

图表 1：当前的互联网模式下巨头事实上垄断了数据、价值和网络效应，处于生态链核心 4
图表 2：Web3.0 的进化史：从比特币到元宇宙 4
图表 3：Web3.0 生态图景（图中仅为部分产品） 5
图表 4：利用 ENS 域名给以太坊创始人 Vitalik 转账示意图 6
图表 5：过去 6 个月 ENS 域名协议日收入最高超过 80 万美元 6
图表 6：使用 Mask Network 查看代币信息 8
图表 7：波卡的概括性原理图 9
图表 8：Horizen 主链与侧链关系 10
图表 9：Horizen 主侧链传输 10
图表 10：Horizen 生态图 11
图表 11：中心化 KMS 与代理重加密 KMS 对比 11
图表 12：代理重加密过程图 12
图表 13：Mirror 创作界面 13
图表 14：Gitcoin 二次方融资实例 14
图表 15：Quests 问题列表 15
图表 16：Kudos 市场 15
图表 17：Mirror 平台目前有 26 种合成资产（图中为部分） 17
图表 18：Mirror 平台特斯拉股票代币铸造界面 17
图表 19：Opensea 月度交易额流量（美元） 18
图表 20：Opensea 月度 NFT 交易数量（个） 18
图表 21：Metamask 钱包集成 swap 交易流水数据（美元） 19
图表 22：关于隐私和匿名，一种可能的监管方案 21

1. 核心观点

元宇宙热潮之下，Web3.0 越来越多地被业界提及，什么是 Web3.0？Web3.0 有哪些特征？为什么我们需要 Web3.0？作为国盛区块链研究院 Web3.0 系列报告的首篇，我们将试着对上述没有标准答案的问题进行探索与分析。

我们认为，在宏观意义上，Web3.0 将是当前热议的元宇宙的底层网络架构，在分布式技术（区块链）的助力下，Web3.0 将从开放、隐私和共建三个角度去颠覆 Web2.0 互联网，打造一个由用户社区主导的去中心化世界，重构互联网流量价值范式。

虽然遥远，但在理想的 Web3.0 范式中，Web2.0 时代互联网巨头享有的生态、数据、流量价值等优势将式微，取而代之的是开放、隐私和共建的互联网新世界。Web3.0 的应用将打破 Web2.0 的生态圈界限，应用之间的复合性、组合性将不受限制，用户在 Web3.0 世界将以开放的姿态驰骋，在隐私得到充分保护的情况下充分发挥创造力，推动 Web3.0 世界更多创新应用发展和内容创建，同时流量价值将回馈给用户和社区。

2. Web3.0 从何而来，又将何去？

当下的 Web2.0 互联网似乎在“吞噬”着一切领域，人们不禁谈论着 Web2.0 红利的消失。始于 2008 年的区块链以去中心化的方式，从最初的点对点支付逐渐开始冲击着整个数字世界，尤其是近年来智能合约、DeFi、NFT 等创新的出现，使得数字网络出现了新的范式可能。电子屏幕和各类终端设备背后的数字世界，将在 Web3.0 的推动下，主导权由互联网巨头向用户转移。

虽然 Web3.0 的轮廓依旧模糊，Web2.0 巨头们似乎并未感受到其压力，但来自社区的创新将很快改变这一切。

2.1. Web1.0 到 Web3.0：互联网经历了什么

回顾互联网从 Web1.0 到 Web2.0 的演进，我们可以看到围绕流量争夺、流量变现的变迁。Web1.0 到 Web2.0，流量从供给不足（互联网刚出现）再到市场争夺流量入口（互联网普及），进而流量变现，中间还经历了从 PC 互联网到移动互联网的演变。Web1.0 和 Web2.0 可以说是流量为王的时代。虽然基础设施到应用层面的创新不断，但是流量为王的逻辑是不变的。流量背后，控制着用户流量的生态公司将享有最多的市场红利。相应的，用户的行为数据、用户体验都是在生态公司的限制下进行，用户创造和建设活动受到了一定的限制、且无法获得数据收益。类似的案例非常普遍，如支付工具的跨平台限制、跨平台的超链接屏蔽等等。流量不仅限于用户的注意力，还包括资金流量，关于后者相当于 Web2.0 对传统金融的侵蚀。

用户在 Web1.0 和 Web2.0 时代，用户的行为是受限的，用户数据隐私得不到充分的保护，用户在互联网中的创作和建设力度是偏弱的，即便是类似抖音这样的短视频平台，用户的创作也接受者平台的监管，创造的形式和内容也无法脱离平台本身的引导和限制；平台通过少数流量大 V 引导着绝大部分用户的内容体验。

可以说，Web2.0 时代，以互联网巨头为核心，形成一个个生态圈，生态内，核心互联网公司“统治”着生态，垄断着生态的数据、价值和网络效应。

图表 1：当前的互联网模式下巨头事实上垄断了数据、价值和网络效应，处于生态链核心

资料来源：国盛证券研究所整理

这一切在 Web3.0 时代将发生深刻的变化：Web3.0 世界将充分开放化，用户在其中的行为将不受生态隔离的限制，甚至可以认为，用户可以（基于基础逻辑）自由畅游在 Web3 世界；用户数据隐私将通过加密算法和分布式存储等手段得到保护；Web3 世界，内容和应用将由用户创造和主导，充分实现用户共建、共治（DAO，去中心化治理），同时用户将分享平台（协议）的价值。

除了完全不同的互联网模式和用户体验，Web3 将带来新的流量入口范式。Web2 时代占据用户注意力的流量入口模式将发生一些有趣的变化。

在以区块链为代表的分布式技术推动下，从去中心化点对点账本实验到去中心化智能合约平台，催生了无数的新型应用（Dapp），慢慢 DeFi 形成了数字世界里的“金融服务”，而 NFT 加速了资产上链。我们看到，传统世界（线上和线下）之外，用户越来越接近一个相融相生的数字世界。至此，人们呼唤一个全新的网络世界——元宇宙，即可信地承载个人的社交身份和资产，社区将拥有更强大的主导权。

以上就是 Web3.0 的进化简史。

图表 2：Web3.0 的进化史：从比特币到元宇宙

资料来源：国盛证券研究所整理

本报告将通过一些具体案例来剖析 Web3 开放、隐私、共建的特点，并分析新的流量入

口和价值范式的内涵。

2.2 . Web3.0 生态已现雏形

Web 3.0 技术堆栈主要可分为三层：协议层、应用层以及网络基础层。这一切主要是基于区块链构建的（当然协议层也可以有链下的辅助部分）。从应用角度看，Web 3.0 则涵盖 DAO（及工具）、隐私、应用、存储和数据、游戏、创作者经济平台、社交等几乎覆盖 Web2.0 的大部分领域。

伴随着加密货币行业的蓬勃发展，近两年涌现了大量的 Web3.0 应用，当然，这些应用最终也许大部分都是过渡期产品。甚至有些应用在经济模式、解决用户痛点方面存在着缺陷，并未体现出比 Web2.0 更真实需求。

无论如何，Web3.0 生态已现雏形，在不断的应用探索中，将一步步揭开 Web3.0 的面纱。

图表 3：Web3.0 生态图景（图中仅为部分产品）

资料来源：国盛证券研究所整理

3. Web3 的标签：开放、隐私和共建的世界

3.1. 开放：Web3.0 打破生态界限

Web3.0 的开放性体现在：

1） **用户在某个互联网应用“领域”中的准入充分自由、门槛低；例如，用户往往利用一个区块链账户地址就可以登录链上的应用，无须注册许可，操作便利；**

2） **用户行为不受第三方主体限制、互联网应用打破原有的所谓生态内、生态间的界限和隔阂，在复合代码运行逻辑的原则下，应用之间具有高度的组合性和复合性；最直接的案例就是所谓 DeFi Lego，任何应用都可以对底层基础协议（如 DEX）做调用或聚合，以及合成资产平台将现实世界资产映射到链上（无交割关系），这等于打破了所谓线上线下和虚拟与现实的界限。**

3） 另外，Web3.0 内部基于不同基础设施的应用之间可以被“跨链”协议解决互联互通；因此，用户在 Web3.0 世界多个应用的行为可以生产类似社交关系图谱，进一步提升数据价值的挖掘潜力。

举一个游戏应用的比喻，用户可以不受第三方限制、很方便进入一个游戏世界；用户可以将自身喜欢的角色/形象自由植入到游戏中去，甚至可以使得角色跨平台/领域行动，而 Web2.0 时代，如王者荣耀这类游戏，你无法决定角色的选择，更不能将喜欢的孙悟空杀进魔兽世界——这方面的连通平台并不难，只是因为控制权并不在用户手中。当然，你也可以交易角色皮肤等装备（借助 NFT），甚至基于其他 DeFi 协议建立复杂的游戏装备衍生品市场。总之，跨应用平台、跨虚拟与现实地完成 Web3.0 的生存方式。

本节将以 ENS、MASK Network 和 Polkdot 为例，阐释开放的意义。

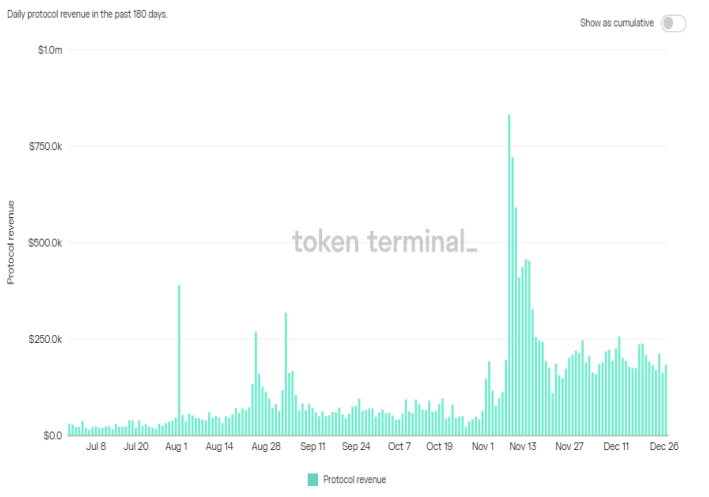
3.1.1 ENS（Ethereum Name Service）：去中心化的身份验证和域名系统

DNS（Domain Name System）是传统 Web2.0 的重要组成部分。当用户上网时，服务器会将用户的网址请求解析成 IP 地址返回给用户。如 www. https://www.bilibili.com/域名对应的 IP 地址可能为 http:// 119.3.211.130。这种可读性更高的域名系统降低了用户访问网址时的难度，为 Web2.0 的建设做出了重要贡献。DNS 解决了 Web2.0 访问的问题，然而随着网址的不断增多以及 Web2.0 中心化的特点，用户往往需要注册大量的网站账号，用来访问不同的网站。针对这一问题，尽管许多应用支持了使用较为主流的第三方社交 APP（如微信等）直接登录，但总体来看，这种各大网站直接分散割裂而导致用户需要注册大量账号的问题依然存在。总体来说，用户需要通过注册，才能够使用中心化机构管理的域名和账户系统来访问应用。用户如何做到无许可、更低门槛访问各类互联网应用？

图表 4：利用 ENS 域名给以太坊创始人 Vitalik 转账示意图

资料来源：imToken，国盛证券研究所

图表 5：过去 6 个月 ENS 域名协议日收入最高超过 80 万美元



资料来源：tokenterminal，国盛证券研究所

不同于 Web2.0 的中心化特点，Web3.0 世界用户登录行为依靠去中心化身份，DID（Decentralized IDentity）。最常用的一类 DID 即用户仅使用一个链上账号（区块链公钥地址，以 0x 开头的 42 位字符串）来访问各类 Web3.0 的 DApp，即单点登录。虽然为 Web3.0 的用户安全提供更自由、门槛更低的访问体验，然而过长的公钥显然难以记忆、可读性差。构建在以太坊上面的域名系统，ENS（Ethereum Name Service）的出现正是

致力于这一问题的解决，将用户的钱包地址与自定义的域名进行连接，如将类似 0xaa111aaa1aa11aaa11a111a111aa1a1a11a11111 的钱包地址改为 GuoSheng.eth 这一更为可读的域名。在之后登录各类 DApp 时，就可以使用 GuoSheng.eth 这一域名进行登录，用户之间可以通过此域名进行转账交互等行为。

总结而言，更为开放的 Web3.0 则支持用户仅使用一个账户（钱包地址）完成访问 DApp、与其他用户进行交互等各种操作。ENS 的出现解决了 Web3.0 中用户互动的可读性难题，为单点登录创造了更便利的条件。

构建在以太坊上的 ENS 可以**支持多链地址的解析**。用户可以将同一个 ENS 域名在比特币、以太坊和莱特币等不同链解析的不同的地址，同时 ENS 也具备内容寻址的功能（不同于 Web2.0 的 IP 寻址），解析到互联网应用网站平台。

可以想象，未来的 Web3.0 时代，用户在元宇宙中遨游（可以跨多个应用），无须注册许可，而通过一个简短的域名账户进行登录即可。

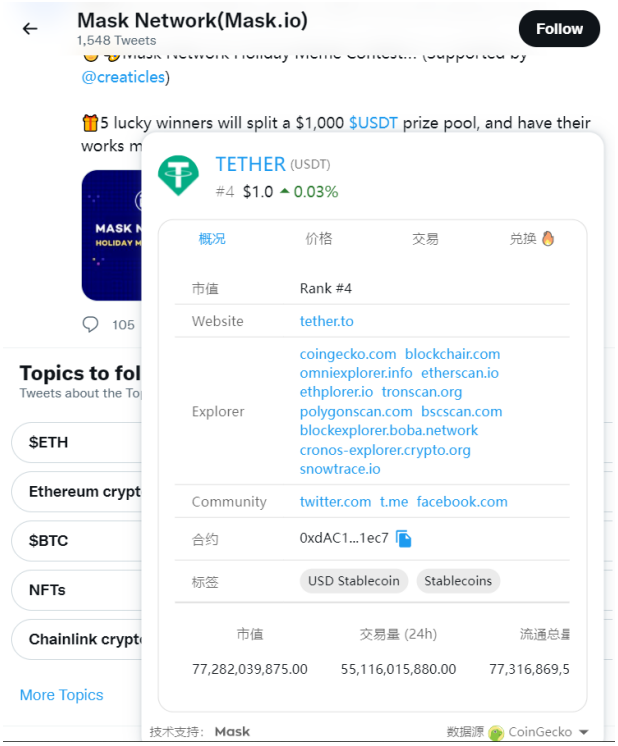
3.1.2. MASK Network：通向 Web3.0 的开放大门

Mask Network 是一组连接传统 Web2.0 应用与 Web3.0 应用的插件，为前者用户提供了进入 Web3.0 的大门。其开发的技术框架 Dapplet（Decentralized Applet）支持在目标网站（如 Facebook、Twitter 等传统 Web2.0 网站），将小程序嵌入其中，以此在中心化的 Web2.0 中实现小程序的去中心化。之后其与 Arweave 展开合作，支持在 Facebook、Twitter 上进行去中心化文件的上传和存储。

当前，用户只用在浏览器中安装 Mask 插件，即可在 Twitter 或 Facebook 上查看 Token 价格、进行 swap、参与 ITO（Initial Twitter Offering）以及参与社区投票（借助如 snapshot 等 Web3.0 应用）。同时还支持用户将链上资产（包括 NFT 收藏、捐赠记录）汇总至 Twitter。

Mask 带来的开放性是显而易见的，即任何 Web2.0 中的用户都可在不借助任何中心化 APP 或平台的前提下，通过 Mask 来直接访问 Web3.0 并进行相关活动。Mask 将开放的 Web3.0 世界，通过零门槛的方式展现在了每位 Web2.0 用户眼前。也就是说，MASK 将 Twitter 与区块链平台打通，用户可以自由地在多个平台应用之间遨游。这在 Web2.0 生态下几乎很难做到。

图表 6：使用 Mask Network 查看代币信息



资料来源：Twitter，国盛证券研究所

3.1.3 Polkdot：连接 Web3.0 内鸿沟的桥

常有投资者问起：未来是一个元宇宙还是多个元宇宙？它们之间能否互通？

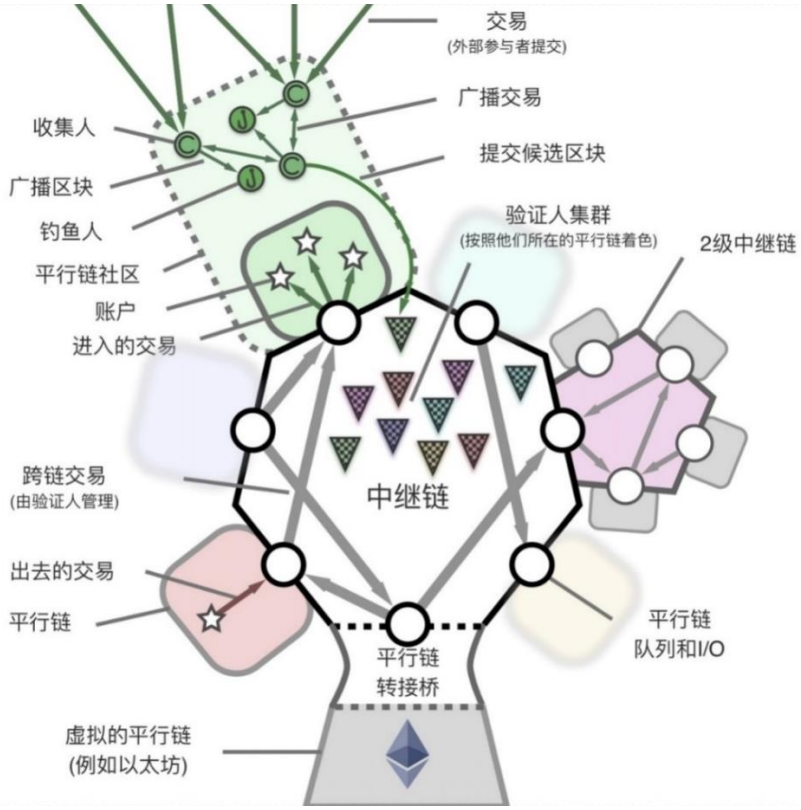
互通分多个层次，应用层、协议层等，一个重要的问题是 NFT 等数字资产无论是存放在联盟链（蚂蚁链、至信链、长安链等）还是公链（以太坊、比特币等），跨链互通是最基本的，而区块链本身是个带时间戳的账本，如何实现互操作？

不同公链之间是无法直接传递消息和执行操作的，Web3.0 内部诸多应用协议（可能是基于不同的底层公链）之间的鸿沟往往通过跨链的方式实现互联互通。当然，Web3.0 协议之间跨接一般不需要第三方主体进行授权（注册），这一点仍然遵循 Web3.0 的开放性原则。跨链可以是跨链资产桥（类似于多链资产兑换银行），也可以是波卡、Cosmos 这类多链协议。

波卡（Polkadot）是一个可伸缩的异构多链系统，能够传递任何数据（不只限于代币）到所有区块链，实现各个链之间资产与数据的互相流通。波卡是由 Web3 基金会发起的项目，由以太坊前 CTO Gavin Wood 主导的 Parity 团队进行设计和开发。波卡网络的基础构架包括中继链（Relay Chain）、平行链（Parachain）和转接桥（Bridge），波卡是一个真正的多链应用环境，使跨链注册和跨链计算等类似操作成为可能。

如果是比特币是计算器（电子现金系统）、以太坊是区块链世界的计算机，那么波卡就是路由器或者交换机，在计算设备（无论是 windows 系统还是苹果系统，甚至是移动设备）之间可以传递数据，实现万链互联。站在这个角度，波卡解决的问题不仅仅是公链自身性能瓶颈（更快的交易处理速度），而是从更丰富的角度解决扩展性——使得原本不兼容的链之间实现互操作，为多链共存的未来世界提供中枢或者路由。波卡系统是由一堆独立运行的区块链组成的，波卡为这些区块链（成为平行链）提供中继路由。

图表 7：波卡的概括性原理图



资料来源：波卡白皮书，国盛证券研究所

波卡作为中继链，为平行链间传递消息提供基础设施，值得注意的是，所传递的消息不仅限于代币（Token），而是任意数据；平行链之间的类型可以不同（异构）。这一点非常重要，目前的区块链作为一个分布式账本，矿工处理的工作主要就是维护账户，区块内最核心的数据就是账户代币余额，其他文本数据可以作为附注写入，但很难在区块间自由传递消息；并且，跨接的两条区块链可以是不同类型（甚至是私有链）。基于波卡可以在公共、开放、未经许可的区块链以及私有、许可区块链之间传输此数据。波卡是真正的多链应用程序环境，在其中可以进行跨链注册表和跨链计算之类的事情。例如，学校的许可链上的私有学术记录链可以向公共链上的学位验证智能合约发送证明。再例如，跟先前主要作为独立环境运行的网络不同，波卡提供了互操作性和跨链通信。这为创新的新服务打开了大门，同时，也允许用户在链之间进行信息传输。例如，提供交易代币化的股票（用代币来标记股票）的交易所的链，可以跟提供股票交易所帧数数据的链（预言机链）通信，例如为代币化的股票交易提供喂价。

3.2. 隐私：数据所有权和价值的转移

数据隐私已成为全球监管的焦点问题，现行的解决方案一是强化法律保护，让使用者意识到盗用用户数据是违法行为；二是引入隐私计算，通过同态加密、多方安全计算、可信执行环境等技术，保证数据在使用过程中是明文不可见的。在 Web3.0 时代，用户将倾向于用更彻底的方式保护个人数据隐私，从而引发数据所有权和价值的转移。随着应用的去中心化，链上数据可查的情况下，用户行为、产生的数据乃至应用协议亦需得到隐私保护。隐私保护是多方面的，包括基础区块链平台隐私保护、存储数据隐私（分布式存储）、用户私钥管理、匿名协议等多方面。

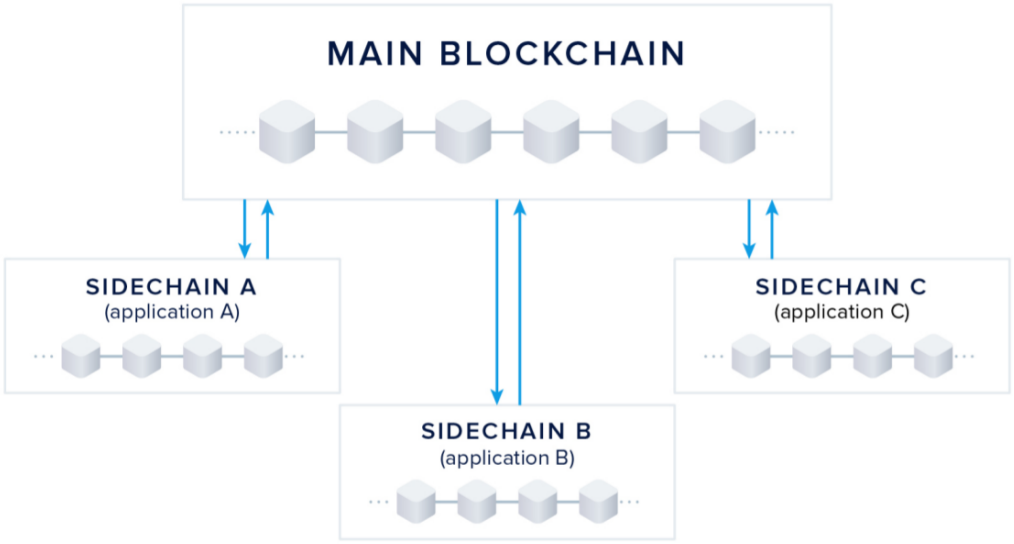
本节以 Horizen、NuCypher 为例探讨 Web3.0 隐私特点，前者可以为用户（包括企业用

户）提供一个不上传本地隐私数据前提下完成开发的基础区块链平台，企业可以借此为用户提供区块链相关服务，但又充分保护了企业的隐私数据；后者为 Web3.0 用户提供了一个分布式私钥共享/托管平台，不同于 Web2.0 时代中心化机构托管用户账户的方式（让渡部分隐私），Web3.0 的管理也可以去中心化地交给网络。

3.2.1. Horizen：保护隐私前提下的开发平台

Horizen 原名 Zencash，致力于打造隐私保护和基础区块链平台，为用户或企业可以在不上传本地隐私数据的前提下提供开发平台。Horizen 由主链和侧链构成。Horizen 主链主要是为用户的交互提供简单且安全的价值传输和存储层，通过原生治理代币 ZEN 为整个 Horizen 的生态运转提供支持，以及为侧链提供必要的基础架构。而具体功能的实现以及网络基础结构等均由侧链开发完成，从而能够针对特定的用例进行更为复杂的性能优化，增强其可扩展性和安全性。Horizen 侧链又称 Zendoo，其具有极高的扩展性和设计性。侧链有独立的共识机制与加密算法，并且真正的实现了去中心化。开发者可通过 Horizen 开放的一套标准通用组件 ZEN 侧链开发套件（SDK）来迅速完成区块链的开发，从而节省区块链的构建时间。利用侧链附带的零知识证明工具可以在不上传本地隐私数据的前提下，完成企业需求的开发。

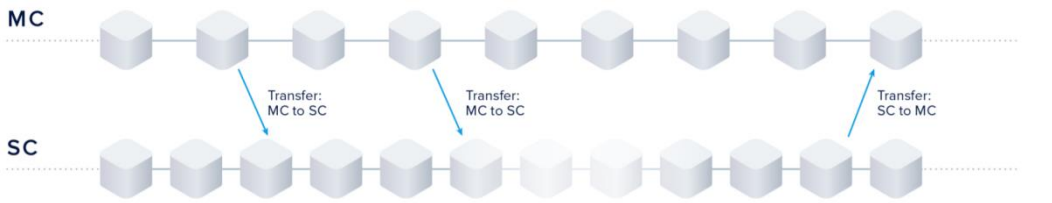
图表 8：Horizen 主链与侧链关系



资料来源：Horizen 白皮书，国盛证券研究所

同时，主链与侧链之间可以通过其独创的跨链传输协议 CCTP（The CrossChain Transfer Protocol）实现代币 ZEN 以及数据的互联传输，为解决可扩展性问题提供基础保障。

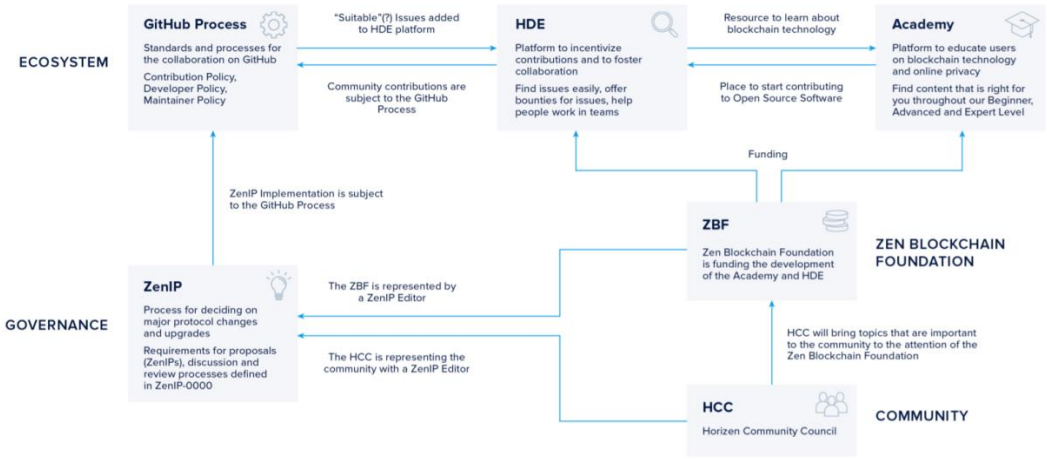
图表 9：Horizen 主侧链传输



资料来源：Horizen 白皮书，国盛证券研究所

Horizen 采用 Zk-snark（零知识证明）以及防 51%攻击等安全解决方案构建了一个具有极高隐私保护性以及安全性的 Web3.0 区块链平台，为用户与开发者提供隐私保护。

图表 10：Horizen 生态图



资料来源：Horizen 白皮书，国盛证券研究所

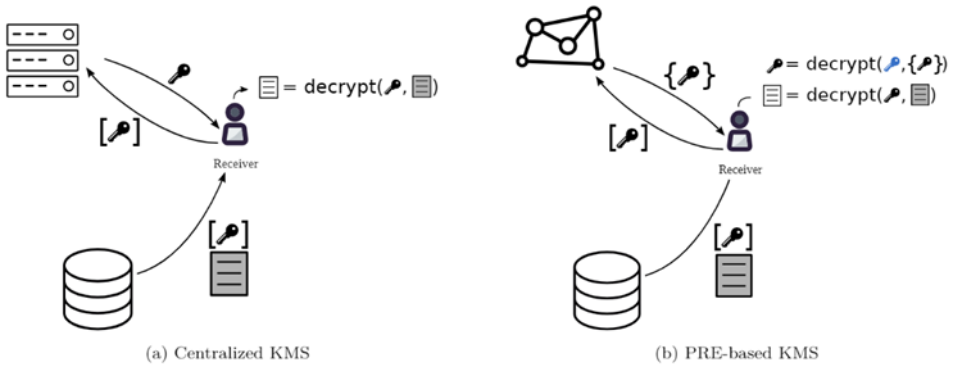
3.2.2 NuCypher：Web3.0 的分布式密钥管理系统

不同于 Web2.0 应用的密钥托管（一般由互联网公司或第三方托管），区块链私钥管理，对很多初级用户来说是一个难题，而多方共享私钥管理（去中心化的方式）则是一个更为现实的需求。用户该如何借助互联网协议安全地管理和共享私钥呢？也就是说，多方共享私钥管理可以将私钥托管给一个去中心化的网络协议（而非 Web2.0 那样交给互联网公司），在指定的用户间安全共享，使得用户解决了进入 Web3.0 之前最基础的需求。

NuCypher 能够在互联网上任意数量的用户之间共享私钥，同时使用其核心技术——代理重加密来代理解密权限。其原生代币 NU 主要用于奖励网络节点参与者来执行密钥管理和权限代理/回收的操作。

传统中心化密钥管理系统（KMS）的用户密钥交由中心化第三方存储，在第三方存储机构安全的前提下，用户密钥可以得到较为充分且安全的保护。在用户双方需要进行数据传输时，数据发送者需要从第三方机构调用数据接收者的公钥对数据进行加密，之后数据接收者使用自己的私钥对数据进行解密。但其缺点在于，数据发送者只能使用数据接收者的公钥进行加密，数据传输后数据接收者可以永久保留对数据的访问权限。

图表 11：中心化 KMS 与代理重加密 KMS 对比

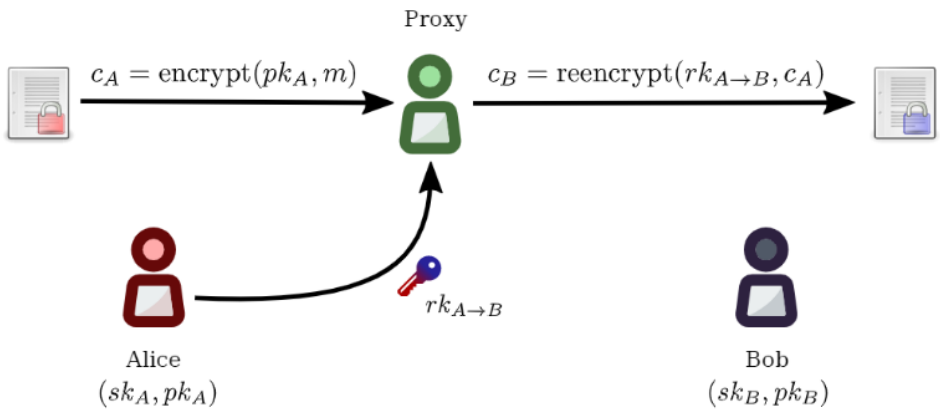


资料来源：NuCypher 白皮书，国盛证券研究所

而 NuCypher 采取的代理重加密 KMS 使用第三方节点分布存储用户的密钥信息。在用户进行数据传输时，首先由数据发送者使用自身私钥和数据接收者公钥生成重新加密密钥，此后将密钥切分为[n]段，将每个片段分发给 NuCypher 上的节点进行保存。之后，数据

接收者仅有权限在由数据发送者制定的时间段内访问该信息，数据发送者也可随时撤销数据接收者的访问权限。

图表 12：代理重加密过程图



资料来源：NuCypher 白皮书，国盛证券研究所

如此一来，NuCypher 保证了数据发送者的加密授权主动性，同时分布式的密钥存储方案确保了用户密钥存储的安全性，为 Web3.0 数据传输的密钥管理提供了安全的保障。

3.3. DAO：共建、共治和共享价值的网络世界

用户在 Web2.0 互联网应用中的内容创造是多方面受限的（受平台审核限制、跨平台限制），在社区治理方面的限制更甚，因此也就限制了用户在创作者经济共享方面的价值捕获。Web3.0 开放性原则将打破这些限制，同时区块链的激励机制将内容经济的价值有效地反馈给创作者。

3.3.1 Mirror：完全由用户主导的内容创作平台

Mirror 类似于 Medium、Substack 等博客类内容创作平台。其解决的问题在于，在传统自媒体中，内容创作者可以输出创意，但获得是收益是有限的，且面临 IP 被盗问题，能否将创意固化为资产并支持交易？Mirror 当前主要功能包括：

1）作品（Entries）：
Entries 是 Mirror 主要的内容创作模块，创作者可以在此处进行文档编辑，编辑支持纯文本+Markdown（类似话题标签）的格式，同时 Mirror 还支持直接将 Medium 或 Substack 等其他平台的文章迁移至 Mirror。对于创作者的每一篇产出，Mirror 均支持将其直接铸造为 NFT。NFT 在链上完成铸造之后，创作者便可将其作品以 NFT 的形式出售。这样一来，便解决了内容创作者的收益问题。创作者还可将作品永久存储在分布式存储平台 Arweave 上，保证作品的永久性存储。

2）众筹（Crowdfunds）：
众筹模块支持创作者进行任何形式内容的众筹，并且可以基于每个支持者的资助金额为支持者分发相应的支持者代币（由众筹发起者铸造），众筹前三名还可获得独特的 NFT 奖励。此代币可以理解为支持者所持有的股份，若作品铸造为 NFT 后出售获得了相应收益，可以此为基准进行相应的收益分配。而 NFT 则是项目社区成员的标志，从而自然而然的建立起一个 DAO。

3）收益拆分（Splits）:
收益拆分模块支持创作者将作品收益或拍卖收益分发给其他多个实体，以此来与合作者共享共同作品的收益。拆分至少需要在两个账户地址之间进行，并且各实体之间的拆分百分比之和必须为 100%。这样一来，在创作者提前预设好收益分配比例和规则之后，每一笔收益都将由智能合约自动完成收益分配的过程，避免中心化收益分配的不透明。

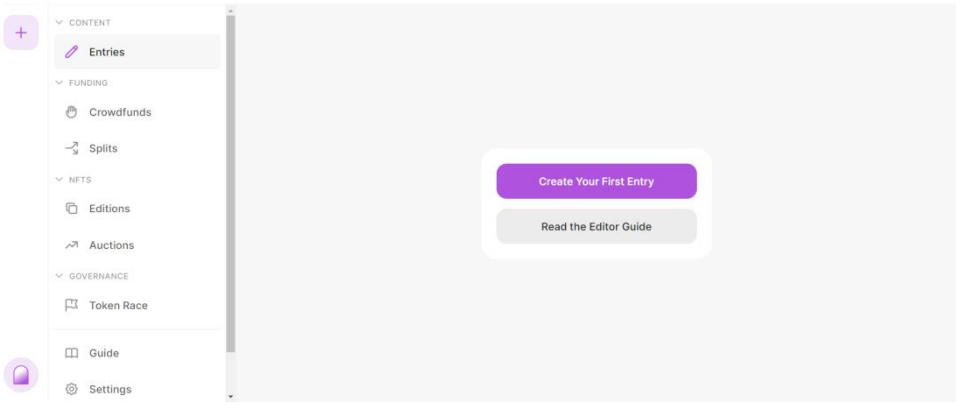
4）NFT 铸造（Editions）:
Editions 模块为 Mirror 的 NFT 铸造模块，用户可以使用此模块在 Mirror 上铸造 NFT 作品，其中包括价格、媒体文件（当前支持.jpg, .png, .gif, 和.mp4 四类文件）、总供应量以及资金首款地址四个创作者自定参数。铸造好之后会生成该 NFT 地址，同时会加上相应的 editionID，该地址可以直接嵌入 Mirror 的其他文章，在链接下方显示 NFT。

5）拍卖（Auctions）:
通过拍卖板块，创作者可以将自己创作的 NFT 作品进行拍卖。创作者需要设定拍卖的保留价格和持续时间，每次出价应不小于上次价格的 10%。拍卖同样可以创建对应的 URL 地址嵌入 Entries 模块之中，拍卖结束后的收益可以直接转入创作者设定的钱包地址，也可转入众筹或收益拆分模块。

6）投票（Token Race）:
投票功能服务于众筹之后所形成的 DAO，其形式类似于 Snapshot。众筹的参与者自然而然的组成了 DAO，通过投票功能可以参与 DAO 的决策，实施社区的各类决议，在此基础上形成了创作者社区的能力闭环。

Mirror 作为 Web3.0 最重要的内容创作平台之一，允许任何一个 Web3.0 用户在其中创作自己的作品，并围绕其开展各类活动。更重要的是，创作者自身完全拥有自己的创作作品，可以完全支配其作品而不受 Mirror 平台的影响。通过 Crowdfunds，Splits 和 Token Race 等模块，创作者可以创建属于每位社区成员的内容社区，并与成员共同建设属于每个人的社区。

图表 13：Mirror 创作界面



资料来源：Mirror 官网，国盛证券研究所

目前看，相比于 Web2.0 时代成熟的内容创作平台，Mirror 这类产品尚处于萌芽期，NFT 的生成流转、DAO 治理都有不成熟之处，也可能被后来用户体验更佳的平台所替代，但作为 Web3.0 前沿且理想主义的探索，Mirror 所实现的方案仍有借鉴意义。

3.3.2 Gitcoin：代码与资源的共享共治平台

在传统网络世界中，如果你有个新奇的想法需要实现怎么办？设立一家公司去拿风投？在大公司争取个创新部门？去一个众筹平台？去车库咖啡碰碰运气？这些看起来都效率偏低，能不能有个平台让新奇的点子、投资者人和代码实现者之间架起桥梁？

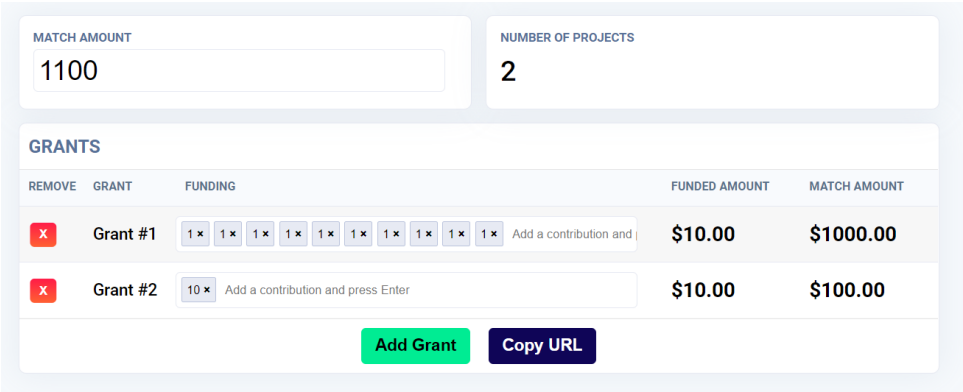
Gitcoin 是基于以太坊构建的去中心化协作平台，其为开发者提供了一个开发协作平台，同时为投资者提供了一个捐赠平台（加密货币捐赠）。可以简单理解为项目的代码和资金的众筹、共享平台。其核心功能主要有：

1）赏金（Bounties）：
该分区主要面向广大 Web3.0 开发者，开发者可通过发布赏金（Bounty）来针对指定问题寻求外部帮助，其他开发者可以通过解决该问题而获得赏金奖励。基于此，项目开发者可以更好的建设社区项目，而解决问题的开发者则可获得相应的奖励。

2）黑客松（Hackathons）：
该分区下集成有许多 Hackathon 项目，开发者可在此处加入由各个项目方所赞助的黑客松比赛，依照其主题开发相应的产品。

3）捐赠（Grants）：
在捐赠分区，用户可以向一些初创且具有公共物品性质的项目进行捐赠，捐赠结束后，部分项目可能会向捐赠用户给予空投回报。Gitcoin 捐赠的核心创新在于二次方融资（Quadratic Funding）。在进行二次方融资时，项目所获资金为社区成员捐出资金的“平方根之和的平方”，即$\int_P^{QF} = [\sqrt{C_1} + \sqrt{C_2} + \cdots + \sqrt{C_P}]^2$，之后基金会将根据每个项目的社区二次方融资金额按比例进行配捐。如在一轮募资中共有两个项目 Grant1 与 Grant2，Grant1 获得来自 10 个人的 1 美金等值加密货币的捐赠，共计 10 美金。而 Grant2 获得来自 1 个人的 10 美金捐赠，共计也是 10 美金。此时若基金会配捐额度为 1100 美金，根据二次方融资公式，Grant1 能获得的二次方融资票数为$\left[\sqrt{1} + \sqrt{1} + \sqrt{1} + \sqrt{1} + \sqrt{1} + \sqrt{1} + \sqrt{1} + \sqrt{1} + \sqrt{1} + \sqrt{1}\right]^2 = 100$美金，而 Grant2 能获得的二次方融资票数为$\left[\sqrt{10}\right]^2 = 10$美金。因此按照两个项目二次方融资的票数，Grant1 所能获得的基金会配捐为$\frac{100}{110} * 1100 = 1000$，而 Grant2 所能获得的基金会配捐为$\frac{10}{110} * 1100 = 100$。这样一来，获得基金会配捐的往往是那些投票人数更多的项目，而并非投票金额最多的项目。一方面鼓励了更多用户参与捐赠投票，从而票选出公共服务性最强的项目。另一方面大大增加了骗取基金会配捐的成本，降低了配捐风险。

图表 14：Gitcoin 二次方融资实例

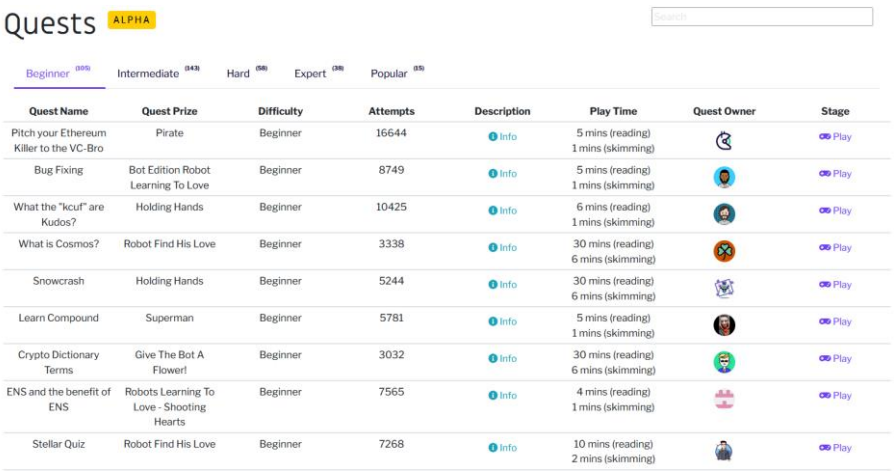


资料来源：Gitcoin 官网，国盛证券研究所

4）探索（Quests）：

该板块可以支持用户以一种游戏的方式去了解 Web3.0 世界以及各类生态系统，用户可以在题库中选择自己感兴趣的题目展开学习，之后以问答攻击的形式检验学习成果（每回答正确一题，系统生成的机器人会减少一滴血），击败机器人之后可获得相应的奖励，因此其本质为 Learn2Earn 的一种。

图表 15：Quests 问题列表

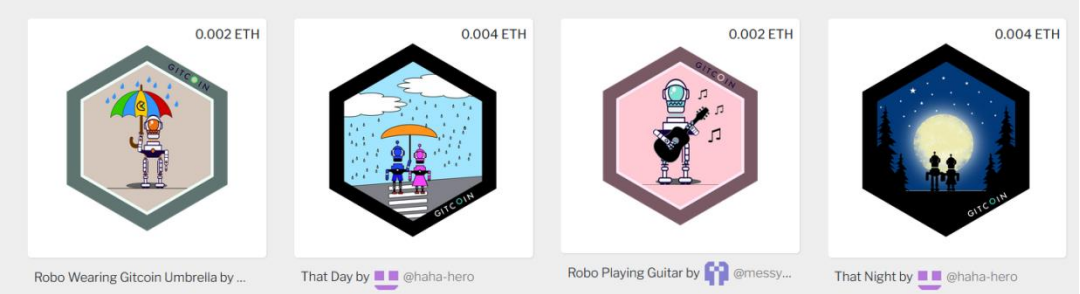


资料来源：Gitcoin 官网，国盛证券研究所

5）荣誉（Kudos）:

Kudos 是一种用户之间相互表达赞赏和建立关系的一种新方式。如用户 A 想通过 Gitcoin 向用户 B 表达感谢时，其可在 Kudos 市场购买荣誉勋章，将其赠送给用户 A。（勋章本身可视作某种形式的 NFT）

图表 16：Kudos 市场



资料来源：Gitcoin 官网，国盛证券研究所

6）学习（Kernal）:

Kernal 是一个点对点学习社区，其通过由社区成员构建的八周课程，为想要深入理解 Web3.0 的用户提供了绝佳的平台，其内容包括以太坊发展历史、全球金融体系、代币经济学等多方面的知识。

Gitcoin 为各类 Web3.0 初创项目以及想要进一步了解 Web3.0 的用户提供了最为友好的孵化平台和学习平台。对于项目而言，从黑客松的开始，到捐赠的发展，充满公共性的 Web3.0 项目在每一个用户的支持下发展，最后又回馈 Web3.0 用户。对于用户而言，在这里了解 Web3.0，支持 Web3.0，通过对项目的捐赠，共建 Web3.0。在这里，每个人都能为 Web3.0 的建设贡献自己的力量，实现真正的共建、共享与共治。

3.4. 元宇宙：Web3 推动“现实世界”与“虚拟世界”的融合

Web3.0 时代，元宇宙将是一个极富想象力和创造力的网络形态。Web2 时代，人们习惯

以“虚拟世界”和“现实世界”来作为线上线下世界的界限。构筑在 Web3 基础上的元宇宙，将是所谓“现实世界”和“虚拟世界”的深度融合。

Web2 时代的互联网存在着明显的生态界限（这是由于中心化公司运作方式下的结果），一家互联网巨头控制住生态的核心准入，跨生态的应用是比较少的——例如在线支付工具跨生态的限制、重要互联网应用入口之间超链接的屏蔽。所谓的互联网应用，其实被限制在不同生态局域内的活动。而 Web3 时代的元宇宙世界，Web2 时代的“鸿沟”和界限将被打破。

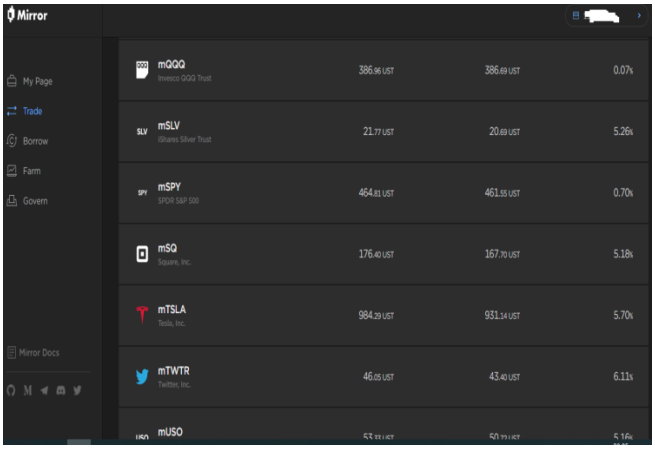
除了上面章节提到的跨链应用解决了基于不同主链生态之间的融合之外，元宇宙世界与所谓的“现实世界”将不断融合。例如，一个元宇宙中的主体，除了在 DeFi 市场从事经济活动，也可以持有现实世界的资产权益。也就是说，元宇宙中的资产，并不存在“虚拟世界”账户与“现实世界”账户系统之间的隔离，元宇宙将是“现实世界”与“虚拟世界”的融合形态。一般会认为，元宇宙的世界虽然由用户共建，不同应用之间可以自由地通过各种手段打通融合，但元宇宙的虚拟世界无法与现实世界的资产账户打通，因为现实世界存在生态之间的隔离，所以“外部的元宇宙”更无法打入目前 Web2 时代的生态。基于 DeFi 的合成资产应用（如 mirror（本节的 mirror 与 3.3 节项目重名，为不同项目）或 synthetix），我们将看到如何以降维打击的模式将 Web2 世界的资产映射到 Web3 世界来。

上线于 2020 年 12 月 4 日的 Mirror Protocol（基于 Terra 公链）是一个可追踪股票、期货、交易所交易基金和其他传统金融资产价格的合成资产（Mirrored Assets，MmAssets）铸造平台——甚至可以将加密货币（比特币、以太坊等）映射到平台铸造代币的代币，MIR（Mirror Token）为平台的治理代币。用户可以通过超额抵押 UST（TerraUSD，锚定美元的稳定币）或者已有的 mAssets 合成 mAssets，不同的 mAsset 将会与不同的股票、期货、基金等资产的价格对应。赎回时，需要用户通过 Mirror 平台销毁铸造时产生的 mAssets，智能合约会收取一部分手续费并返还给用户铸造时抵押的 UST 或 mAssets。

简单说，Mirror 就是将传统金融市场（或者加密市场）的资产合成为 Token 的形式，映射到加密货币世界。比如，可以在 Mirror 平台上铸造特拉斯的股票通证——mTSLA，也可以讲 ETH 代币映射到 Mirror 平台——铸造 mETH 代币。实际上用户获得 mAssets 并不等同于购买了相对应的金融资产，所以也不存在股票分红等收益——但由于价格跟金融资产关联、且有抵押物支撑合成资产的价值，所以可以理解为合成资产可以获得对应金融资产的部分收益权，也可以将其类比为金融资产的期货（不可交割）。

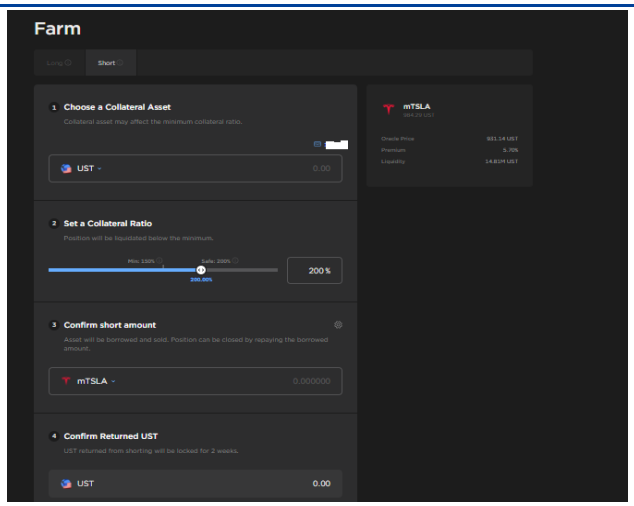
目前平台已经上线 26 种合成资产，包括特斯拉、苹果等股票和 BTC、ETH 等主流加密货币资产，以特斯拉股票代币为例，24 小时流动性尝过 1480 万美元，交易量在百万美元级别，Mirror 平台总流动性已经超过 10 亿美元。

图表 17：Mirror 平台目前有 26 种合成资产（图中为部分）



资料来源：terra.mirror.finance，国盛证券研究所

图表 18：Mirror 平台特斯拉股票代币铸造界面



资料来源：terra.mirror.finance，国盛证券研究所

Mirror 平台上的个股价格是如何锚定真实现货市场？这就需要用到预言机机制，通过程序算法来链接两个市场的价格。具体详情请参与我们的报告《DeFi 新金融（二）：超额抵押与资产映射》。

类似 Mirror 或 synthetix 这类合成资产应用，相当于在 Web2 世界毫无感知的情况下，将资产映射到 Web3 世界。从这个意义上讲，基于 Web3 的元宇宙可以将“现实世界”资产融合进来。这也是 Web3 实现“开放”特点的例证。

4. 向 Web3.0 流量价值新范式的演进

互联网重要的流量（入口）价值，在 Web3.0 时代会是怎样的范式？

Web2.0 争夺用户注意力和资金流量，从而实现流量价值变现。Web3.0 时代，流量入口价值依旧重要，但绝不局限于此。

例如，推动“DeFi Summer”的最大功臣之一的 Uniswap，从面向用户的角度来说，同样想 Web2.0 一样的流量入口——用户利用其 DEX 协议完成交易兑换功能，用户支出的手续费作为协议（平台）的流量变现（其中一部分反馈给 LP），站在这个角度看，Uniswap 同 Web2.0 其他应用没什么本质区别。但作为基础 DEX 协议，Uniswap 可以被其他协议调用，产生复合性特点（即所谓的 DeFi 乐高）。最典型的如收益机枪池、交易聚合器等应用，用户在这些应用上完成 DeFi“挖矿”收益、交易兑换功能，其背后往往是调用 Uniswap 等 DEX 协议，而这些协议对用户来说是隐藏在背后的，而且中间可能隔了多个协议调用过程。但对于 Uniswap 基础协议流量变现来说，效果是一样的。

由于 Web3.0 世界的开放性，这些调用不存在授权许可和生态界限等问题，完全是开放的。因此 Web3.0 的流量价值范式将呈现出开放化特点。另外，Web3.0 流量价值还与协议调用的次数强相关。

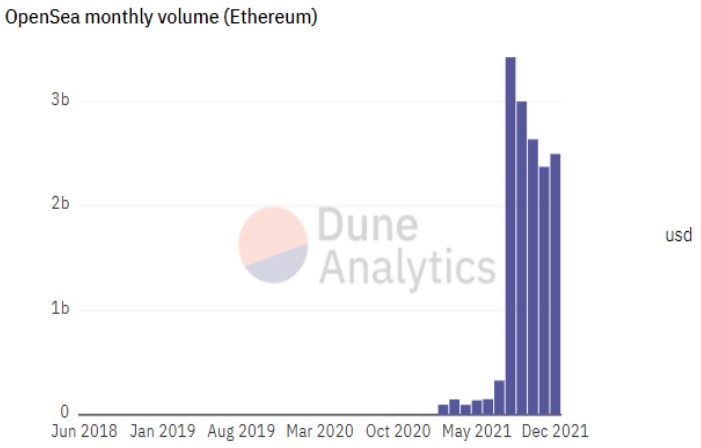
当前我们看到的众多社交（微信、微博）、娱乐（Steam）、金融（东方财富）等平台都是 Web1.0 向 Web2.0 演进中的受益者，未来向 Web3.0 演进形态是怎样的？

Web3.0 充满了想象力，其最终的落地形态现在并不能清晰判断。但其趋势已然出现苗

头。在向 Web3.0 演进过程中，有很多 Web 2.0 和 Web 3.0 混合的形态的产品出现。这方面典型的代表是 NFT 交易平台 Opensea 和 Metamask 钱包。Opensea 的收入依靠 NFT 交易手续费，这类似传统的电商或者中心化交易所的模式。Metamask 钱包有嵌入如 Chrome 等 PC 浏览器插件和手机 app 形式，作为重要的用户入口，Metamask 集成了 swap 聚合功能，用户可以直接通过其调用 DEX 协议完成代币兑换，则额外付手续费给 Metamask 平台。这两者都是典型的 Web 2.0 产品。但用户在这两个平台上操作则是 Web 3.0 世界的典型产品或功能。

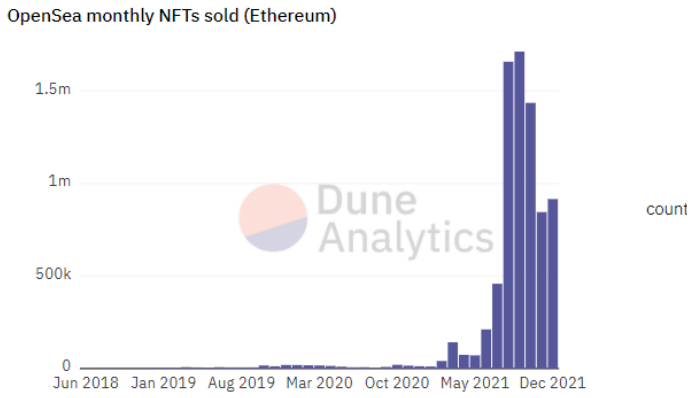
2021 年下半年随着 NFT 交易市场的火爆，Opensea 进入交易额和交易量激增时期，8 月单月交易额超过 34 亿美元。作为应用最为广泛的浏览器钱包插件，Metamask 的流量入口价值得以体现，用户基于其使用 swap 交易额和平台手续费亦有较大增长。2021 年 9 月 30 日交易额近 4 亿美元，平台手续费收入 350 万美元。

图表 19：Opensea 月度交易额流量（美元）



资料来源：dune.xyz，国盛证券研究所

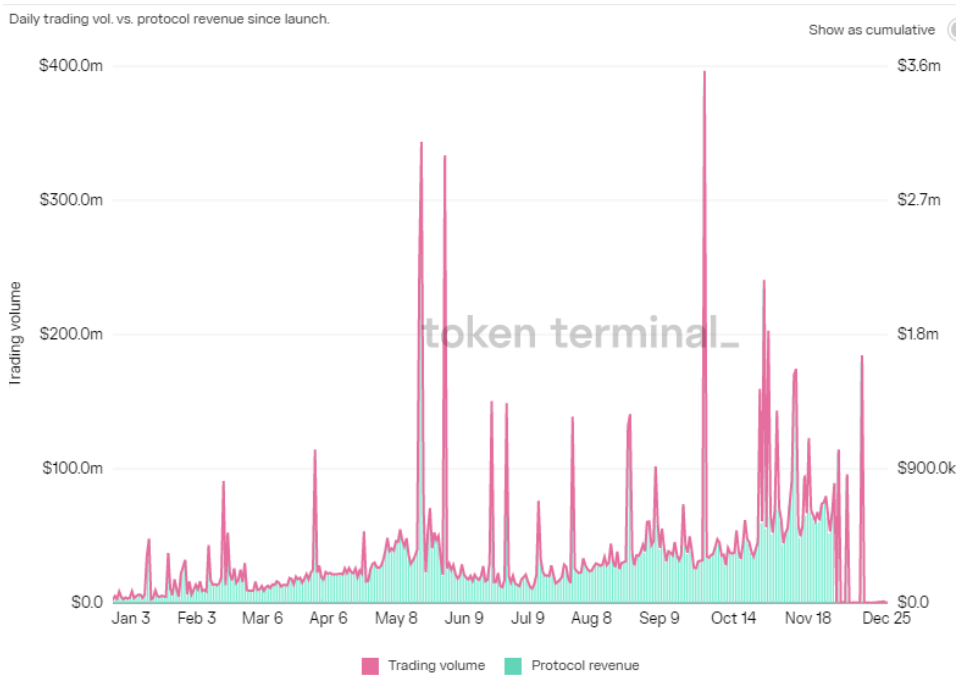
图表 20：Opensea 月度 NFT 交易数量（个）



资料来源：dune.xyz，国盛证券研究所

这也许是目前最有意思的一个现象。用户基于对 Web 3.0 的信仰和向往，却化为 Web 2.0 商家的流量和收入。严格来说，Opensea 和 Metamask 是再典型不过的 Web 2.0 产品，其流量变现模式极为简单和传统。NFT 交易和 DeFi 挖矿，这些看似是 Web 3.0 世界的基础构成，却最终为 Web 2.0 产品创造了流量价值。也许正是因为这个原因，Elon Musk 在其推特上提到：“有人看到过 Web 3.0 吗？我没有”。

图表 21：Metamask 钱包集成 swap 交易流水数据（美元）



资料来源：tokenterminal，国盛证券研究所

当然，这只是过渡时期的形态，也许这种形态要存在很长一段时间，但我们相信 Web 3.0 新的应用、新的产品逻辑和新的流量范式正在发生。

从 2D 到 3D?

近期随着百度希壤、网易伏羲等发布，而三星也在 Decentraland 上构建虚拟商店，市场逐步关注 3D 数字世界。而从 2D 向 3D 的演进有望成为普通用户最触手可及的变化。以国盛区块链研究院在 Decentraland 中的虚拟总部为例，虚拟建筑本身相当于团队首页，可以展示研究产品和团队情况，当然也可以通过虚拟人进行交互。当需要路演时可在二楼路演大厅演示 PPT 或接入流媒体，观众可通过发放徽章 NFT 进行白名单管理。我们判断，在 IT 基础设施逐渐完备的基础上，2022 年将有更多社交属性的流量将升级到 3D。

图表 22：国盛区块链研究院在 Decentraland 中的虚拟总部

资料来源：国盛证券研究所

图表 23：3D 虚拟总部中的路演现况

资料来源：国盛证券研究所

在传统 Web2.0 中，同时浏览首页的用户彼此之间并没有交互，而当进入 3D 世界后，社交欲望将更强，且通过 NFT、皮肤等可以提高个体分辨度。我们认为，元宇宙的沉浸更多来自社交、分享和经济活动，而非限于 AR/VR。从 2D 到 3D 就演进到 Web3.0 了？当然不是。这只是用户看到的界面升级，更深层次的是如何激励玩家进行创作、分享和交互。简言之，如果 Roblox、TikTok 没有经济激励，还会有那么多用户在其中进行游戏、短视频的内容创作吗？本质上，沉浸感的构建来自内部分享、创作带来的自我满足感和外部经济激烈的叠加。

浏览器还是 APP？

Web2.0 时代，各类 APP 成为应用的主阵地，催生了买量、刷机等生意，用户的大量时间、数据被捆绑在头部 APP 中。而现存的 Web 3.0 应用，在 PC 端主要以 web 浏览器方式访问。手机端为 web 浏览器访问，钱包 App 也可以作为入口，但仍以 web 方式访问具体应用。不同于 Web 2.0 时代厂商喜欢开发独立的移动端 App 和 PC 客户端，Web 3.0 也许将打破这一现象。App 和客户端对于用户行为数据收集可能更为方便、也方便核心厂商对生态应用的管理（类似 appstore 那样的应用商店审核和管理），这一点在注重隐私和开发的 Web 3.0 时代将改变。也许 Web 3.0 正如其名字一样，web 将作为一切应用的基础。

5. Web3.0 时代的监管思考

Web3.0 带来的监管挑战无疑是巨大的，开放、隐私和共建的背景下，并非意味着 Web3.0 应用不需要监管。但毫无疑问，由于 Web3.0 应用业务模式的巨大革新，监管方式势必会产生大的变化以适应新事物的发展业态。

因此，我们认为 Web3.0 时代，监管将呈现以下发展趋势：

1）对于沟通 Web3.0 和 Web2.0 两个世界的通道/业务，将首当其冲，寻求适合的监管模式，以适应 Web3.0 的发展：

例如稳定币作为传统世界财富进入 Web3.0 世界的重要通道，将最先产生监管行为。我们在《DeFi 新金融（二）：超额抵押与资产映射》报告中层指出，长期而言，稳定币与现实经济世界融合是大趋势，稳定币是沟通两个世界财富的重要桥梁。

稳定币目前最大问题在于与当下货币政策相冲突。很显然，稳定币在加密货币市场充当了"法币"的作用，某种程度上违反了当下各国的货币政策（同时还存在违反其他金融监管政策，如证券、期货等，甚至包括税收政策的可能），这也是加密货币资产的共同面临的问题。2020 年 11 月，《中国金融稳定报告（2020）》首次提及稳定币（中国人民银行金融稳定分析小组，2020），2021 年 7 月《中国数字人民币的研发进展白皮书》指出：有的商业机构计划推出全球性稳定币，将给国际货币体系、支付清算体系、货币政策、跨境资本流动管理等带来诸多风险和挑战，并将稳定币纳入虚拟币监管之列。

但对全球市场而言，稳定币或将随着加密货币市场快速增长。因此未来一段时间，稳定币与监管的冲突将成为行业发展的大背景。最终结果，或许是创新与监管的相向而行，推动监管演进和迭代，在欧美等地率先出现加密货币市场与传统金融市场进一步融合，各国央行会将稳定币纳入货币监管体体系，未来的货币政策有可能包含了稳定币的政策。而这一切的前提是，先明确稳定币的监管定位——禁止使用、接纳为货币或视为新的金融产品，都是潜在的可能选择，这依据各国不同的市场情况来定。

2）隐私和匿名方面，有可能存在底层实现 KYC，应用层实现适度匿名：

对于分布式网络带来的隐私和匿名功能，一方面存在隐私和匿名的需求，另一方面，并非隐私和匿名意味着会完全忽视监管。在现实世界中，监管必定存在，Web3.0 亦将探索中与监管的融合之道。一种似乎可行的办法是：在区块链网络底层实现监管，意味着底层账户将存在着 KYC 等监管约束，而在中间协议层和应用层实现适度匿名。当然，监管的手段也是灵活的，用户 KYC 等信息可以存储在由监管参与的多签网络中。

图表 22：关于隐私和匿名，一种可能的监管方案

资料来源：国盛证券研究所整理

3）DAO 治理过程中，势必会引入监管作为治理一方：

DAO 是 Web3.0 世界运行的重要的治理机制，但理想的的 DAO 方案似乎并不能解决所有问题，往往在需要仲裁、追讨被盗资产等问题发生后，现实社会政府机构和监管机构往往有着非常现实的作用。例如在 DeFi 系统经常发生的黑客攻击事件、以及其他难以预料事件导致的损失发生时，完全依靠 DAO 是不够的。这时候往往要借助现实社会政府和法律等手段解决。例如，当 DeFi 项目发生风险时，仅仅依靠社区的去中心化治理未必能够敦促开发团队保护或追回用户的加密资产。相反，在危机发生时，真正能够威慑到攻击者的，还是现实社会中的中心化机构和法律威慑。例如，当黑客的部分个人信息暴露以及部分资产被中心化机构所冻结时，黑客才愿意与开发团队谈判并承诺退回被盗的资产。例如，2021 年 8 月 Poly Network 项目被盗事件中，被盗资金中最为安全的部分就是被稳定币发行公司 Tether 宣布冻结的 3300 万美元等值的资产——作为中心化公司，Tether 拥有冻结链上 USDT 资产的权限。

由此我们可以设想， DAO 的治理，势必少不了现实社会监管机构的参与，监管机构作为 DAO 的治理一方似乎是非常理想的方案。

风险提示

区块链商业模式落地不及预期：Web3.0 基于区块链、密码学等技术，相关技术和项目处于发展初期，存在商业模式落地不及预期的风险。

监管政策的不确定性：Web3.0 实际运行过程中涉及到多项金融、网络及其他监管政策，目前各国监管政策还处于研究和探索阶段，并没有一个成熟的监管模式，所以行业面临监管政策不确定性的风险。

免责声明

国盛证券有限责任公司（以下简称"本公司"）具有中国证监会许可的证券投资咨询业务资格。本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为客户。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

本报告的信息均来源于本公司认为可信的公开资料，但本公司及其研究人员对该等信息的准确性及完整性不作任何保证。本报告中的资料、意见及预测仅反映本公司于发布本报告当日的判断，可能会随时调整。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。本公司不保证本报告所含信息及资料保持在最新状态，对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本公司力求报告内容客观、公正，但本报告所载的资料、工具、意见、信息及推测只提供给客户作参考之用，不构成任何投资、法律、会计或税务的最终操作建议,本公司不就报告中的内容对最终操作建议做出任何担保。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。投资者应当充分考虑自身特定状况，并完整理解和使用本报告内容，不应视本报告为做出投资决策的唯一因素。

投资者应注意，在法律许可的情况下，本公司及其本公司的关联机构可能会持有本报告中涉及的公司所发行的证券并进行交易，也可能为这些公司正在提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。

分析师声明

本报告署名分析师在此声明：我们具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，本报告所表述的任何观点均精准地反映了我们对标的证券和发行人的个人看法，结论不受任何第三方的授意或影响。我们所得报酬的任何部分无论是在过去、现在及将来均不会与本报告中的具体投资建议或观点有直接或间接联系。

投资评级说明

投资建议的评级标准		评级	说明
评级标准为报告发布日后的 6 个月内公司股价（或行业指数）相对同期基准指数的相对市场表现。其中 A 股市场以沪深 300 指数为基准；新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准；香港市场以摩根士丹利中国指数为基准，美股市场以标普 500 指数或纳斯达克综合指数为基准。	股票评级	买入	相对同期基准指数涨幅在 15%以上
		增持	相对同期基准指数涨幅在 5%~15%之间
		持有	相对同期基准指数涨幅在-5%~+5%之间
		减持	相对同期基准指数跌幅在 5%以上
	行业评级	增持	相对同期基准指数涨幅在 10%以上
		中性	相对同期基准指数涨幅在-10%~+10%之间
		减持	相对同期基准指数跌幅在 10%以上

国盛证券研究所

北京
地址：北京市西城区平安里西大街 26 号楼 3 层
邮编：100032
传真：010-57671718
邮箱：gsresearch@gszq.com

上海
地址：上海市浦明路 868 号保利 One56　1 号楼 10 层
邮编：200120
电话：021-38124100
邮箱：gsresearch@gszq.com

南昌
地址：南昌市红谷滩新区凤凰中大道 1115 号北京银行大厦
邮编：330038
传真：0791-86281485
邮箱：gsresearch@gszq.com

深圳
地址：深圳市福田区福华三路 100 号鼎和大厦 24 楼
邮编：518033
邮箱：gsresearch@gszq.com