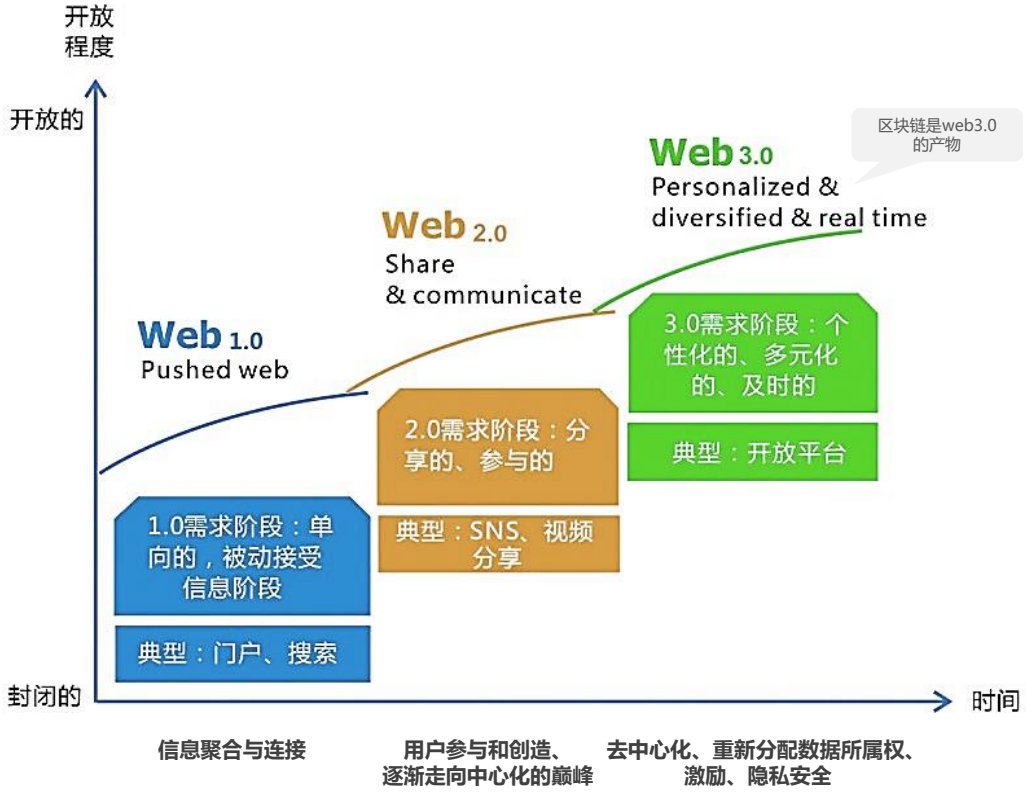
那些正在被区块链重构的事物

火星财经及共识实验室 发起人

王 峰

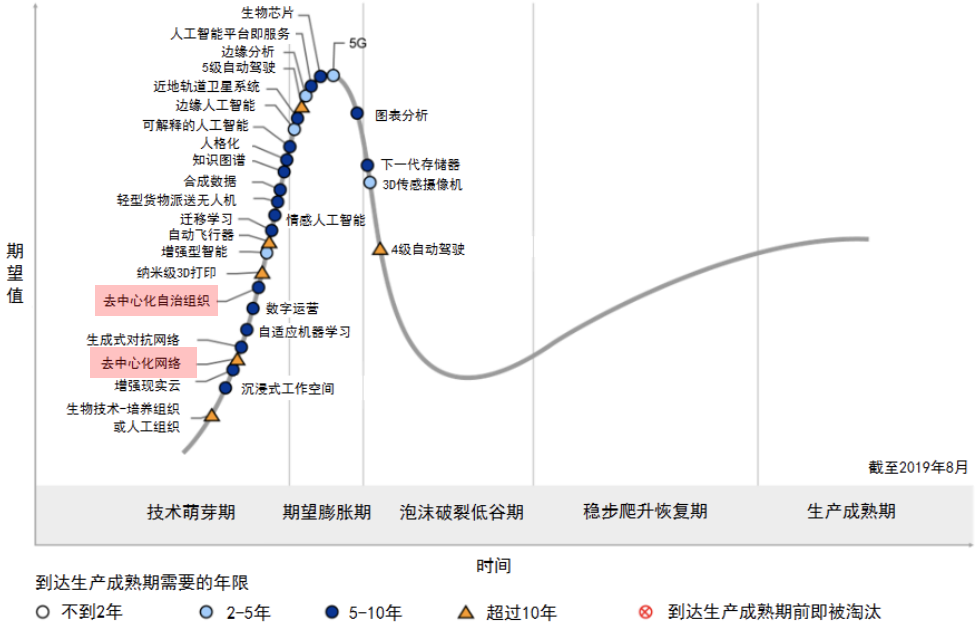
2019年9月

从计算机网络迁移看Web3.0发展方向



图表来源：imedia360

从Gartner2019技术成熟度曲线看区块链技术的发展阶段



- Gartner2019年新技术成熟度曲线中，首次将“去中心化自治组织(DAO)”和“去中心化网络”列为热点技术趋势之一。
- 此外，区块链与自动驾驶、沉浸式体验、量子计算等，还一并被列入Gartner 2019 年十大战略技术发展趋势。

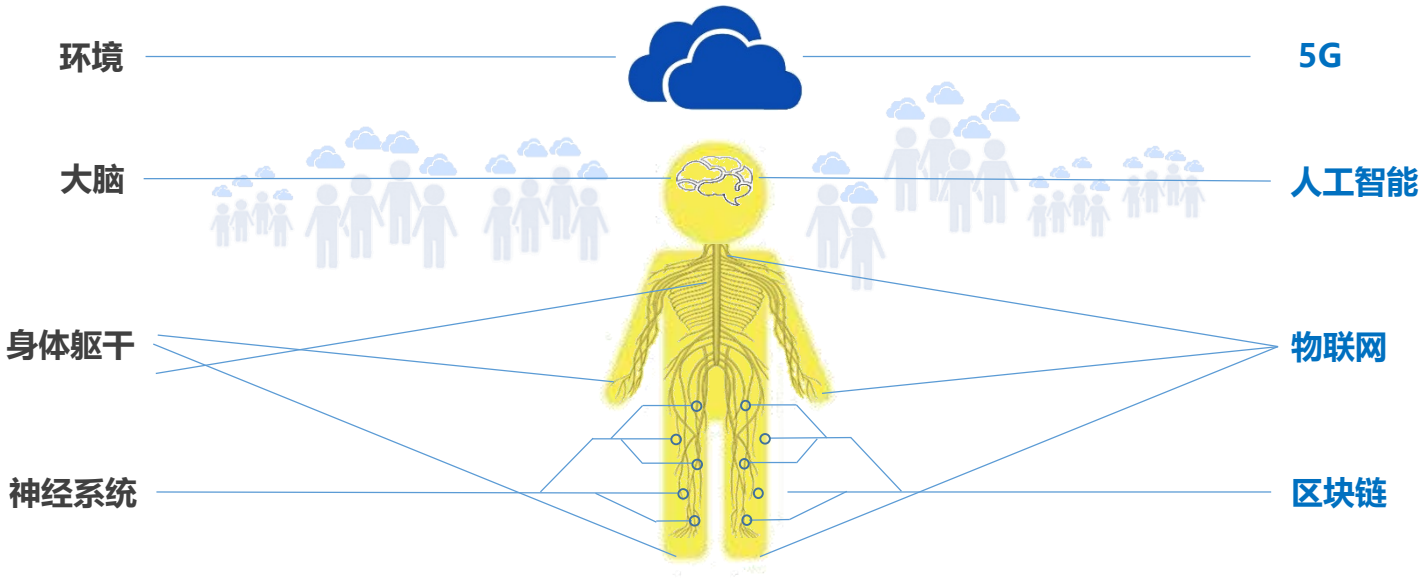
图表来源：Gartner《Hype Cycle for Blockchain Technologies, 2019》

区块链会替代互联网?

互联网核心业务的覆盖范畴

- 互联网的繁荣催生了金融科技革命。而区块链技术的出现，将推动今天的信息互联网进入价值互联网时代。
- 融合了区块链技术、拥抱了数字资产的新兴互联网企业会更加强大。

5G 时代的新物种生态



5G时代

人工智能、物联网和区块链

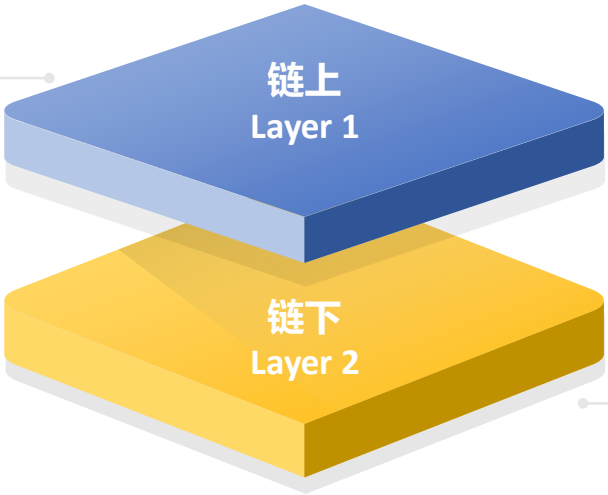
将促成更高阶的信息技术繁荣

2019区块链技术与应用十大趋势

一

1. 扩容问题

共识机制的创新
分片
比特币隔离验证
.....

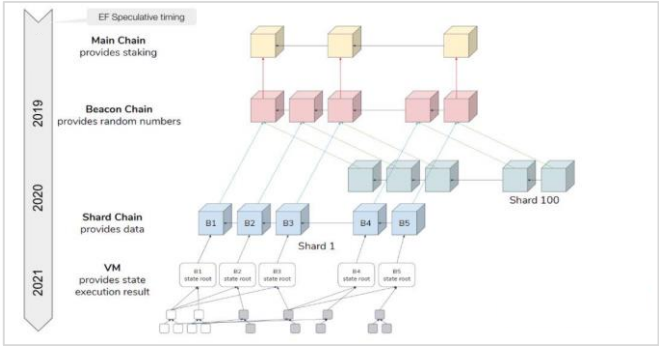


侧链
状态通道
闪电网络
.....

- 今天我们遇到的最大挑战是，在更大的去中心环境下，如何实现高并发的TPS。

Reference① 以太坊2.0

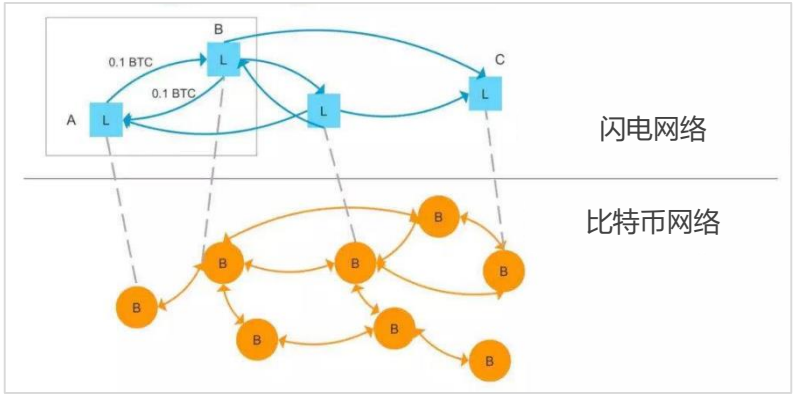
以太坊创始人Vitalik Buterin



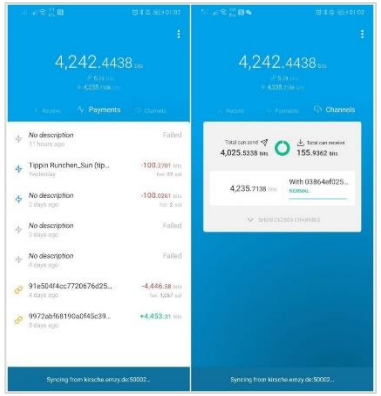
以太坊 2.0 设计路线图

- **背景**｜以太坊2.0，或称Serenity（宁静），是以太坊开发的第四阶段，其核心是实现以太坊网络大规模应用，大幅提升网络扩容性。以太坊 2.0 计划在 2019 年至 2021 年间，分四个阶段发布。2019年4月，Vitalik表示，为了在现有以太坊网络上改善扩展性问题，以太坊2.0带来的变化大致有两种：将PoW算法变更为PoS，以及Sharding（分片技术）。
- **分片**｜ Sharding英文原意是“碎片”，在计算机技术领域多译为“分片”，它常被运用在数据库的性能扩展上，典型的应用场景是各类线上游戏，特别是MMORPG（大型多人在线角色扮演游戏）。分片技术由某个节点服务器协调分配工作，其他节点按不同形式来分流服务器负载，如地图服务器只处理用户的地图需求，战斗服务器只处理用户的战斗需求等。
- **TPS**｜在2019以太坊技术及应用大会上，Vitalik提出，以太坊2.0将采用1024个分片的设计。在这种方法中，每个分片节点仅负责整个网络中发生的一部分交易，并且许多块可以并行发生，从而线性地增加整体网络吞吐量，预计将以太坊性能提升约1024倍，从目前的10TPS左右提至10000TPS以上。
- **信标链**｜信标链（Beacon chain）在ETH2.0上扮演“协调器”的角色，可协调各个分片的验证等工作。以太坊基金会表示，预计2020年1月前，信标链正式上线。

Reference② 闪电网络



闪电网络是比特币网络在另一个维度上的扩充



支持闪电网络协议的钱包使用图示

- **技术**｜闪电网络是一项解决比特币扩容问题的革命性技术，通过建立链下快速支付通道，以大幅提高交易速度，缓解比特币网络高负载和网络拥堵问题。截至2019年8月19日，闪电网络节点数量为4796个，同比去年增长218%；通道数量为31924个，同比增长283%；网络容量为1104.676个BTC，同比增长812%。
- **闪电火炬**｜2019年4月，一场全球使用闪电网络的马拉松活动“闪电火炬”引发热捧，Twitter联合创始人兼CEO杰克·多西等硅谷知名人士纷纷发声支持；2020年美国总统大选候选人之一Andrew Yang也表示将接受闪电网络支持的比特币捐赠。
- **国内发展**｜由于尚未看到闪电网络明确的商用价值，以及外部监管环境的不确定性，国内实际使用闪电网络和搭建基础设施的人并不多。截至2019年8月19日，国内闪电网络容量为2.97个BTC，节点数30个，全球占比分别为0.35%和0.5%。

数据来自：1ml

2. 隐私计算

传输网络隐私保护	交易隐私保护	内容隐私保护
• 洋葱网络 • 匿名通信协议I2P	• 混币 • 环签名 • 零知识证明	• 同态加密 • 安全多方计算

目前隐私保护机制的主要研究方向

- **背景**｜在信息互联网时代，隐私问题没有合理有效的解决方案。而区块链上的私有数据受加密保护，能够实现不同程度的匿名性、机密性和隐私保护。
- **技术**｜虽然区块链自身具有公开透明的特性，决定了任何人可以根据交易关联记录推测出账户的地址，这样一来，难以真正做到交易的匿名性。如今，隐私保护正在不断丰富扩充自己的含义——从仅仅确保交易隐私匿名性，逐渐加入了对数据所有权、使用权的隐私保护。

Reference③ MimbleWimble

比特币与MimbleWimble交易的比较

Grin与BEAM的比较

- **背景**｜ MimbleWimble：旨在提高比特币可扩展性和隐私性而创建的区块链协议，2016年7月发布白皮书。名字取自《哈利波特》中的咒语（即结舌咒，可让他人口齿不清或发不出声音），创始人Tom ElvisJedusor名字取自《哈利波特》中伏地魔角色。2019年初主网正式上线的Grin和Beam，是MimbleWimble技术的典型项目。
- **技术**｜在MimbleWimble中，隐私性和可扩展性得到保证的原因在于：不存在交易地址，交易金额也是隐藏的，同时中间状态的交易可以得到合并（如：先有A转给B钱，后又有B转给C钱，无需全部记录这两笔交易，只需记录A转给C多少钱，合并交易的中间状态，同时附上B的签名即可）。

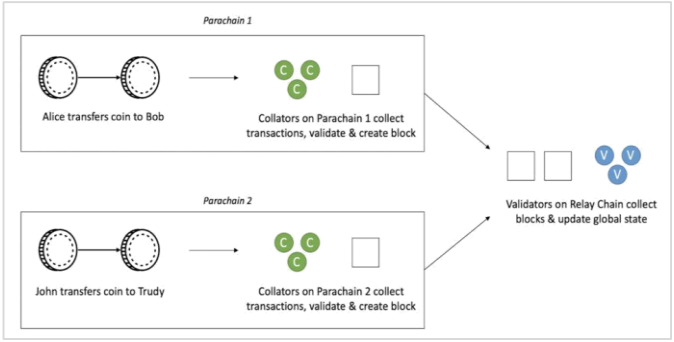
图表来自：ladybitcoin

3. 互操作性

区块链互操作性的发展层级

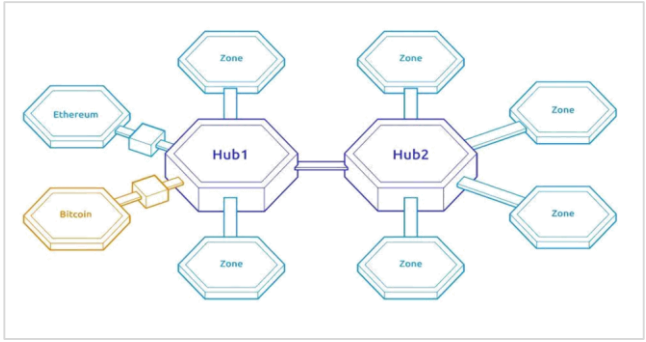
- **背景**｜今天的区块链还没办法叫做网络，无法实现在不同链之间的价值传递。这就像上世纪60年代的计算机网络一样，当时多以局域网形式存在，传输速度极慢且不能与局域网范围外的计算机连接，直到后来TCP/IP协议诞生互联情况才有所改变。区块链要想真正实现价值互联，并被大规模应用，就必须像互联网那样容纳多样性，在不同区块链之间进行衔接和拓展。
- **技术**｜互操作性（Interoperability），也被称做互用性，是指不同的计算机系统、网络、以及操作系统和应用程序一起工作并共享信息的能力。区块链互操作性具有以下几个特点：1. 不需要信任，不同的区块链即可直接安全地进行资产转移；2. 不同链之间的智能合约可以实现交互；3. 某些专用链可供其他区块链使用。

Reference④ Polkadot和Cosmos



Polkadot 网络架构

每条Parachains（平行链）的安全性来源于Relay Chain（中继链）上的验证者，一旦成为平行链连接到Polkadot网络，就能同时收获与Polkadot网络同级别的安全性。

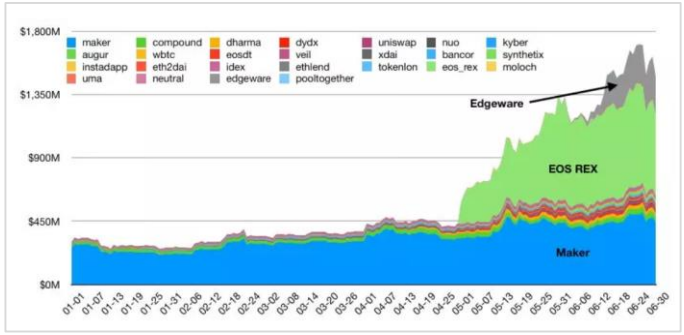


Cosmos 网络架构

使用hub-zone（中心区）模式，连接不同的zone（分区）。任何使用PoW机制的区块链系统，如比特币、以太坊或其他特定的区块链，都可以通过内部区块链通信架构连接到桥梁区域。

- **技术**｜跨链技术确保了区块链之间的互操作性，是实现价值互联网的关键。早期，跨链技术更多关注的是资产转移，典型项目包括瑞波、BTC Relay等；如今，跨链技术更多关注的是跨链基础设施，尝试建立一套多链的架构，让所有接入此架构的区块链，能更好的完成互相之间的信息和价值交互。
- **项目**｜以Polkadot（由以太坊联合创始人兼前CTO Gavin Wood于2015年创立，主网预计于2019年年底上线）和Cosmos（由Jae Kwon和Ethan Buchman于2016年创立，主网于2019年3月14日上线）为代表。

4. DeFi



2019 上半年 DeFi 应用锁仓总值

#	名称	主链	分类	7天用户 ≎	锁仓(美元) ≎
1	EOS REX	EOS	借贷	1.72K	$ 379M
2	Maker	ETH	借贷	16.8K	$ 256.47M
3	Edgeware	ETH	锁仓空投	24	$ 191.83M
4	Compound	ETH	借贷	16	$ 97.1M
5	InstaDApp	ETH	借贷	1	$ 23.45M
6	Synthetix	ETH	衍生品	467	$ 16.97M

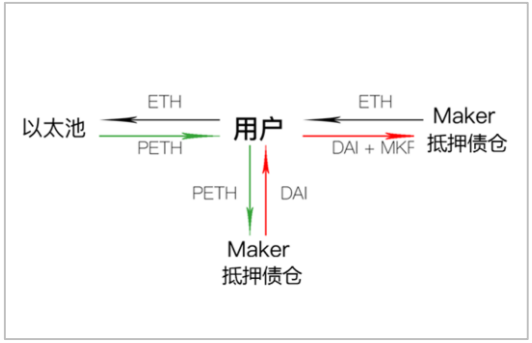
DeFi 应用排行榜（2019年8月15日）

- **技术**｜ DeFi，Decentralized Finance的简称，即去中心化金融。借助区块链技术，来解决传统及中心化金融存在的天然短板，如金融体制不平等、审查流程繁琐、缺乏透明性和潜在的交易风险等。
- **市场**｜ DeFi 最初是为了以太坊生态内的各种代币搭建金融基础设施，MakerDAO成为引爆 DeFi 的第一大应用。截至2019年8月30日，DeFi行业的总锁仓价值为10.2亿美元，较之1月1日的3.02亿美元，半年时间增长了近230%。随着以太坊2.0等公链技术不断突破，以及Libra这样具备传统互联网庞大用户的项目不断上线，DeFi市场容量和用户数或出现爆发性增长。
- **应用**｜ DeFi当前最值得关注的三个应用领域：稳定币、借贷市场和去中心化交易所：稳定币，链上总交易量2019年6月30日当天达到 8.59 亿美元；借贷总额 (贷出+借入)， 2019年6月为 5.44 亿美元，较2019年1月的 3400 万美元，增长了 16 倍；DEX，2019年6月总交易额为2.88 亿美元，较2019年1月的 7100 万美元，增长了 3倍。

数据来自：DAppTotal

Reference⑤ MakerDAO

MakerDAO 创始人Rune Christensen

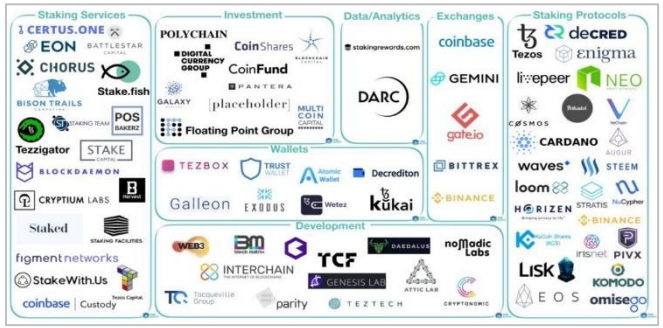


MakerDAO的运作机制

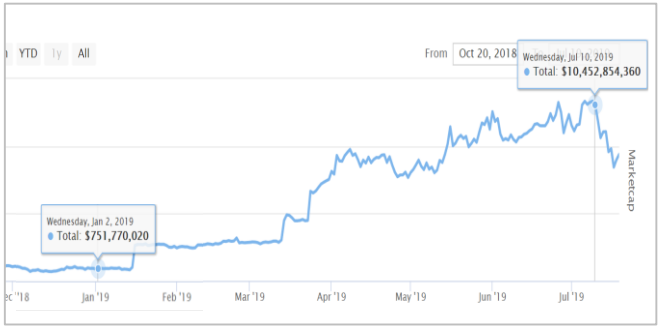
- **背景**｜去中心化借贷逐渐兴起的主要原因在于，一是加密货币市场需要新的融资工具，以MakerDAO为例，借方主要以企业为主，去中心化借贷逐渐成为了一种金融工具；二是2018年下半年加密数字资产价格整体下降，部分投资者从炒币转向理财、借贷、保证金交易等，进行增值保值。
- **技术**｜ MakerDAO由丹麦创业者Rune Christensen发起，成立于2014年，是以太坊上的自动化抵押贷款平台。它采用了双币模式，一种为稳定币Dai，另一种为权益代币和管理型代币MKR。通过双币机制，MakerDAO使得整个去中心化的质押贷款体系得以运转。MakerDAO团队目前拥有约50人左右，其中有一部分技术开发者来自BitShares。
- **市场**｜截至2019年8月30日，MakerDAO 项目共锁定2.4亿美元，占据DeFi项目锁仓总市值的23.9%，其最高峰时甚至占比达到85%。

数据来自：defipulse等

Staking涌现，基于权益证明的商业模式



Staking生态中的典型代表公司

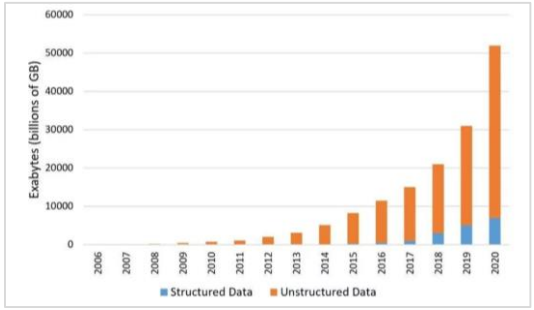


2019 上半年 Staking 市场抵押资产规模

- **概念**｜Staking是基于PoS（Proof of Stake，权益证明）共识机制，对持有的Stake行使相关权益的行为。Staking Economy是一种商业模式，Stake持有人通过质押、投票、委托和锁定等行为获取交易费、区块奖励以及分红等收益。
- **背景**｜Staking Economy趋势，最初由2019年初Stake.us获Coinbase（美国首家合规比特币交易所）、Pantera Capital（美国最大的加密货币对冲基金之一）等机构的450万美元投资引燃，之后，EOS、以太坊2.0、Dfinity、Polkadot、Harmony则进一步将Staking推向大众视野。
- **市场**｜截至2019年6月5日，全球共有75只加密资产支持Staking；在目前已经或者将要支持Staking的逾90个项目中，市值排名前50的项目就有21个。以太坊、Cardano、Polkadot等16个项目也将在下半年陆续支持Staking。目前，全球已上线Staking项目锁定市值达69.6亿美金，其中，EOS通过Staking锁定的市值最大，约为28亿美元，按其1.84%的年化收益率计算，相当于每年派发5000多万美元的红利。

数据来自：DAppTotal 、StakingRewards、theblockcrypto

5. 分布式存储



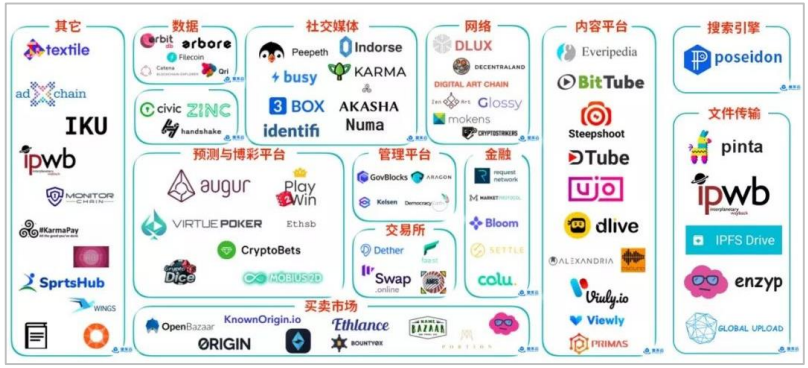
全球数据量增长状况

分布式存储的使用场景

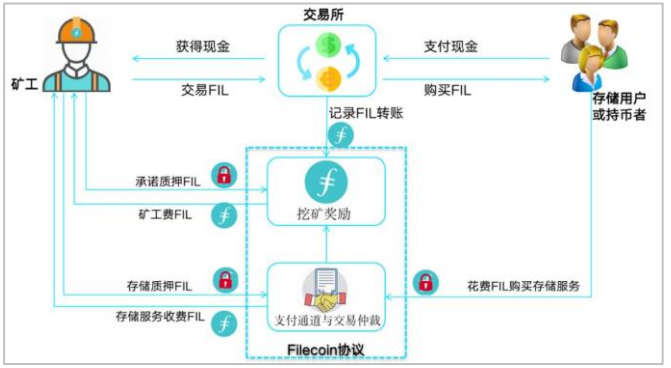
- **背景**｜随着互联网的飞速发展，数据呈现几何级增长，全球数据总量2024年预计为175ZB（1ZB约合10.7亿TB），本地存储和云存储都面临巨大压力；但是，亚马逊和微软垄断全球70%的公有云市场（特别是微软，依靠云计算业务增长推动其市值在2019年4月首次突破1万亿美元），服务商可以随意定价；加之云存储数据安全事故频发，如2018年10月苹果iCloud故障，2019年3月谷歌全球性服务宕机事件等。在此背景下，分布式存储应运而生。
- **市场**｜对标目前中心化云服务市场1万亿美金的规模，可以预测，分布式存储或将成为下一个千亿甚至万亿级市场，应用生态也会更丰富，分布式存储领域或将诞生世界级的公司。目前典型项目包括：Filecoin和Lambda，国内也出现了YottaChain、FileStorm等项目。

数据来自：IDC、Marketresearchfuture

Reference⑥ IPFS 和 Filecoin



IPFS 生态体系

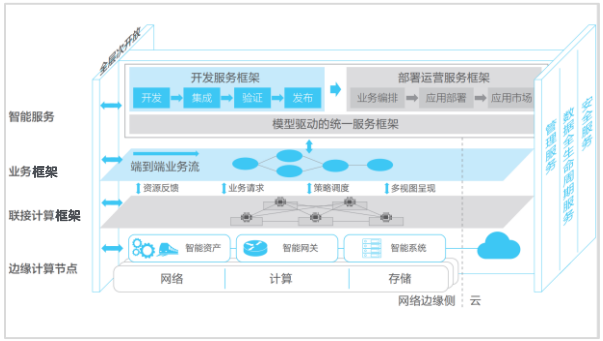


Filecoin 经济体系设计

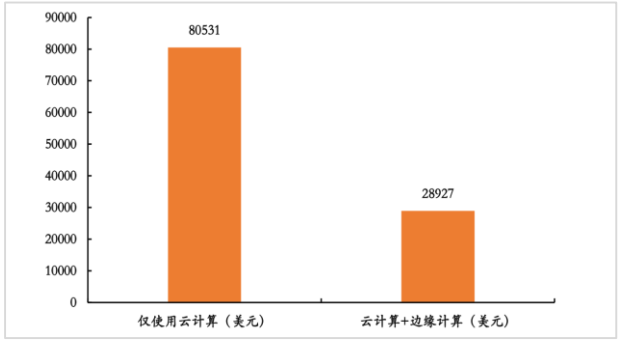
- **背景**｜如今，基于HTTP协议网络的弊病慢慢显现出来，如网络中心化、服务器成本昂贵、历史文件易丢失等。
- **技术**｜IPFS（InterPlanetary File System，星际文件系统）是一个旨在创建持久且分布式存储和共享文件的网络传输协议。由Juan Benet于2014年设计开发。IPFS通过网络删除重复具有相同哈希值的文件，通过计算判断哪些文件是冗余重复的，并跟踪每个文件的版本历史记录。
- **项目**｜Filecoin是建立在IPFS基础上的一条公链，旨在创立一个分布式的储存市场，维系IPFS生态的正常运行与发展。Filecoin在2017年8月进行了众筹，融资超过2.57亿美金，成为史上规模最大的公链发行之一，其中红杉资本领投5千万美元。

数据来自：星系云

6. 边缘计算



边缘计算模拟架构



3 年内使用不同计算方式处理的成本费用（以200英里距离计）

- **技术**｜边缘计算（Edge computing），即在终端设备附近靠近数据源的一侧进行的本地计算分析。它将数据处理从云中心转移到网络边缘，计算和数据存储可以分散到互联网靠近物联终端、传感器和用户的边缘，不仅可以缓解云带宽、计算等压力，还可以优化面向感知驱动的网络服务架构。
- **数据**｜到2020年，预计将有超过500亿的终端和设备联网，其中超过50%的数据需要在网络边缘侧分析、处理与存储，边缘计算市场规模可超万亿元，成为与云计算平分秋色的新兴市场。
- **物联网**｜边缘计算与区块链融合是物联网发展的下一步方向。一方面，二者的融合能提高物联设备整体效能。以物联网设备群为例，移动边缘计算可以充当物联设备的“局部大脑”，存储和处理同一场景中不同物联设备传回的数据，并优化和修正各种设备的工作状态和路径，从而达到场景整体应用最优。另一方面，物联终端设备可以将数据“寄存”到边缘计算服务器，并在区块链技术的帮助下保证数据的可靠性和安全性，同时也为将来物联设备商业模式发展提供了可能性。

数据来自：Wikion、广证恒生、IDC等

Reference⑦ 任正非谈边缘计算

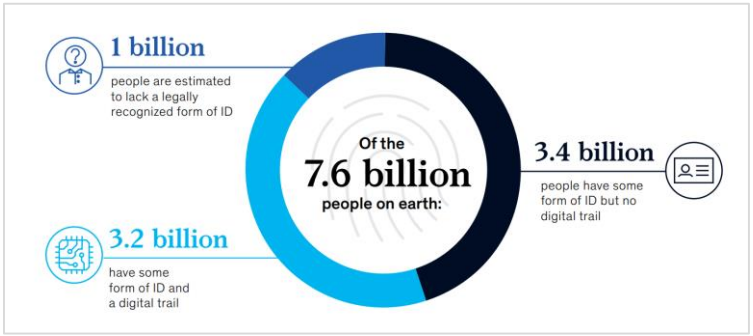
2019年4月，华为创始人任正非接受美国财经媒体CNBC访谈

- 任正非在访问中提到，“首先，我们希望在世界上提供最好的互联，5G就是互联的一个部分；其次，我们将力争打造世界上最好的边缘计算。我们已经放弃了超级计算和中级计算，我们只专注于边缘计算。”

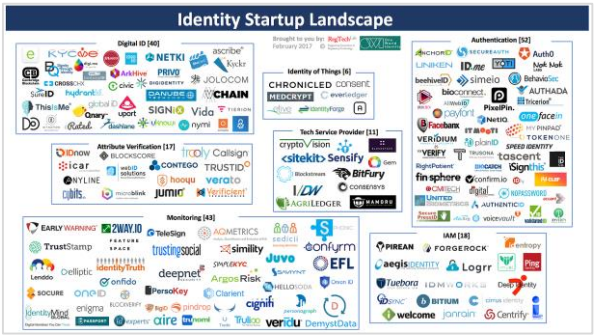
Reference⑧ 物联网商业闭环

- 没有区块链技术的赋能，物联网很难发挥其在经济结构、经济制度和商业模式上的重大革新作用。

7. 数字身份



全球人口拥有数字身份状况

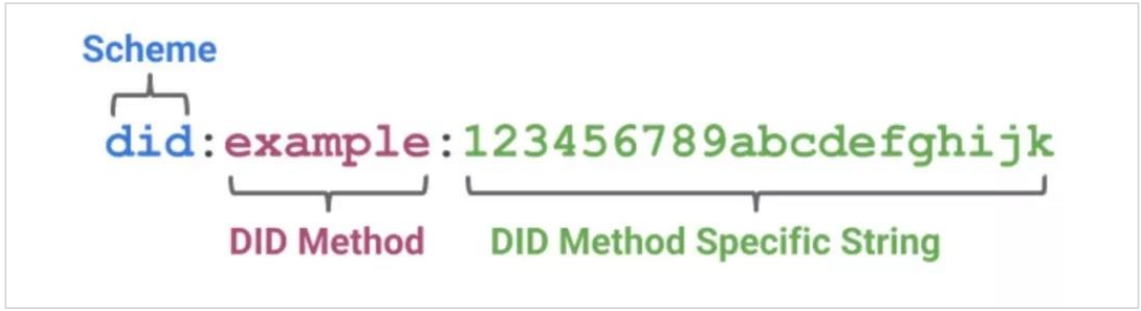


数字身份相关的创业项目图谱

- **概况**｜数字身份是政府治理、公共服务、医疗、电信、金融等各领域数字化的重要基石。使用数字身份，个人在更多地融入金融服务和获得就业机会方面受益最大；政府和企业能够更有效的提供服务，降低福利、工资和税收相关的欺诈问题，从而在节省成本方面获益最多。
- **趋势**｜阿里巴巴达摩院《2019年十大科技趋势》中，将“数字身份将成为第二张身份证”列入其中。
- **市场**｜麦肯锡报告显示，到2020年，身份验证有望成为一个价值200亿美元的市场，其他相关服务更是可能高达千亿美元。

数据来自：36kr

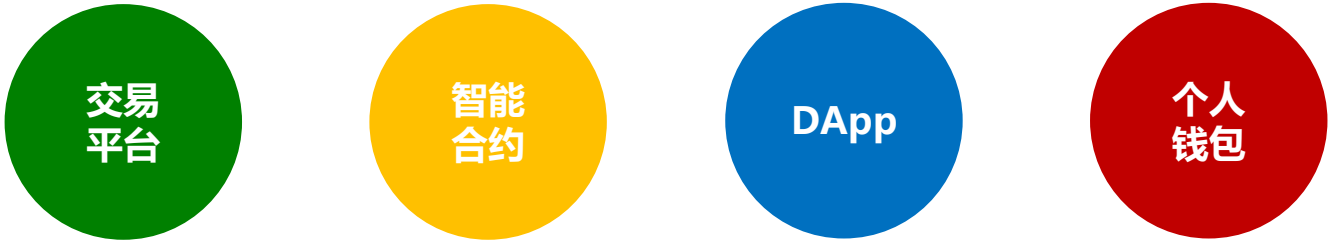
Reference⑨ 微软 ION 去中心化数字身份



微软ION的去中心化身份（DID）标准结构

- **背景**｜去中心化数字身份认证是提供个人数据所有权的新方式。每个人都有权拥有其数字身份，它以安全、私密的方式存储所有个人数据，而且这个数字身份ID必须无缝集成到日常生活中，让用户完全掌控数据访问和使用情况。
- **概况**｜2019年5月初，微软发布了名为 ION（Identity Overlay Network，身份覆盖网络）的去中心化身份（DID）网络的早期预览版。任何互联网用户都可以通过这个基于比特币区块链的专用公网，来创建其去中心化的身份标识，进而管理他们的个人数据与信息。
- **意义**｜ION网络可能会消除应用程序和平台对身份标识符的控制，如果ION网络满足巨大交易量需求，并实现规模化运作，传统数据行业将面临巨大挑战，以中心化、不透明的方式处理数据将成为历史。因此，有观点认为，“微软发布ION的意义，堪比Facebook发布Libra”。

8. 安全问题



区块链行业目前面临的主要安全隐患

- 互联网的安全是信息的安全，密码错了更换一个也可以，但在区块链领域绝对行不通，因为它绑定了太多的东西。区块链面临着来自数据层、网络层、共识层、激励层、合约层、应用层的安全风险，安全问题正成为许多区块链公司的达摩克利斯之剑。
- 据【火星号】“成都链安科技”数据，2018年全球区块链领域发生近百起安全事件，损失超20亿美元。2019年7月，加密数字资产市场共发生15起安全事件，造成超4亿人民币损失。

Reference⑩ 2019年1至8月区块链安全事件

黑客攻击盗币

1月13日至14日，Cryptopia交易所被盗， 损失28773 枚 ETH

3月24日， DragonEx平台钱包遭受黑客入侵，损失价值 600余万美元的数字资产

4月11日，波场TronWoW游戏被黑客攻击，损失约216万TRX

5月8日，币安发现“大规模安全漏洞”，损失4100万美金

8月4日，EOS Royale游戏遭受黑客攻击，损失约18000EOS

暗网非法交易

2019年上半年，已有价值 5.15 亿美元的比特币被用于非法活动。

4月，德国警方逮捕了3名德国籍犯罪嫌疑人，他们涉嫌参与运营名为“华尔街市场”的非法暗网交易平台。该平台上卖家超过5400个，客户超过115万，在被关闭前，毒品、窃取数据、伪造证件和恶意软件等交易项目超过6.3万个。

勒索软件

6月，GandCrab 勒索病毒传播，累计总收益已高达20亿美元，平均每周获益250万美元。

7月，在北美地区危害严重的Ryuk勒索病毒在国内传播，该病毒作者要价11个比特币，价值约75万元。

跑路事件

1月，Angel Token数字钱包APP跑路，套取20多名投资者近千万元

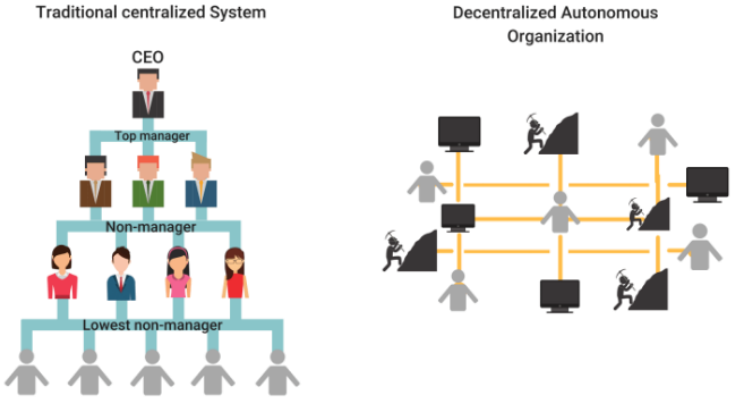
3月20日，DOGX wallet关网跑路，至少卷走价值5000万人民币的ETH

6月10日，加密货币理财钱包项目TokenStore携带数十亿元资金“人间蒸发”

6月29日， PlusToken钱包被曝光跑路，涉及资金池规模高达200多亿人民币

数据来自：成都链安科技

9. 分布式自治组织

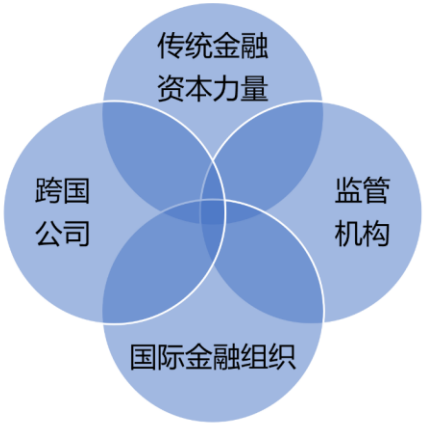


中心化组织　　分布式自治组织

- **概念**｜DAO：Decentralized Autonomous Organization的简称，即分布式自治组织。它开创了一种新型的组织结构，治理和运营规则都可以被编成代码放进智能合约中，并由遵守这套规则的股东进行管理，且不存在中心化控制组织的权威机构。Vitalik将DAO定义为“一个生活在网络且独立存在的实体，但也严重依赖于人来执行它本身无法完成的某些任务”。
- **意义**｜分布式自治组织正在颠覆传统公司的治理和财富分配模式。对投资者来说，DAO将公司运营中人为失误和高管腐败两个最大风险最小化，因此，与普通公司的股票相比，DAO成为风险较小的投资类别，提供比大多数股票股息更可预测的投资回报率。

图片来源：nirolution.com

10. 开放式金融



参与全球货币金融领域博弈的四种主要力量

不是走向开放
而是走向封闭

不是走向竞争
而是走向垄断

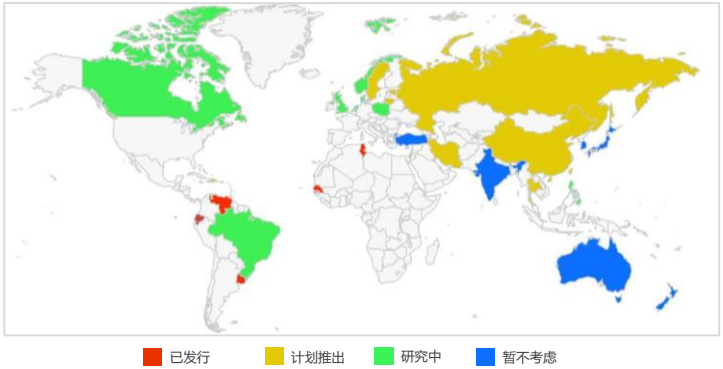
不是货币金融共享
而是被个别利益集团独占

当前货币金融领域面临的问题和挑战

- 由区块链新技术所推动的开放金融，必将成为全球化竞争的下一个重要领域，谁也回避不了。
- 有人还在讨论中心化和去中心化，其实意义并不大。去中心化和不完全去中心化的区块链谁会笑到最后，取决于在这场已经到来的由区块链新技术所推动的开放金融革命中，谁能解决更多问题，谁能发挥更大作用。

Reference⑪ Libra及央行数字货币

2019年6月18日，Facebook公布Libra白皮书



世界各国中央银行发行法定数字货币的现状

- Libra白皮书中，提到其使命是：“建立一套简单的、无国界的货币和为数十亿人服务的金融基础设施”。
- 对于区块链及加密数字货币市场来说，Facebook发布Libra，其意义恰如微软在操作系统中嵌入IE浏览器。Libra的横空出世，会带动更多的交易场景涌现，很可能把全世界二十亿以上人口引向拥抱数字资产世界的大门。

- 8月10日，中国人民银行支付结算司副司长穆长春公开表示，央行数字货币已经呼之欲出，并将采用双层运营体系，即先把数字货币兑换给银行或者其他运营机构，再由这些机构兑换给公众。彭博社认为“中国将成为首个推出央行数字货币的主要经济体。”
- 央行发行的数字货币，既可以像现金一样易于流通，有利于人民币的流通和国际化，同时可以实现可控匿名，将是一场货币体系的重大变革。

数据来自：清华大学金融科技研究院区块链研究中心

至少我相信
信息产业和金融市场的基础设施
正在被区块链重构

专注于区块链信息及金融服务

火星财经

扫码下载火星财经APP