

Web3.0: 脱胎换骨、擎天架海

华西计算机团队

2022年11月13日

分析师：刘泽晶

SAC NO: S1120520020002

邮箱：liuzj1@hx168.com.cn

核心逻辑:Web3.0脱胎换骨、擎天架海

- ◆ **从Web1.0到Web3.0，从用户只读到用户拥有。** Web1.0是只读模式的网络，是静态的、单向的网络，代表产品为浏览器与电子商务；Web2.0更注重用户的交互，用户既是浏览者，也是内容的制造者，在模式上由“读”向“写”发展，代表产品为社交媒体、短视频平台；Web3.0是价值互联网，Web3.0是一组包容性协议，为应用程序制造商提供构建块，**内容由用户创造，数据归用户所有，每个人都能掌握自己的（数字）身份、资产和数据。**目前代表产品为虚拟货币与NFT，此外我们认为元宇宙是Web3.0的终极设想。
- ◆ **Web3.0：去中心化、价值确权、用户自主。** Web 1.0/2.0时代数据存储在统一的服务器上，服务厂商可以决定数据的删减去留，Web 3.0时代的数据是存储于去中心化的区块链上，具有不可篡改、集体维护、规则透明的特点。**Web3.0用户权利提升，用户责任增大，实现更大程度上的用户“权责对等”，此外用户不仅具有对数据的所有权，还能参与规则制定和组织治理。**Web3.0的三大特性为：**1、开放性：**互联网应用打破界限，实现真正意义上的互联互通；**2、隐私性：**数据所有权归用户所有，价值转移不需要第三方授权。**3、共建性：**区块链的代币激励机制有效反馈内容经济的价值给创作者。
- ◆ **Web3.0的底层技术架构。** Web3.0与元宇宙两者相辅相成、一体两面，元宇宙是上层建筑，Web3.0是基础设施，Web3.0代表的是技术发展方向。Web3.0技术架构具备颠覆性，拥有不可篡改、集体维护、规则透明的特点；与Web2.0的核心差别在于**1、区块链：**Web3.0的数据存储主要集中在区块链上，应用程序具有去中心化的能力；**2、智能合约：**是一种自动执行程序，无需中间人参与，满足条件自动触发。此外，**3、密码学为区块链和Web3.0技术保驾护航，**Web3.0与密码学紧密相连，每一个新的区块链都需要一个核心算法；**4、分布式存储、分布式数据库为Web3.0提供底层技术支持，**具有成本低、安全性高、低延时、数据稳定等特点。
- ✓ **投资建议：**关注三条投资主线 **1)具备密码学能力的相关厂商，受益标的为卫士通、信安世纪；2)具备分布式数据架构能力的厂商，受益标的为：海量数据、星环科技；3)具备区块链能力的应用厂商，受益标的为四方精创、荣联科技、京北方、东方国信、蓝色光标、榕基软件、天地在线、福石控股、天娱数科、二六三、三湘印象等。**
- ◆ **风险提示：**核心技术水平升级不及预期的风险、区块链政策监管风险、政策推进不及预期的风险、中美贸易摩擦升级的风险



目录

01 从Web1.0到Web3.0，从用户只读到用户拥有

02 Web3.0的特性与典型应用

03 Web3.0的底层技术架构

04 投资建议

05 风险提示



01

**从Web1.0到Web3.0 ,
从用户只读到用户拥有**

1.1 从Web1.0到Web3.0，从用户只读到用户拥有

- ◆ **Web1.0是只读模式的网络，是静态的、单向的网络**，比如各类新闻网站。
- ◆ **Web2.0更注重用户的交互**，用户既是浏览者，也是内容的制造者，在模式上由单纯的“读”向“写”以及共同建设发展。比如各类博客、视频平台、论坛社区等。
- ◆ **Web3.0是价值互联网**，用户不仅能创作数据，还能拥有自己的数据，并能在不同平台交互共享，强化虚拟货币、网络安全和网络财富的共识，以及语义化的实现。

Web1.0到Web3.0发展历程

阶段	大致时间段	提出人	概念文献	属性特点	代表公司/应用	相关核心技术
Web1.0	1990-2005	Tim Berners-Lee	《在全球范围内建立超媒体信息检索系统》	信息交换和展示门户	Netscape Yahoo!	数据存储、处理和传输
Web2.0	2005至今	Darcy DiNucci 及Tim O'Reilly	《Fragmented Future》	内容创造与交互平台	Google Facebook Twitter Amazon	大数据、云计算
Web3.0	目前处于开端	Gavin Wood	《Insight into a Modern World》	用户自己创造和掌握的自主环境	比特币 以太坊 NFT	区块链、人工智能、边缘计算

1.2 从Web1.0到Web3.0，从用户只读到用户拥有

- ◆ **1990年万维网诞生**，蒂姆·伯纳斯·李与罗伯特·卡里奥在CERN一起成功通过Internet实现了HTTP代理与服务器的第一次通讯，并提出了万维网的概念。
- ◆ **1991年蒂姆·伯纳斯·李建立世界第一个网站**，标志着Web1.0时代的开启。
- ◆ **1994年万维网标准提出**。蒂姆·伯纳斯·李创立了万维网联盟，它由不同的意愿建立万维网标准和提高万维网质量的公司组成。
- ◆ **Web1.0时代从1991年到2004年**，互联网是静态的、只读的HTML页面。

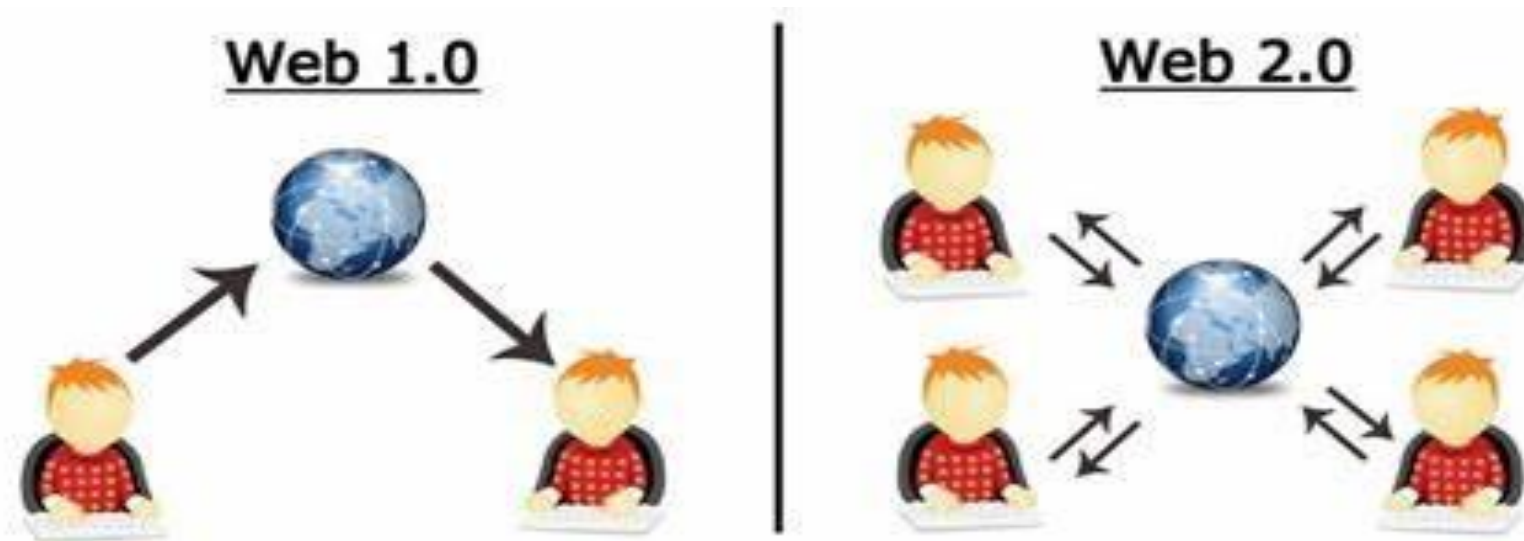
Web1.0时代



1.3 从Web1.0到Web3.0，从用户只读到用户拥有

- ◆ **2004年Web2.0时代开启**，Tim O'Reilly和Dale Dougherty提出Web2.0概念。
- ◆ **Web2.0是读写时代**。用户不再仅仅是互联网的读者，同时也成为互联网的作者。用户由被动地接收互联网信息向主动创造互联网信息发展。
- ◆ **Web2.0更加注重交互性**。不仅用户在发布内容过程中实现与网络服务器之间交互，而且，也实现了同一网站不同用户之间的交互，以及不同网站之间信息的交互。

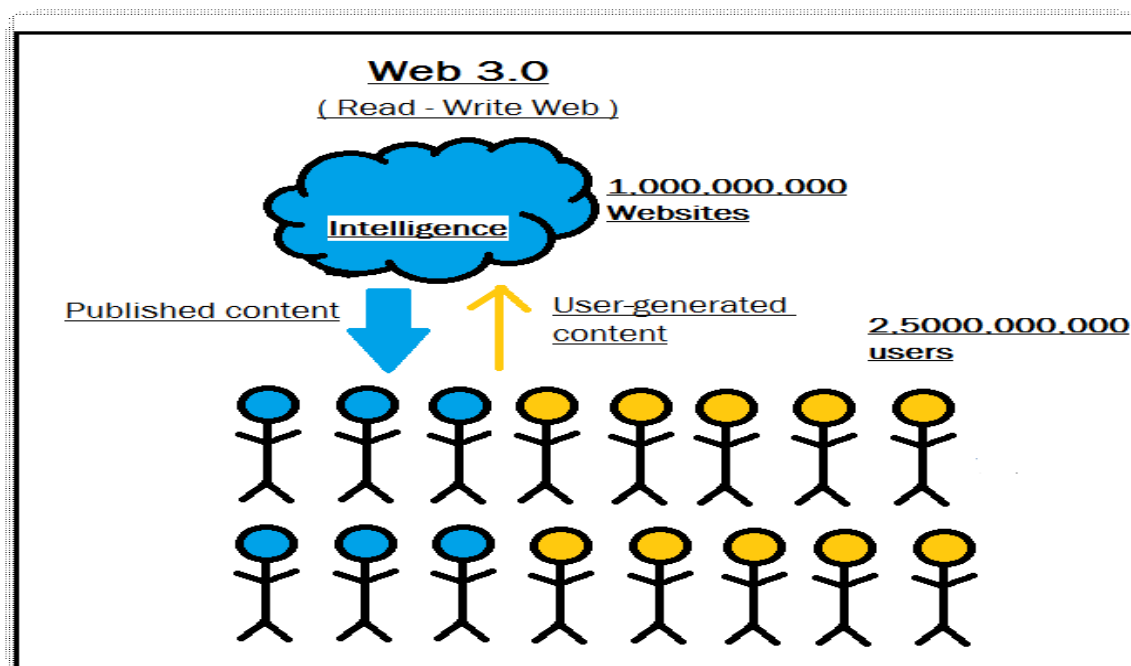
Web2.0时代



1.4 从Web1.0到Web3.0，从用户只读到用户拥有

- ◆ Web3.0最早是由以太坊联合创始人、Polkadot创始人Gavin Wood在2014年提出。
- ◆ Web3.0是一组包容性协议，为应用程序制造商提供构建块。这些构建块取代了传统的 Web 技术，如 HTTP，AJAX，MySQL，提供了一种创建应用程序的全新模式。这些技术为用户提供了强大且可验证的保证，从而保证了他们接收信息和提供信息的安全性，以及让他们的信息得以保密。
- ◆ Web3.0是价值互联网。内容由用户创造，数据归用户所有，每个人都能掌握自己的（数字）身份、资产和数据。

Web3.0时代





02 Web3.0的特性与典型应用

2.1 Web 1.0/2.0/3.0的主要区别汇总

- ◆ **Web 3.0的核心区别是区块链带来的N中心效应，用户对ID、内容、数据拥有自主权。**将生产和所有权交还给用户，而不是由互联网平台或者控制互联网平台公司的少数人拥有。**用户不仅具有对数据的所有权，还能参与规则制定和组织治理。**
- ◆ **Web 1.0/2.0时代数据存储在统一的服务器上，服务厂商可以决定数据的删减去留；Web 3.0时代的数据是存储于去中心化的区块链上，具有不可篡改、集体维护、规则透明的特点。**

Web 1.0/2.0/3.0的主要区别

互联网时代	 Web1.0	 Web2.0	 Web3.0
定位	• 门户互联网	• 平台互联网	• 用户互联网
中心	• 1个中心：网站	• 1个中心：平台	• N个中心：用户
内容传输	• 单向信息输出	• 双向信息交互	• 信息聚联与价值共享
ID模式	• 无数字身份	• 基于平台账户的数字身份	• 用户自主的数字身份
用户角色	• 内容消费者	• 内容生产者	• 内容拥有者
数据形态	• 无个人数据概念	• 个人数据缺乏自主权 • 算法被平台把控	• 数据用户自主 • 算法用户自主

2.2.1 Web1.0：中心化、只读模式

- ◆ **Web1.0是只读模式的网络，是静态的、单向的网络。**用户只能被动地浏览文本、图片及视频内容，网站提供什么，用户查看什么，几乎没有互动。
- ◆ **Web1.0基本采用的是技术创新主导模式，信息技术的变革和使用对于网站的产生与发展起到了关键性的作用。**新浪最初就是以技术平台起家，搜狐以搜索技术起家，腾讯以即时通讯技术起家，盛大以网络游戏起家，在这些网站的创始阶段，技术性的痕迹相当之重。
- ◆ **Web1.0的盈利都基于一个共通点，即巨大的点击流量。**无论是早期融资还是后期获利，依托的都是为数众多的用户和点击率，以点击率为基础上市或开展增值服务，受众群体的多少，决定了盈利的水平和速度。

Web1.0时代网站



2.2.1 Web1.0 : 中心化、只读模式

- ◆ **Web1.0的发展出现了向综合门户合流现象**，早期的新浪与搜狐、网易等，继续坚持了门户网站的道路，后来的腾讯、MSN、GOOGLE等，都纷纷走向了门户网站，尤其是对于新闻信息有着极大的、共同的兴趣。这一情况的出现，在于门户网站本身的盈利空间更加广阔，盈利方式更加多元化，占据网站平台，可以更加有效地实现增值意图，并延伸出主营业务之外的各类服务。
- ◆ **Web1.0的合流同时，还形成了主营与兼营结合的明晰产业结构**。新浪以新闻+广告为主，网易拓展游戏，搜狐延伸门户矩阵，各家以主营作为突破口，以兼营作为补充点，形成组合发展方式。
- ◆ **Web1.0的主要协议是HTTP, HTML 和 URI。**

Web1.0特点



2.2.2 Web1.0的典型应用: 浏览器与电子商务

- ◆ **Web1.0的理念:** Web1.0是只读模式的网络,是静态的、单向的网络,多数参与者是内容消费者,而创造者大多是网络开发者,且数据和内容来自静态文件系统而不是数据库,而且网页上的互动性有限。典型应用如下:
 - ✓ **浏览器:** 万维网 (WWW) 的诞生和商业化浪潮,推动着互联网走向大众,以浏览器为首的Web1.0应用显现于大众视野,代表公司为谷歌、雅虎、新浪等。
 - ✓ **电子商务:** 是传统商业活动各环节的电子化、网络化,许多公司将自己将电子商务的功能增加到网站上,例如连锁超级市场Albertsons和Safeway都开始了附属的电子商务功能,消费者可以直接在线订购食品;阿里巴巴也开始设立小型企业的电子商务网站。

1997年的Google搜索引擎界面



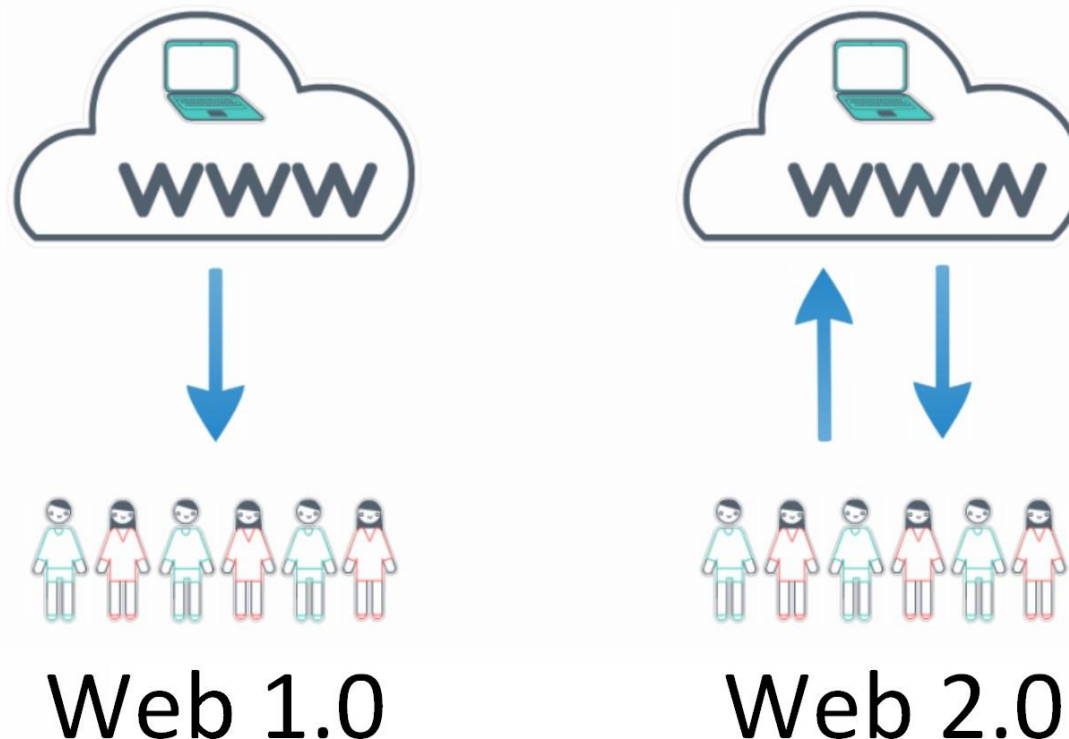
早期的阿里巴巴商务网站



2.3.1 Web2.0 : 中心化、读写交互模式

- ◆ **Web2.0让用户参与网站内容制造。**与Web1.0网站单向信息发布的模式不同，Web2.0网站的内容通常是用户发布的，使得用户既是网站内容的浏览者也是网站内容的制造者，这也就意味着Web2.0网站为用户提供了更多参与的机会。
- ◆ **Web2.0更加注重交互性。**不仅用户在发布内容过程中实现与网络服务器之间交互，而且，也实现了同一网站不同用户之间的交互，以及不同网站之间信息的交互。
- ◆ **Web2.0 网站与 Web1.0 没有绝对的界限。**Web2.0技术可以成为Web1.0网站的工具，一些在Web2.0概念之前诞生的网站本身也具有Web2.0特性，例如B2B电子商务网站的免费信息发布和网络社区类网站的内容也来源于用户。

Web2.0与Web1.0区别



2.3.1 Web2.0 : 中心化、读写交互模式

- ◆ **Web2.0是符合Web标准的网站设计。**Web标准中典型的应用模式是“CSS+XHTML”，摒弃了HTML4.0中的表格定位方式，其优点之一是网站设计代码规范，并且减少了大量代码，减少网络带宽资源浪费，加快了网站访问速度。更重要的一点是，符合Web标准的网站对于用户和搜索引擎更加友好。
- ◆ **Web2.0是互联网的一次理念和思想体系的升级换代，**由原来的自上而下的由少数资源控制者集中控制主导的互联网体系，转变为自下而上的由广大用户集体智慧和力量主导的互联网体系。
- ◆ **Web2.0的平台是专有的、封闭的，属于某个互联网公司的。**虽然用户通常可以免费使用它们，但用户自身并未真正拥有这些平台上的用户数据。

Web2.0应用产品



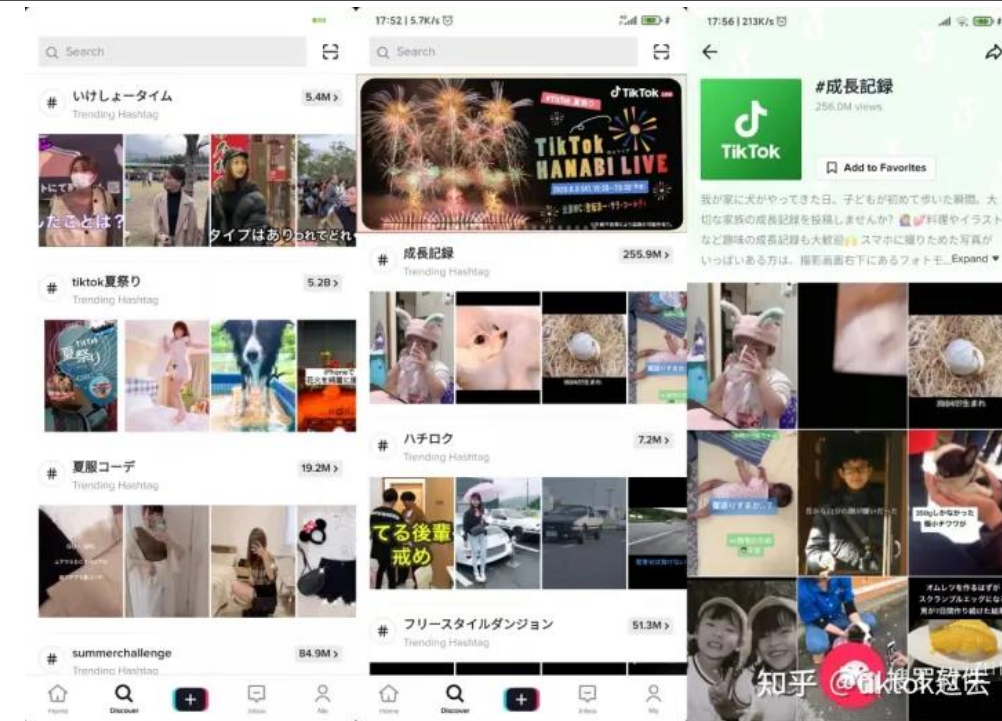
2.3.2 Web2.0的典型应用: 社交媒体、短视频平台

- ◆ **Web2.0的理念:** Web2.0让用户参与网站内容制造，且更加注重交互性，同一网站的不同用户之间可以交互，是自下而上的由广大用户集体智慧为主导的互联网体系。**从应用来说Web2.0分为两个时间点段：**
- ◆ **Web2.0初期:** 此时的应用主要是博客、社交媒体等兴起，网民成为内容的生产主体，此时的代表应用为MSN、QQ、博客等，**此时更注重用户之间的内容交互。**
- ◆ **Web2.0移动互联时代:** 随着智能手机全面崛起，移动互联网成为全球互联网新一轮扩散的主力军，更加深入地改变着人们的日常生活。代表产品为INS、Facebook、Youtube、微信、抖音、微博、等产品，**用户更关注交互体验。**

2006年的QQ应用



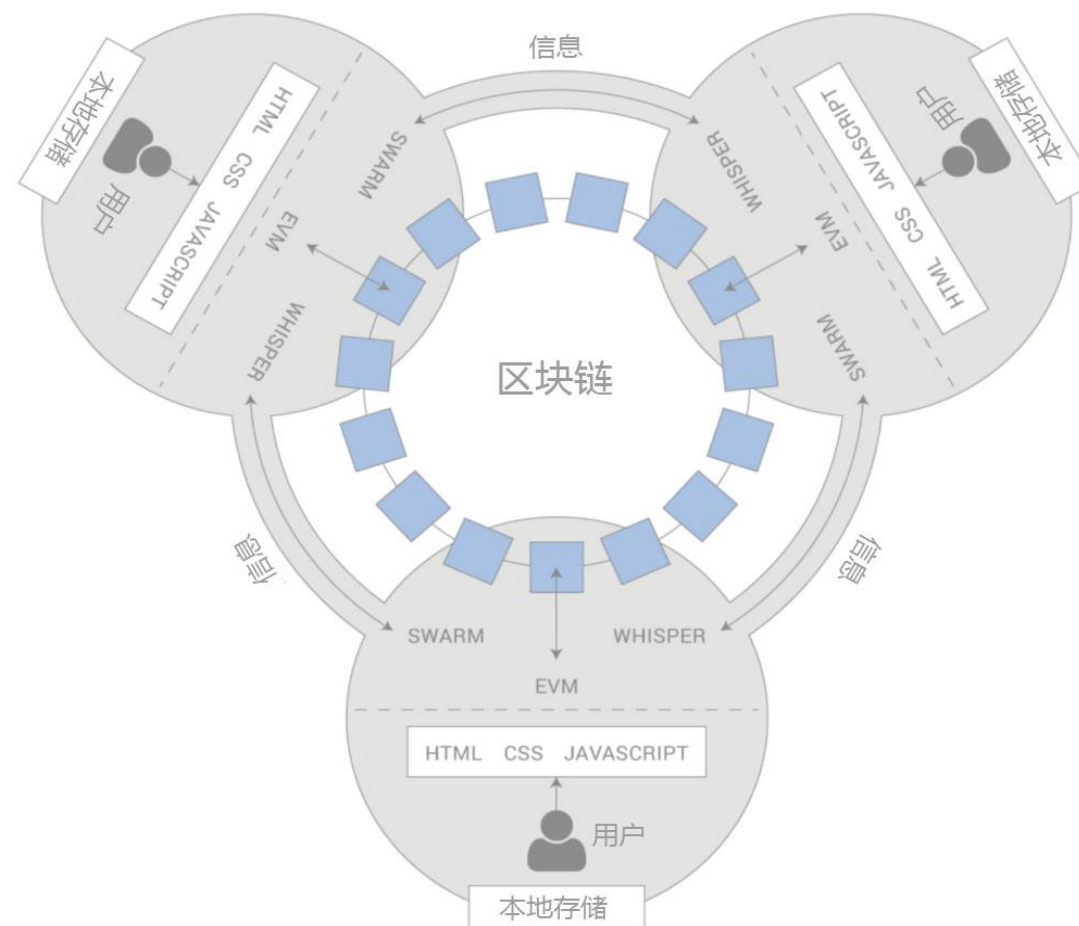
TikTok的分享生活应用



2.4.1 Web3.0 : 开放、隐私、共建

- ◆ **Web3.0具备开放性。**用户在某个互联网应用“领域”中的准入充分自由、门槛低；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。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。
- ◆ **Web3.0具备隐私性。**数据所有权归用户所有，价值转移不需要第三方授权。
- ◆ **Web3.0具备共建性。**用户在Web2.0互联网应用中的内容创造是在受平台审核限制、跨平台限制等多方面受限的，尤其在社区治理方面，限制更多，所以就限制了用户在创作者经济共享方面的价值捕获。Web3.0有望打破限制，区块链的代币激励机制有效反馈内容经济的价值给创作者。

Web3.0可以“跨链”与“跨协议”



2.4.2 Web3.0：专注语义网络，连接知识，转向用户授权

- ◆ Web2.0是一种参与式社交网络，或支持读写功能的第二代互联网服务。**Web3.0**是第三代网络，专注于语义网络，专注于在去中心化的基础设施上实现用户和机器之间更好的沟通和理解。
- ✓ **语义网络**：Web2.0专注于使用户能够与互联网上的内容进行交互。**Web3.0** 主要想促进用户对互联网内容的沉浸。
- ✓ **连接知识**：Web2.0旨在连接人，而**Web 3.0** 旨在连接知识。
- ✓ **用户授权**：Web2.0的重点主要反映在标记和最终用户体验上。Web 3.0通过促进提高信任度、安全性和隐私性，**将重点转向了用户授权**。
- ✓ **个人发展**：Web2.0侧重于社区发展，而**Web3.0**则侧重于个人发展。

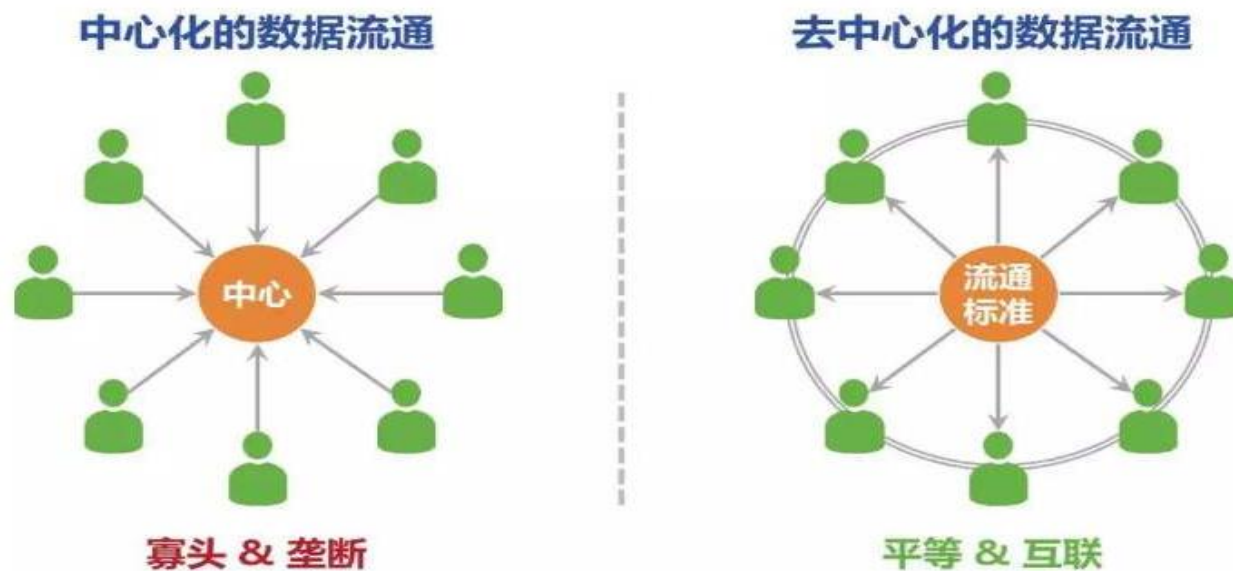
Web3.0与Web2.0区别



2.4.3 Web3.0 : 基于人工智能技术实现虚拟环境等应用

- ◆ **技术方面**：Web 2.0 技术包括 AJAX 和 JavaScript。此外，CSS3 和 HTML5 在支持 Web 2.0 的技术中也占据了主导地位。Web 3.0 为创新技术的实施提供了支持。支撑 Web 3.0 基础的主要技术包括**人工智能、语义网和去中心化协议**。
- ◆ **应用方面**：Web 2.0 应用程序的一些示例包括双向网页、视频网站、微博和个人博客。相反，Web 3.0 通过利用 ML 和 AI 功能增强了智能应用程序的增长，Web 3.0 应用程序的显着示例可能包括多用户**虚拟环境、3D 门户和集成游戏**。

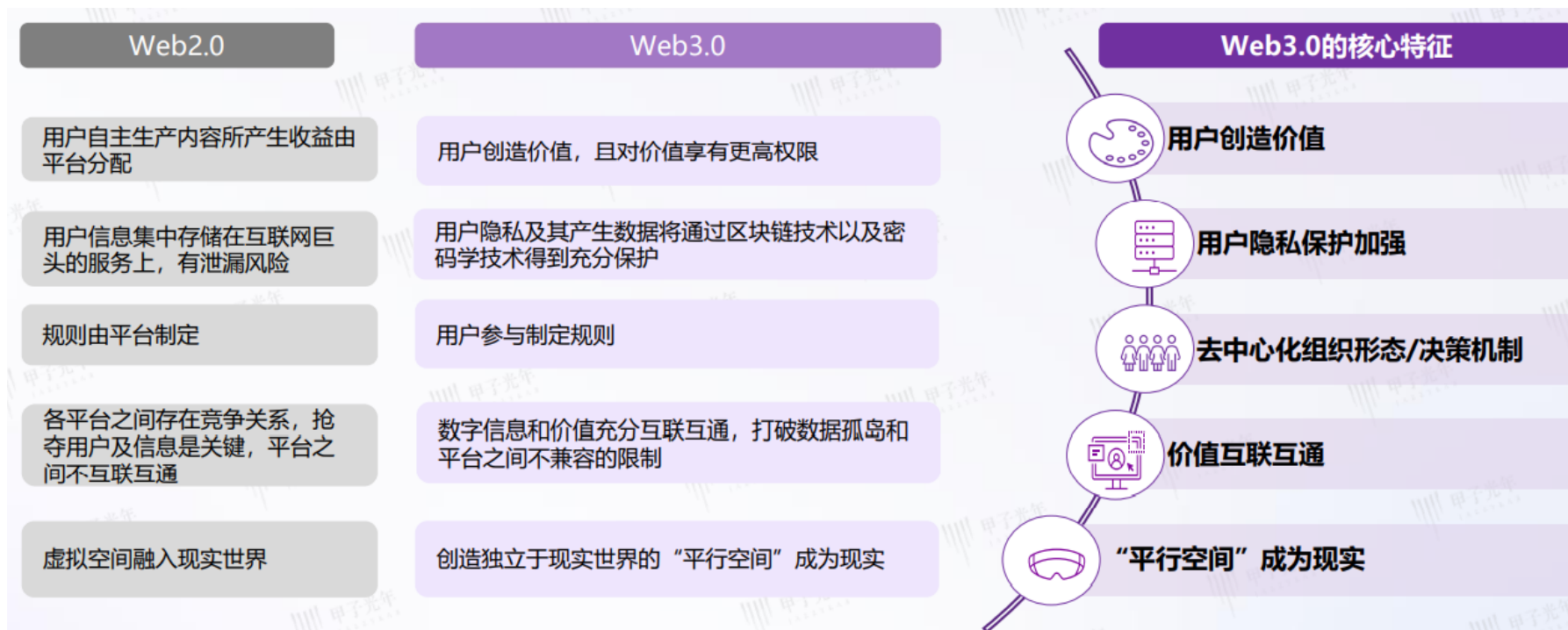
Web3.0去中心化



2.4.4 Web3.0：核心特征汇总

- ◆ 基于区块链分布式技术，**Web3.0用户权利提升，用户责任增大，实现更大程度上的用户“权责对等”**：
 - ✓ 用户之间的信息交互种类及内容更多，同时交易过的痕迹将被保留。
 - ✓ 用户对平台拥有更高的权限，同时承担整个平台的被信任程度。
 - ✓ 用户数据资产的权利逐步得到保障，同时承担数据资产的价格变化。
- ◆ Web3.0是一个用户共建、隐私保护、平台开放的生态体系。用户具有拥有权，具有参与项目治理的权利，从而实现了价值生成和价值确权。

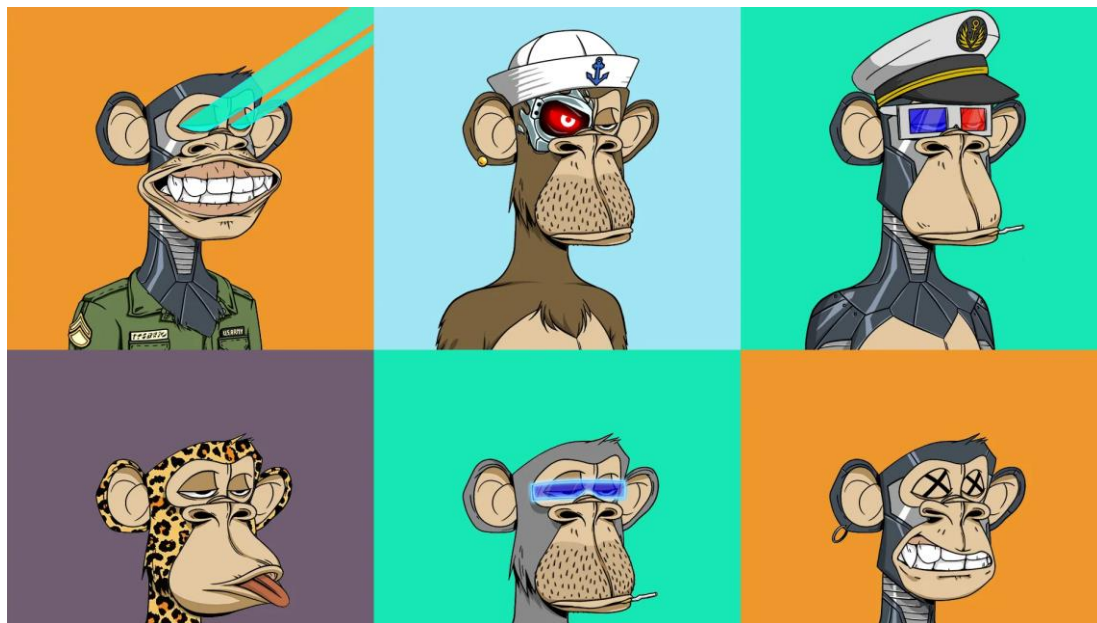
Web3.0核心特征



2.4.5 Web3.0的典型应用: 虚拟货币、NFT

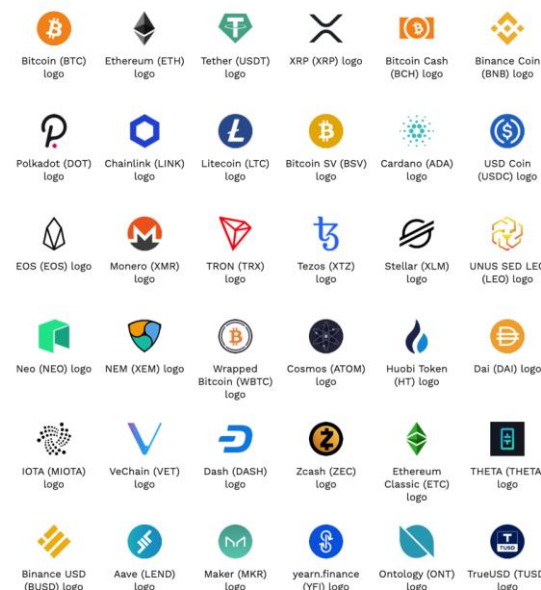
- ◆ **Web3.0的理念:** Web3.0具备开放性、隐私性和共建性，其核心的设计理念是用户可以创造价值、去中心化的组织形态和决策机制、价值互联互通，进而实现“平行空间”。目前阶段的典型应用如下：
- ◆ **虚拟货币:** Web3.0设计理念之一就是拥有独特的经济系统、生态系统，从而再虚拟的世界里衍生出完整的经济体系，该体系不需要管理者，而是通过自己的激励机制维护运行，而虚拟货币就是其独特的激励机制，其目的是通过“矿工”来维持该体系的平稳运行，例如比特币、以太坊、LUNA、泰达币、USDC、BUSD等。
- ◆ **NFT:** 是一种被称为区块链数字账本上的数据单位，例如画作、艺术品、声音、视频或其他形式创意作品。每个NFT可以代表一个独特的数字资料。由于Web3.0独特性质，NFT拥有独自の“商标”，原因是这些代表它们的代币在其底层区块链上能被完整追踪，故能为买家提供所有权证明。目前部分NFT作为数字资产底本供商业使用。

NFT Monkey



资料来源：公开资料整理、华西证券研究所整理

虚拟货币图示



2.4.6 Web3.0的终极设想: 元宇宙

- ◆ **元宇宙的理念和Web3.0的理念具有异曲同工之妙：**元宇宙的理念为平行于现实世界、拥有完整社会经济系统的虚拟世界，而Web3.0则为用户提供用户共建、隐私保护、平台开放的生态体系。目前Web3.0可以通过用户自己的区块链钱包进行登录，进行NFT交易与币币兑换，我们认为未来Web3.0的相关体系可以应用在元宇宙中。
- ◆ **我们认为Web3.0符合元宇宙的设计理念：**例如电影《头号玩家》中未来人们世界的人们通过AR/VR硬件设备进入“绿洲”虚拟世界，绿洲中的货币与现实世界货币拥有官方互换渠道。在这个虚拟世界里，有完整运行的经济、货物、内容以及 IP ，用户和公司可以进行内容创作，商品交易，实现生活中的绝大部分活动

《头号玩家》中男主



《头号玩家》绿洲中的娱乐场所



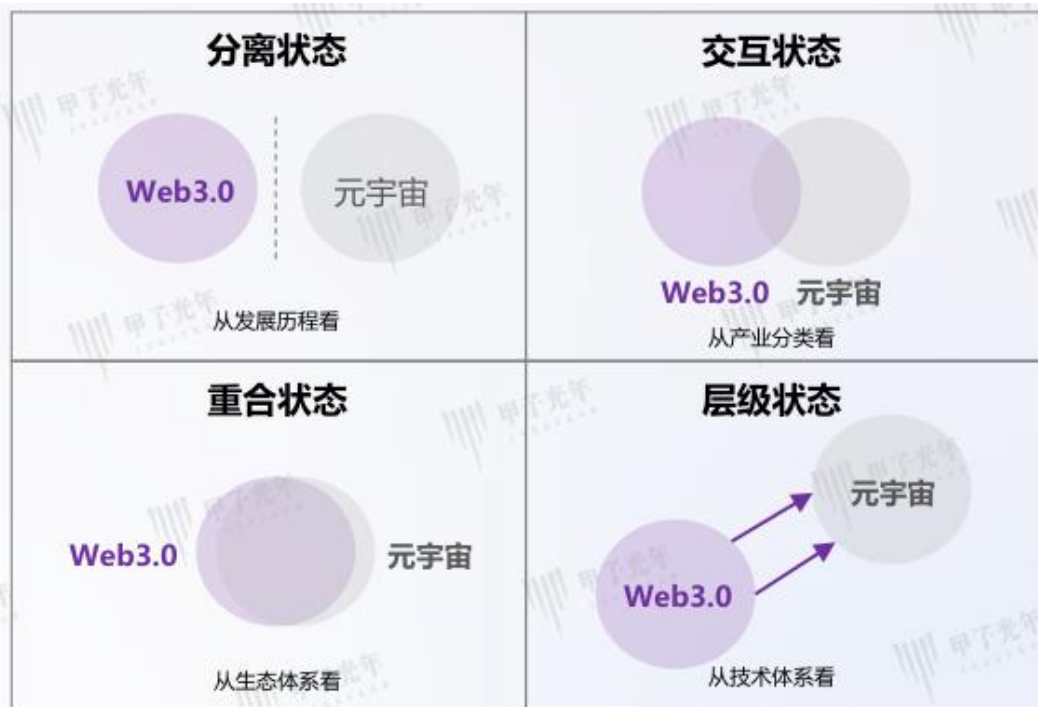


03 Web3.0的底层技术架构

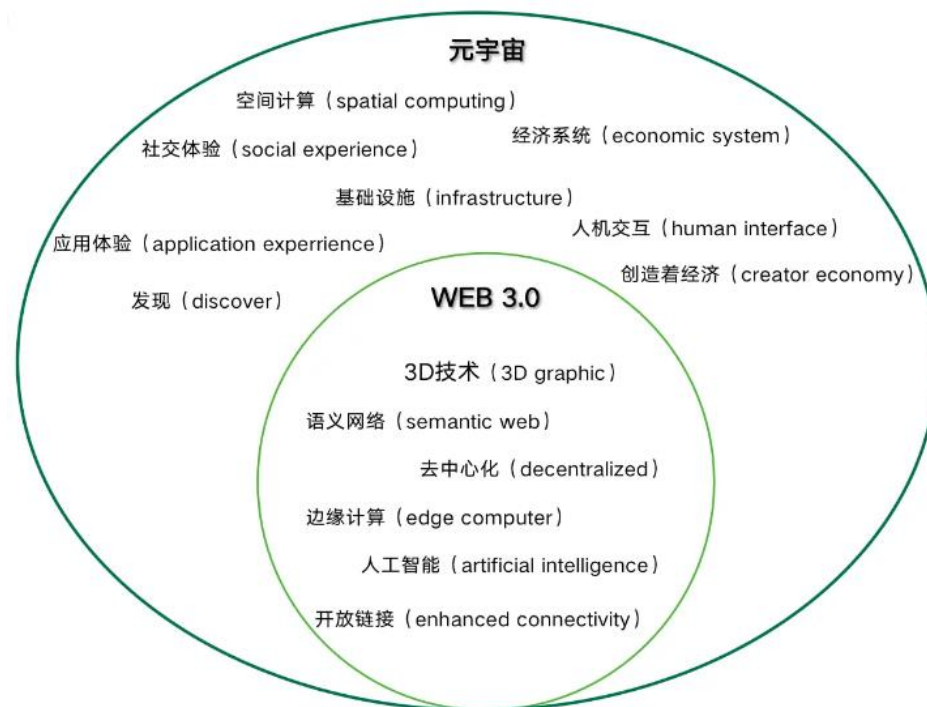
3.1 Web3.0与元宇宙是一体两面的关系

- ◆ **元宇宙是上层建筑，Web3.0是基础设施**：**Web3.0和元宇宙均代表互联网的未来，Web3.0代表的是技术发展方向**，而元宇宙代表了未来应用场景和生活方式，两者相辅相成，呈现一体两面的关系。
- ✓ **Web3.0技术与核心特征**：Web3.0是元宇宙的底座，技术包括区块链、人工智能、大数据等技术和用户共识社区(DAO)等，核心特征为用户隐私保护能力加强、去中心化组织形态、价值互联互通、“平行空间”成为现实。
- ✓ **元宇宙技术与核心特征**：在Web3.0技术基础上更叠加AR、VR等技术，特征为沉浸式体验、数字身份、经济系统、虚拟社会治理等，其中数字身份、虚拟社会治理、经济系统需要Web3.0的技术加持。

Web3.0和元宇宙关系图解



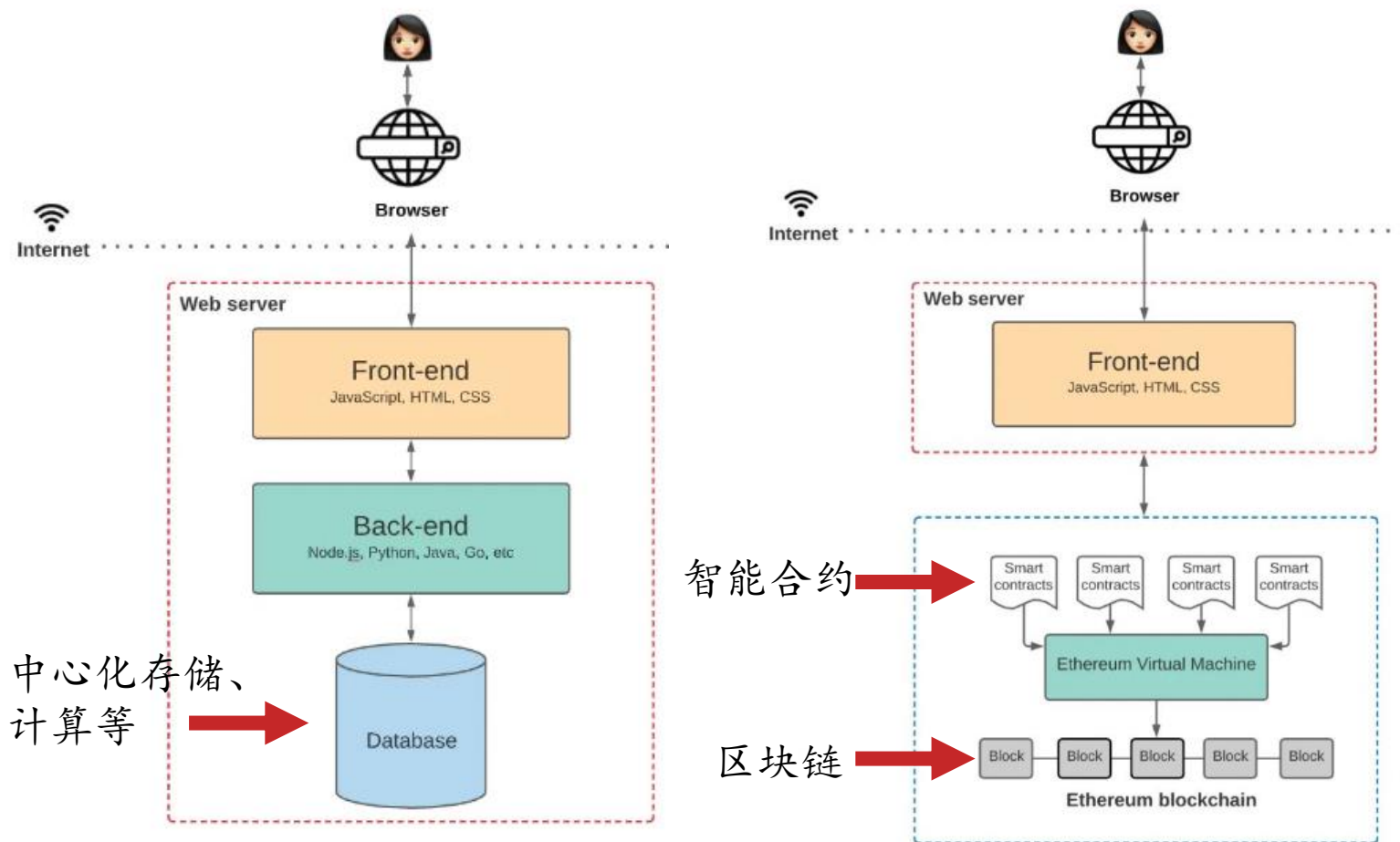
Web3.0和元宇宙技术框架



3.2 Web3.0与Web2.0系统架构区别

- ◆ **Web3.0的打破传统Web2.0的思维理念：**
 - ✓ **Web3.0的设计理念为：**1、成员之间相互平等，并且完全民主；2、集体决策；3、代码自动执行、不需要中间人即可自动执行；4、提供去中心化的服务；5、基于区块链的底层逻辑，所有活动公开透明。
 - ✓ **Web2.0目前存在问题：**1、上下层级明确；2、选择经过人工处理；3、集中控制理念较强，结果容易篡改、4、部分活动秘密进行。
- ◆ **Web3.0技术架构具有颠覆性，拥有不可篡改、集体维护、规则透明的特点：**
 - ✓ **核心差别1, 区块链：**Web3.0的数据存储主要集中在区块链上，应用程序具有去中心化的能力，而Web2.0的数据存储主要集中在服务器中。
 - ◆ **核心差别2, 智能合约：**智能合约是程序代码的载体，智能合约运行在以太坊的虚拟机上，是一种自动执行程序，无需中间人参与，满足条件自动触发。

Web3.0系统技术架构与2.0系统架构的核心差异(左图为Web2.0，右图为3.0)



3.3 Web3.0生态场景与技术支持

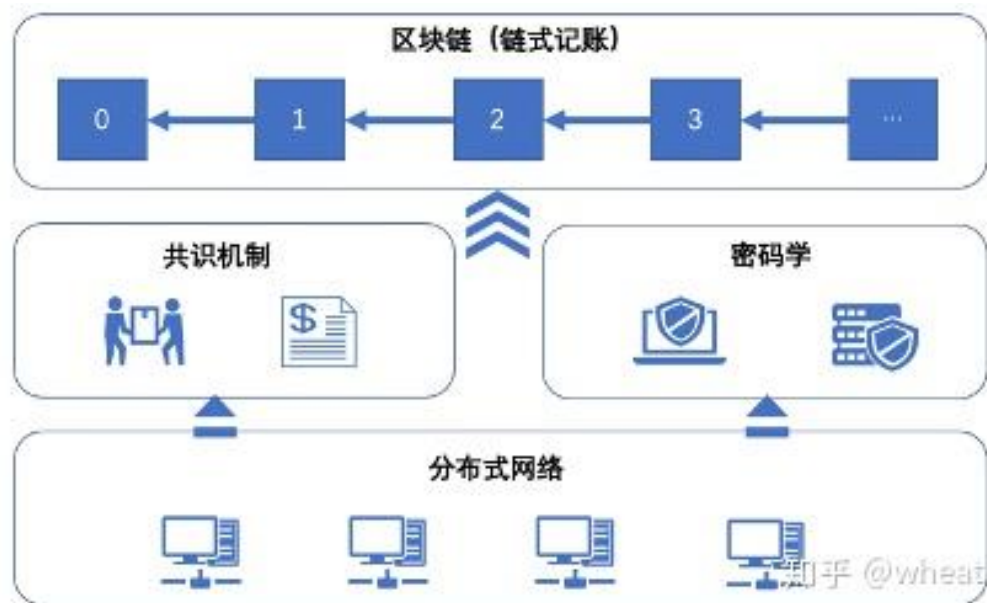
Web3.0与Web2.0技术和场景差异

层级	Web2.0	Web3.0	相关技术
应用层	...	...	...
	支付方式:电子支付、信用卡支付 如Paypal、支付宝等	支付方式:数字货币、例如比特币、 NFT等	数字货币相关技术
交互层	存储:云存储等	存储、分布式存储如IPFS等	分布式存储技术
	数据库:关系型数据库如Mysql、 Oracle等	数据库:非结构化去中心数据库, 例如GUN	分布式数据库技术
协议层	安全保障:用户名+密码	安全管理:隐私计算、公匙加密等 技术	隐私计算、密码学等技 术
	一致性逻辑:服务器程序例如php、 java、c++等	一致性逻辑:智能合约	智能合约、AI等技术
基础设施和 网络层	传输协议:例如 http/https/ftp/smtp	传输协议:例如P2P、EVM、UTXOs、 WASM	区块链技术
	域名:中心化DNS	域名:去中心化DNS例如ENS、 Namercoin等	区块链技术

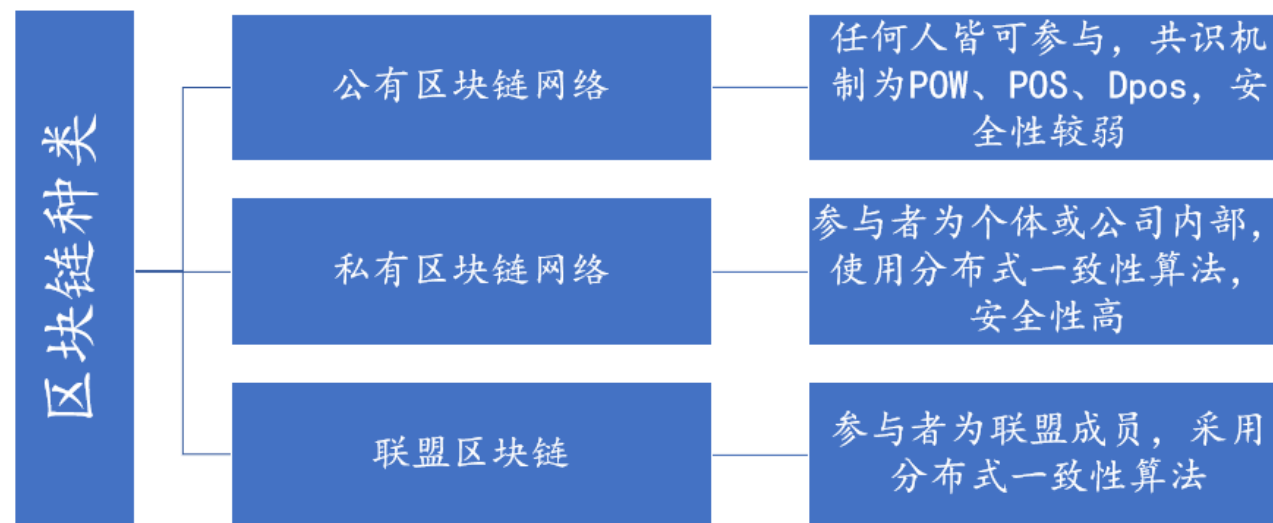
3.4.1 区块链技术是Web3.0的核心技术

- ◆ **区块链技术是实现Web3.0的核心前提**：区块链技术是一种高级数据库机制，允许在企业网络中透明地共享信息。区块链通过链式记账法，将数据存储链式记账中，数据库则连接到一个链条中。由于数据在链条的时间上是一致的，因此无法删除或者修改，具有一致性。
- ✓ **区块链特点**：1、**去中心化**：将控制权从中心实体转让给分布式网络；2、**不可变性**：任何参与者不得篡改交易；3、**共识**：有且只有参与者就交易达成共识，才能记录新交易。
- ✓ **区块链工作机制**：1、记录交易→2、达成共识→3、区块链串联→4、共享记账。
- ✓ **区块链核心组件**：1、共识机制(智能合约)、2、密码学(公匙加密等)、3、分布式网络包括分布式存储和分布式数据库等。

区块链示意图



区块链的种类



3.4.2 智能合约是Web3.0在区块链上的载体

- ◆ **智能合约是Web3.0在区块链上的载体：**智能合约是存储在区块链的程序，通常用于自动执行协议，无需中间人参与，及时触发。

◆ 智能合约与传统合约的差异：

- ✓ **传统合约：**双方合作必须通过第三方机构接入，如果有乙方违反条约，需要第三方机构判决，在应用方的表现如APP，需要中心化的服务器。
- ✓ **智能合约：**双方合作线上签署合约，合约为区块链上的代码存储在公共资料中，且不能被篡改，合约被强制执行，在应用方的表现为Dapp，具有去中心化、数据不可篡改、公开透明的特点。

◆ 智能合约的特点与优点：

- ✓ **特点：**1、**自治：**无需任何人干预；2、**自足：**可以自主调配计算所需要资源；3、**去中心化：**通过分按时节点自动运行，不用通过中心化的服务器。
- ✓ **优点：**1、兼具合约执行速度、效率、和精准度；2、由于没有第三方参与，具备信任度和透明度；3、安全性极高，由于区块链交易经过加密，因此很难破解。

智能合约和传统合约的差异化



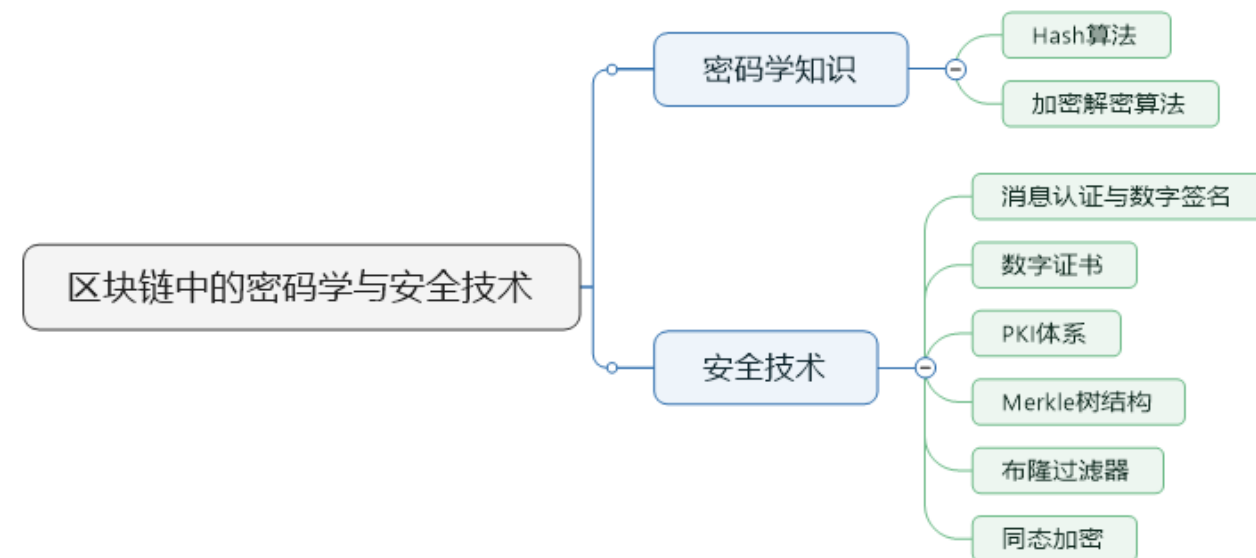
3.4.3 密码学为区块链和Web3.0保驾护航

- ◆ **Web3.0与密码学紧密相连**：密码学是区块链技术的核心组成部分，每一个新的区块链都需要一个核心算法，例如比特币的Pow算法利用Hash函数。
- ◆ **密码学为Web3.0和区块链保驾护航**：密码学主要作用为加密、认证、试别，其主要作用防止恶意篡改数据、恶意读取数据等，可用于网络安全协议、数字证书、电子支付、隐私保护、地址生成等方向，在区块链技术中，应用极其广阔。在区块链中主要使用的密码学算法为：
 - ✓ **Hash算法**：可以将数据转换为标志，且标志和源数据对每个字节关系紧密，其中，比特币系统中使用Hash函数，用于比特币地址生成、身份识别和消息认证。
 - ✓ **对称密码算法**：指加密和解密使用相同密钥的加密算法，可以用于比特币钱包的私钥加密，确保私钥的安全，在区块链的主要使用算法为分组加密和序列加密。
 - ✓ **非对称加密算法**：需要两个密钥，公钥负责加密，私钥负责解密，可实现数字证书、身分认证等功能，通过此算法，可以形成信任链架构，比特币中使用算法为ECDSA算法。

密码学算法在WEB3.0和区块链的应用

算法类型		特点	优点	缺点	代表算法
Hash算法		将数据转换成标志,标志和源数据的字节关系紧密	计算效率高、编程较为容易	受数据结构影响较大	MD5-1、SHA-1
加密解密算法	对称加密	加解密的密钥相同	计算效率高、加密强度高	需要提前共享密钥、易泄露	DES、3DES、AES、IDEA
	非对称加密	加解密的密钥不相关	无需提前共享密钥	计算效率低	RSA、椭圆去线系列算法

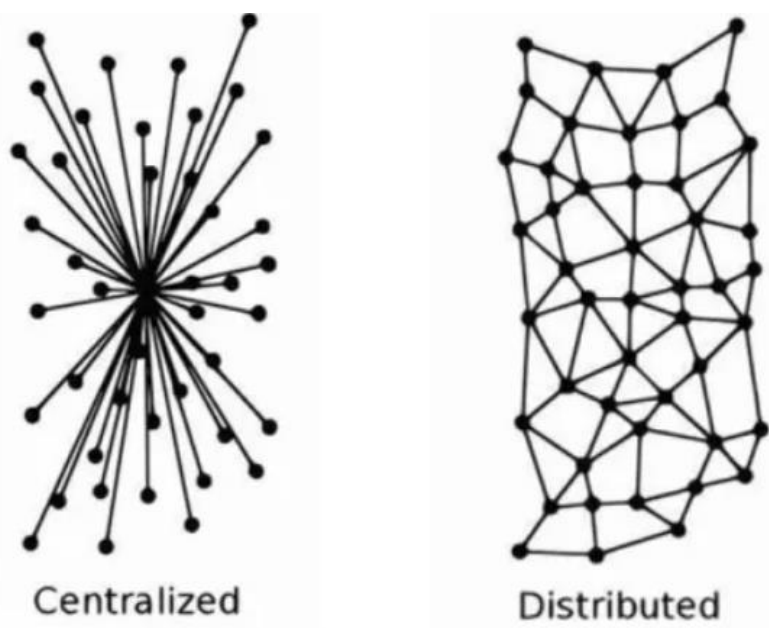
区块链中的密码学与安全技术



3.4.4 分布式存储为Web3.0提供底层技术支持

- ◆ **分布式存储是Web3.0的数据存储层：** 分布式存储为Web3.0提供底层技术支持。在Web3.0的应用中，用户交互、身份认证等都需要去中心化的方式进行存储。分布式存储的特性在于高拓展、易运维、效率高，更符合Web3.0的减少中心化巨头的垄断、将个人价值发挥到最大程度的理念。其中，IPFS是实现分布式存储的技术路径之一，具有去中心化、用户共建、价值激励等特性。
- ◆ **去中心化存储相比于中心化存储优势明显：** 1、**存储成本低：**去中心化存储是把数据分布到多个网络节点，类似分布式账本技术；2、**安全性较高：**去中心化存储数据被切割成若干小块，且加密后分散在众多节点，可以避免集中式数据泄露的风险。3、**存储费用较低：**在检索量较少的情况下，去中心化存储中的冷数据存储费用比中心化存储要低很多。

分布式存储与中心化存储示意图(右图为分布式)



分布式存储和中心化存储的对比

方向	去中心化存储	中心化存储
存储空间	节点存储	云端存储
存储费用	分类付费	定期付费
安全保护	分散存储	集中存储
发展程度	发展中	成熟期

3.4.5 分布式数据库是Web3.0和分布式存储的基石

- ◆ **数据库和存储属于相互依存的关系：**存储是一个以数据存储和管理为核心的系统，而数据库为存储数据的文件，是长期存储在计算机内、有组织、可共享、统一管理的大量数据的集合，然而数据库文件最后需要存储在本地硬盘当中，所以两者相互依赖。
- ◆ **分布式数据库更符合Web3.0的理念，其特征和优势如下：**
 - ✓ **低延时：**去中心化的数据库在网络上存在多个副本，网络的每个节点都会保存数据库，分散在全球各地，客户可以访问最快的节点实现低延时；
 - ✓ **数据安全性高：**去中心化数据库由于其特性避免了集中式数据泄露的风险，如果某一节点遭受攻击，全球范围内的信息不会受到影响。
 - ✓ **数据稳定：**由于分布式架构的特性，当单个节点出现故障时，不会影响整个网络。
 - ✓ 目前随着去中心化的吸引力和Web3.0的强势崛起，部分海外数据厂商正在围绕相关技术创立项目，例如BigchainDB、HarperDB、CovenantSQL。

Bigchain 分布式数据库的功能和用例



权力下放

没有单点控制。没有单点故障。通过投票节点联盟的分散控制构成了 P2P 网络。



询问

编写并运行任何 MongoDB 查询来搜索所有存储的交易、资产、元数据和块的内容。由 MongoDB 本身提供支持。



不变性

不仅仅是防篡改。一旦存储，数据将无法更改或删除。



多资产的原生支持

在 BigchainDB 上没有原生货币的情况下，可以发行任何资产、代币或货币。



拜占庭容错 (BFT)

网络中多达三分之一的节点可能会遇到任意故障，而网络的其余部分仍将就下一个区块达成共识。



低延迟

全球网络大约需要一秒钟才能就新区块达成共识。换句话说，交易终结性发生得很快。



可定制

使用自定义资产、交易、权限和透明度设计您自己的专用网络。



丰富的权限

在事务级别设置权限，以确保职责明确分离并强制执行选择性访问。



开源

对社区开源，以便每个人都可以使用它并在其上构建自己的应用程序。



公共或私人

针对特定行业用例推出您自己的公共或专用网络。



04 投资建议

投资建议: 梳理Web3.0的受益厂商

- ◆ 我们认为Web3.0致力打造一个基于区块链技术、用户主导、去中心化的网络生态，未来Web3.0将为互联网时代带来更好的体验和更高的用户权限，积极的推荐以下三条投资主线：
 - ✓ 1)具备密码学能力的相关厂商，受益标的为**卫士通、信安世纪**；
 - ✓ 2)具备分布式数据架构能力的厂商，受益标的为：**海量数据、星环科技**；
 - ✓ 3)具备区块链能力的应用厂商，受益标的为**四方精创、荣联科技、京北方、东方国信、蓝色光标、榕基软件、天地在线、福石控股、天娱数科、二六三、三湘印象**等。

Web3.0的A股受益标的

公司名称	股票代码	收盘价	市值(亿元)	EPS (元)			PE (倍)		
		2022/11/11	2022/11/11	2021	2022E	2023E	2021	2022E	2023E
卫士通	002268. SZ	35.91	303.75	0.28	0.47	0.71	127.7	75.8	50.9
信安世纪	688201. SH	56.67	78.11	1.81	1.40	1.82	31.4	40.6	31.1
海量数据	603138. SH	23.20	65.69	0.04	0.03	0.05	580.0	722.7	425.7
星环科技	688031. SH	79.40	95.95	-2.70	-1.68	-0.89	-	-	-
四方精创	300468. SZ	11.49	60.97	0.24	-	-	47.9	-	-
荣联科技	002642. SZ	9.76	64.89	0.08	0.00	0.00	115.9	-	-
京北方	002987. SZ	30.85	97.15	1.03	0.93	1.26	30.0	33.2	24.5
东方国信	300166. SZ	8.95	103.14	0.27	0.28	0.37	33.1	32.3	24.0
榕基软件	002474. SZ	9.23	57.43	0.05	-	-	191.9	-	-
天地在线	002995. SZ	35.96	45.58	0.60	-	-	60.2	-	-
福石控股	300071. SZ	4.38	40.40	0.25	-	-	17.5	-	-
天娱数科	002354. SZ	4.75	78.59	0.03	0.01	0.03	184.8	633.3	175.9
二六三	002467. SZ	5.47	74.86	0.02	0.06	0.07	273.5	93.0	73.6
三湘印象	000863. SZ	4.40	52.99	0.10	-	-	44.0	-	-

注：盈利预测均来自WIND一致预期

资料来源：华西证券研究所

4.2.1 密码领域的传统龙头: 卫士通

- ◆ **卫士通是密码领域的传统龙头**: 卫士通成立于1998年, 是中国电子的控股子公司, 在加密认证类产品市场长期保持领先。公司业务横跨网络安全、主机安全、数据安全、应用安全等多个场景。
- ✓ **卫士通密码产品齐全, 且产品范围较广**: 公司密码覆盖从算法、芯片、模块、板卡、整机到系统的全产业链, 产品功能从密码算法、数据加解密、认证鉴别、证书管理、密钥管理、密码防伪到密码综合应用。
- ✓ **公司积极布局新兴领域**: 公司内部设立密码创新中心, 开展卫星互联网、北斗、密码态势感知、数字货币、可信身份等新场景新技术领域的密码应用研究, 增强公司在同态加密、多方计算、可搜索加密、区块链等前沿密码算法方面的技术积累

卫士通部分密码产品

金融数据密码机

金融数据密码机是由卫士通自主研制, 通过国家主管部门鉴定的安全密码设备, 为金融业务系统提供数据机密性、数据完整性、

服务器密码机

服务器密码机具有数据加解密、签名、验签、MAC、杂凑等功能, 支持SM1/SM2/SM3/SM4/SM9及ZUC国密算法, 可为用户

数字证书认证系统

数字证书认证系统是卫士通研制的一套公钥基础设施解决方案。系统基于PKI关键技术, 实现了用户注册、审核, 密钥产生、分

移动终端密码软卡

移动终端密码软卡| 产品特色安全性高● SM2 签名私钥分割、混淆, 协同签名计算时私钥不会出现在内存中

密钥管理系统

密钥管理系统是依据国家及行业相关标准规范研制的安全基础设施产品, 使用经国家密码管理局批准的密码设备, 支持

商用PCI-E密码卡

商用PCI-E密码卡是由卫士通自主研制的安全密码产品, 该密码卡支持国家密码管理局发布的SM1/2/3/4算法, 通常嵌入服务器

签名验证服务器

签名验签服务器是卫士通依据国密局、工信部、公安部等主管单位的相关标准规范, 自主研发的新一代数字签名服务器。

4.2.2 密码领域的小巨人: 信安世纪

- ◆ **信安世纪以密码学为抓手，致力于解决网络安全：**公司目前基于密码安全领域已经拓展到网络安全领域，公司形成了身份安全、通信安全、数据安全、移动安全、云安全和平台安全六大产品系列；此外，公司密码产品包括数字证书认证系统、动态密码系统、密码模块软件、密码应用、密码安全服务、密码安全可视化监管系统、全密码安全服务平台等。
- ◆ **公司积极布局区块链等相关技术：**目前，公司参与组建的湖北省区块链技术创新研究院获批成立，在推进区块链技术研究；此外，公司目前仍在深度研发区块链产品架构，目的是支持新技术架构对产品的应用需求。

信安世纪产品体系



信安世纪部分密码产品

- 证书认证系统（NetCert）
- 证书认证系统鼎安系列（NetCert-DA）
- 统一身份认证管理系统（NetAuth）
- 动态密码系统（NetPass）
- 动态密码系统鼎安系列（NetPass-DA）
- 安全运维网关（NetFort）

4.3.1 国内领先的数据库与存储提供商: 海量数据

- ◆ **海量数据是中国数据技术的领航企业：**公司数据库种类包括Vastbase E100数据库，和Vastbase G100数据库，具有高安全、高可用、高兼容等特性。公司数据存种类众多，可广泛适用于政府、金融、制造等行业。
- ◆ **海量数据生态优势：**生态是数据库发展的关键，目前，公司自主研发的 Vastbase 数据库已完成与鲲鹏 CPU、飞腾 CPU、海光 CPU 等主流国产芯片的兼容适配，能够在欧拉操作系统、麒麟操作系统、统信操作系统等主流国产操作系统中平稳运行；
- ✓ **公司积极布局分布式数据库，**今年10月28日，海量数据联合华为，以面向分布式数据库的创新存储方案为核心，倾注多年来数据库、数据库一体机研发的能力，与华为共同打造“存算分离”的端到端国产化数据库一体化解决方案。
- ✓ **公司具备分布式存储的能力：**公司Vastorage 数据存储产品通过软件定义新型分布式存储技术以及集群技术的综合应用，实现了高并发数据读写访问功能，优点为高可靠、高性能、高扩张、高效率、智能化。

资料来源：海量数据官网、华西证券研究所

海量数据公司数据存储产品



海量数据公司数据库产品



4.3.2 分布式数据库的超新星: 星环科技

- ◆ **公司数据产品种类齐全**：公司是一家企业级大数据基础软件开发商，围绕数据的集成、存储、治理、建模分析、挖掘和流通等数据全生命周期提供基础软件及服务，已形成大数据与云基础平台、分布式关系型数据库、数据开发与智能分析工具的软件产品矩阵。
- ✓ 公司主要产品包括星环数据云平台 TDC、分布式关系型数据库、智能分析工具Sophon、大数据开发工具TDS、大数据基础平台TDH等。
- ◆ **公司专注于分布式数据库，且技术领先**：公司已被Gartner 评为图数据库管理的全球代表厂商。主要产品包括：
 - ✓ **ArgoDB产品**：是一站式的分布式分析型闪存数据库，兼容Oracle等语言，具备灵活查询、联邦计算、快速响应等功能。
 - ✓ **KunDB产品**：是星环分布式交易性数据库，具备SQL兼容、一致性强、高性能等优势。

星环科技星环分布式分析型数据库





05 风险提示

- ◆ **核心技术水平升级不及预期的风险:** Web3.0相关产业技术壁垒较高，公司核心技术难以突破，进程低于预期，影响整体进度。
- ◆ **区块链政策监管风险：**区块链的应用发展存在政策的不确定性。
- ◆ **政策推进不及预期的风险:** 受到宏观经济、财政、疫情影响，政策推进节奏不及预期。
- ◆ **中美贸易摩擦升级的风险:** 供应链存在部分海外提供商，容易受到美国“卡脖子”制裁，导致产品研发不及预期。

分析师与研究助理简介

刘泽晶（首席分析师）2014-2015年新财富计算机行业团队第三、第五名，水晶球第三名，10年证券从业经验。

分析师承诺

作者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，保证报告所采用的数据均来自合规渠道，分析逻辑基于作者的职业理解，通过合理判断并得出结论，力求客观、公正，结论不受任何第三方的授意、影响，特此声明。

评级说明

公司评级标准	投资评级	说明
以报告发布日后的6个月内公司股价相对上证指数的涨跌幅为基准。	买入	分析师预测在此期间股价相对强于上证指数达到或超过15%
	增持	分析师预测在此期间股价相对强于上证指数在5%—15%之间
	中性	分析师预测在此期间股价相对上证指数在-5%—5%之间
	减持	分析师预测在此期间股价相对弱于上证指数5%—15%之间
	卖出	分析师预测在此期间股价相对弱于上证指数达到或超过15%
行业评级标准		
以报告发布日后的6个月内行业指数的涨跌幅为基准。	推荐	分析师预测在此期间行业指数相对强于上证指数达到或超过10%
	中性	分析师预测在此期间行业指数相对上证指数在-10%—10%之间
	回避	分析师预测在此期间行业指数相对弱于上证指数达到或超过10%

华西证券研究所：

地址：北京市西城区太平桥大街丰汇园11号丰汇时代大厦南座5层

网址：<http://www.hx168.com.cn/hxzq/hxindex.html>

华西证券股份有限公司（以下简称“本公司”）具备证券投资咨询业务资格。本报告仅供本公司签约客户使用。本公司不会因接收人收到或者经由其他渠道转发收到本报告而直接视其为本公司客户。

本报告基于本公司研究所及其研究人员认为的已经公开的资料或者研究人员的实地调研资料，但本公司对该等信息的准确性、完整性或可靠性不作任何保证。本报告所载资料、意见以及推测仅于本报告发布当日的判断，且这种判断受到研究方法、研究依据等多方面的制约。在不同时期，本公司可发出与本报告所载资料、意见及预测不一致的报告。本公司不保证本报告所含信息始终保持在最新状态。同时，本公司对本报告所含信息可在不发出通知的情形下做出修改，投资者需自行关注相应更新或修改。

在任何情况下，本报告仅提供给签约客户参考使用，任何信息或所表述的意见绝不构成对任何人的投资建议。市场有风险，投资需谨慎。投资者不应将本报告视为做出投资决策的惟一参考因素，亦不应认为本报告可以取代自己的判断。在任何情况下，本报告均未考虑到个别客户的特殊投资目标、财务状况或需求，不能作为客户进行客户买卖、认购证券或者其他金融工具的保证或邀请。在任何情况下，本公司、本公司员工或者其他关联方均不承诺投资者一定获利，不与投资者分享投资收益，也不对任何人因使用本报告而导致的任何可能损失负有任何责任。投资者因使用本公司研究报告做出的任何投资决策均是独立行为，与本公司、本公司员工及其他关联方无关。

本公司建立起信息隔离墙制度、跨墙制度来规范管理跨部门、跨关联机构之间的信息流动。务请投资者注意，在法律许可的前提下，本公司及其所属关联机构可能会持有报告中提到的公司所发行的证券或期权并进行证券或期权交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务。在法律许可的前提下，本公司的董事、高级职员或员工可能担任本报告所提到的公司的董事。

所有报告版权均归本公司所有。未经本公司事先书面授权，任何机构或个人不得以任何形式复制、转发或公开传播本报告的全部或部分内容，如需引用、刊发或转载本报告，需注明出处为华西证券研究所，且不得对本报告进行任何有悖原意的引用、删节和修改。

THANKS