区块链行业研究报告

（来源：上海北外滩金融研究院，2017-08-17）

2017 年 4 月 1 日起以比特币为首的各数字资产迎来一波极大的上涨。短短两个月时间比特币价格增长为过去的三倍达到近 3000 美元。数字资产是否已经迎来了最好的时代？上海北外滩金融研究院就此推出区块链行业研究报告，试图勾勒出一幅完整的区块链行业发展图景。

一、区块链概述

区块链(Blockchain)目前并没有一个统一的定义，综合来看，区块链就是基于区块链技术形成的，具有去中心化、去信任特性的公共数据库。

区块链技术是一种解决信任问题、降低信任成本的信息技术方案。到目前为止，解决信任问题的最重要机制是“信任中介”模式，政府、银行都是信任中介，我们对货币，对交易的接受都基于对发钞银行和政府的信任。这是一种中心化的模式。然而也是由于信任模式的中心化，用户的许多需求也会被复杂化。无论在生活还是在工作中，用户都需要在各类机构中提供各式的大量的证明，而这些手续也为这些机构带来了巨大的人力成本、时间成本、资源成本。区块链技术的应用可以取缔传统的信任中介，解决陌生人间的信任问题，大幅降低信任成本。这也是常说的区块链“去中心化、去信任”的意思。

通过区块链技术，互联网上的各个用户成为一个节点并相互连接起来，所有在此区块链架构上发布的内容都会在加密后被每一个节点接收并备份，换而言之每一个节点都可以查看历史上产生的任何数据。各节点将加密数据不断打包到区块中，再将区块发布到网络中，并按照时间顺序进行连接，生成永久、不可逆向的数据链，这便形成了一个公开透明的受全部用户的监督的区块链。

如上所述，区块链可以实现市场参与者对全部资产的所有权与交易情况的无差别记录，取缔交易过程中所有权确认的环节，因而这可能会是一种可以完全改变金融市场格局的技术，甚至会出现在各行各业以及生活中的每个角落里。

2009 年 1 月 3 日区块链技术的第一个成熟应用——比特币网络上线，也正是比特币网络使得区块链进一步完善并正式进入了公众视野。目前，类似比特币和超级账本 Fabric 等的许多应用已经开始出现在生活中。

二、区块链分类

公有链(Public Blockchain)：对所有节点都开放的区块链。在公有链中任何数据都是默认公开的，节点之间可以相互发送有效数据，参与共识过程且不受开发者的影响。已存在的应用有比特币、莱特币和以太坊等等。

私有链(Private Blockchain)：权限仅在一个组织的管理下的区块链。读取权限可以完全对外公开或者从任意程度上被限制，组织有权控制此区块链的参与者。相比于传统的分享数据库，私有链利用区块链的加密技术使错误检查更加严密也使数据流通更加安全。

联盟链(Consortium Blockchain)：只对特定的组织团体开放的区块链，本质上可归入私有链分类下。已存在的应用有 R3 区块链联盟、Chinaledger、超级账本项目联盟等。

三、区块链特性

不可篡改：区块链加密技术采用了密码学中的哈希函数，该函数具有单向性因此存在于链中的非本节点产生的数据是不可被修改的。同时由于区块链系统共识算法的限制，几乎无法单方面修改本节点产生的数据并使其被确认(除非达到全网算力的 51%)。

去中心化：相对于“中心化”的一个概念。区块链系统没有特定的中央服务器，是一个基于点对点技术的开源系统。每个节点共同实

现系统的维护并保证信息传递的真实性。整个系统采用分布式存储模式，数据完全公开透明没有中心进行集中管理。

去信任化：任意节点之间的连接或数据交换都不需要信任为前提并受到全网监督，即每个节点都是区块链系统的监督者。

实时性：从信息披露角度来看，数据交换一旦完成便会立即上传到区块链网络中。从数据传输角度来看，如跨境支付这类目前数据处理缓慢的领域，已经可以通过区块链技术大大提升效率；在日常支付领域，随着区块链技术的进步，区块链应用最终会超过中心化应用的效率。

四、区块链技术逻辑

1. 区块链加密技术

哈希算法：又称为散列函数，是指将任意长度的二进制数据通过算法映射为固定长度的二进制数据的过程。它是一种单向的密码体制，加密后无法反推出原始数据。在区块链中的应用涉及到区块创建过程、信息封装过程和数据验证过程。

SHA-256 算法：SHA(Secure Hash Algorithm，安全哈希算法)是一套由美国标准与技术局制定的加密哈希函数的总称。SHA-2 是这套算法里安全性较高的一类函数群，SHA-256 则为此函数群中一种包含 32 位哈希值数据的算法。

公钥加密算法：这种密码算法需要两个密钥——公开密钥和私有密钥。算法通过私钥产生公钥，但是反向通过公钥推导出私钥则几乎不可能。公钥加密的数据只有对应私钥才能解开，私钥签名的信息通过公钥验证。在区块链中使用的公钥密码算法是基于椭圆代数的特性开发的椭圆曲线算法。

2. 区块链连接方式

这里以比特币区块链为例进行解释。2009 年 1 月 3 日中本聪制作了比特币区块链的创世区块，也就是第一个区块，并以此作为数据

的源头。连接某区块的前一个区块称为其父区块。每一个区块分为两部分——区块头和区块主体。区块主体用于储存区块链网络中发布的交易信息，区块头则用来储存各种哈希值数据。包含于其中的两条哈希值是 Merkle 根值和父哈希值。

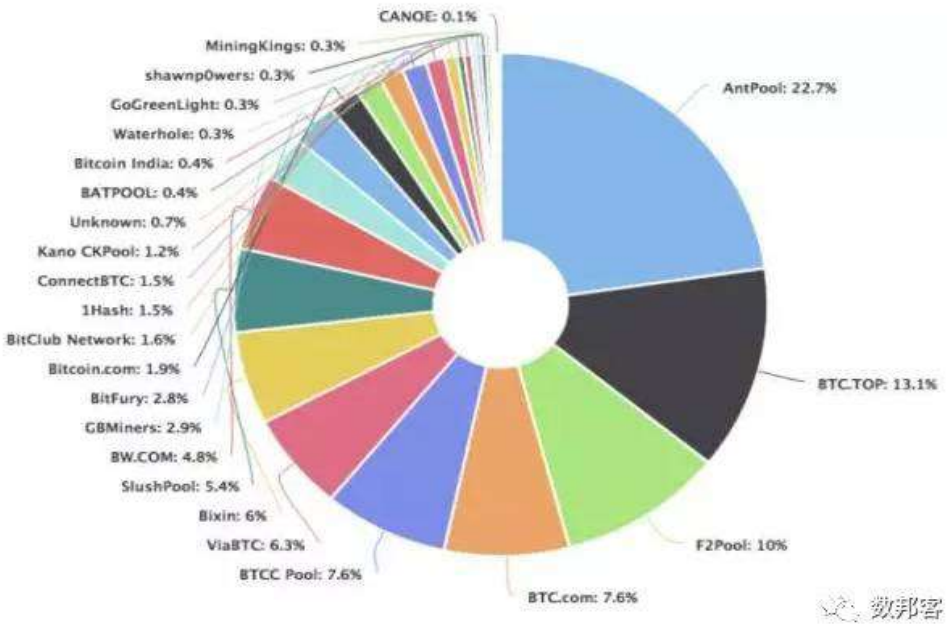
Merkle 根值是对区块主体中的所有交易记录进行哈希运算得到的一个值。

父哈希值是上一区块的头哈希值。

当新的区块被创造时首先会根据交易记录产生新区快的 Merkle 根值并加入到新区块的区块头中，这一行为会使得父区块对其自身区块头的所有数据进行处理生成一个头哈希值并将此值植入新区块的区块头中成为其父哈希值。以此方式完成了区块间的连接。

3. 区块链共识算法

工作量证明机制(Proof of Work,POW)：目前大部分数字资产使用这种算法，如比特币、以太坊。区块的产生需要一定的算力，即计算设备每秒能进行哈希运算的次数。一台设备的算力在全网算力中所占的比重即由这台设备创建新区块(挖矿)的概率。目前众多平台组织各个节点进行联合挖矿，这些平台称之为矿池。下图为目前各大矿池的算力分布图（资料来源：blockchain.info）。



权益证明机制(Proof of Stake,POS)：目前小部分数字资产使用该算法，如未来币、黑币。此机制引入了“币龄”概念。一个节点拥有一定的数字资产，每持有单位数字资产一天则积累一个币天的币龄，若发现新的区块则现有的币龄将清零并重新累计。POS 部分保留了 POW 机制用来生成初始数字资产，之后便通过区块链网络中币龄的消耗来产生新的数字资产。节点所拥有的币龄在全网币龄中所占的权重即由此节点创建新区块的概率。

股份授权证明机制(Delegated Proof of Stake,DPOS)：该算法较为成熟的应用有比特股。在该机制下，每一个持有数字资产的节点可以对全网络节点进行投票并由此产生 101 位代表。可以将这些代表类比为 POW 机制下的 101 个超级矿池，他们因为占据了大部分的算力因而几乎对区块链的开发占有绝对主导权。而在 DPOS 机制下，这 101 个超级节点彼此的权利是完全相等的。若代表不能按时生成区块则会被除名并被新选出的代表取代。

4. 区块链分叉

区块开采产生分叉:如果在很短的时间间隔内同时有两个节点 A、B 创建了下一个区块，由于网络传输速度的限制，一部分网络节点会先收到 A 节点的确认信息，另一部分网络节点则先收到 B 节点确认信息。区块 A 和区块 B 会以平行区块的形式同时以前一个区块为父区块连接到链中。这两个区块都是有效的，包含了几乎相同的数据信息。之后全网的网络节点将按照其认可的区块为父区块继续创建下一区块，当某一支链优先创建出下一区块的时候这条支链将会成为长链(在 POW 算法下长链指包含算力最高的链，在 POS 算法下长链指总消耗币龄最高的链)并被全网确认，分叉结束。

系统升级产生分叉：区块链的共识协议包括交易结构的协议和区块结构的协议。如果区块链系统出现问题需要修复或者结构上需要升级便会通过分叉的方式实现。这样的分叉分为软分叉和硬分叉。

1） 软分叉：在新协议下创建的区块可以被旧区块接受，反之亦然，是一种向上兼容的模式。实际上新旧区块会交替出现在区块链中，随着节点对新协议的逐渐接受，旧区块将最终消失，不会产生支链。

2） 硬分叉：在新协议下创建的区块不可以被旧区块接受，是一种向下兼容的模式。新区块会从旧有区块链中分叉，各节点达成共识并将算力投入到将新区块作为父区块的新链中，最终完成硬分叉。

无论是何种分叉都需要大部分算力达成共识并通过。以太坊于 2016 年发生硬分叉，然而有一部分节点依然坚持在旧链上工作并且拥有一定的算力，由此以太坊成为两链并行的硬分叉案例。旧链对应的数字资产称为以太坊经典(ETC)，新链仍称作以太坊(ETH)。

五、区块链发展历程

比特币

2008 年 10 月 31 日，一位化名为中本聪的人在论坛上发布《比特币：一种点对点式的电子现金系统》一文，宣告了历史上第一个区块链应用比特币诞生，次年 1 月 3 日，中本聪通过代码制作了比特币区块链的第一个区块：创世区块，比特币网络正式上线。

以太坊

2013 年 12 月，俄罗斯天才少年 Vitalik Buterin 发表以太坊项目白皮书，定义以太坊为一个能创建分布式应用(DAPP)的区块链平台。次年 7 月，以太坊项目开始融资，7 月 30 日，以太坊平台正式上线。该平台改变了区块链的应用格局，使其不再局限于比特币和类似竞争币触及的支付领域，而使得区块链技术开始有机会应用到各方各面。

R3CEV

这是一家专注发展联盟链的区块链创业公司，目前已经和四十余家金融机构合作并开发区块链项目。该公司对于比特币技术的测试和应用真正的结合了传统体系，涉及范围十分广阔。

纳斯达克

2015 年美国证券交易所纳斯达克启动了一项关于区块链技术的实验，旨在为金融机构业务探究高效解决方案。这是首家大型金融机构主动接受并研究区块链技术。

The DAO

DAO 意为去中心化自治组织。其目的是为组织规则以及决策机构编写代码，从而消除书面文件的需要，以及减少管理人员，从而创建出一个去中心化管理架构项目。The DAO 是一个特定 DAO 组织的名称，是由德国初创公司 Slock.it 的团队创建而成。The DAO 项目基于以太坊平台开发，是一个资金募集项目，募集的资金会用于对其他项目的投资。该项目于 2016 年 4 月 30 日正式上线开始融资并迅速筹得 1.5 亿美元。然而由于技术上的漏洞，同年 6 月 18 日该项目遭到

黑客攻击并被盗取了价格近 6000 万美元的以太坊。为了解决这一问题，大部分节点最终达成共识——施行以太坊硬分叉方案，将区块链回滚到未发生黑客攻击事件之前。自此以太坊分为以太坊(ETH)与以太坊经典(ETC)。

The DAO 是去中心化自治组织中最大的一个组织；而该项目也是一次重要的尝试;此次被攻击事件是有史以来技术平台遭到的涉及资金额度最大的攻击事件;其造成的结果也成为了目前唯一的区块链硬分叉且双链并行的案例。

EOS

2017 年 6 月 26 日,区块链底层操作系统 Enterprise Operation System 开始进行融资。该项目在多方面进行了技术革新，有望将区块链技术和应用格局带向一个新的高度，甚至取代以太坊。

Fabric

2017 年 7 月 12 日，超级账本联盟发布了其首个可用于构建应用的产品级解决方案 Fabric 正式版。超级账本联盟是受到世界广泛关注的研究区块链技术的联盟，其发布的 Fabric 产品是第一个落地的可开发商业应用的区块链平台。

六、区块链参与者

1. 技术社区

基层参与者：在区块链技术开发、区块开采、数字资产投资方面操作的参与者，大致可分为

1) 开发人员：开发区块链技术，构建并维护区块链平台。

2) 矿工：构建区块以获得数字资产奖励。

3) 数字资产持有者:通过平台交易与场外交易获得数字资产并看重其投资性而非应用性。

交易平台：为数字资产提供交易场所的平台，大致可分为

1) 现货交易:提供各种法定货币和数字资产充值、提现功能的，

可直接交易的平台。国内如云币网，其交易品种的数量和质量在国内均属一流。国际上如 Poloniex，其交易品种的数量和交易额度规模均为世界第一。

2) 场外交易：在交易所外的，通过交易双方直接联系或借助中介人联系的方式完成数字资产的交易。场外交易网站中交易额最大的当属 LocalBitcoin，该平台成立于 2012 年，总部位于芬兰。国内目前只有“币看”一家交易平台。

2. 传统企业

金融机构：传统金融机构目前正在积极引进区块链技术。如中国招商银行是首家实现将区块链技术应用于全球现金管理（Global Cash Management）领域的跨境直联清算、全球账户统一视图以及跨境资金归集这三大场景的银行。2016 年 6 月，招行已通过跨境直联清算业务 POC 实验，2017 年 3 月 9 日招商银行通过首创区块链直联跨境支付应用技术，为永隆银行向其在香港同名账户实现跨境支付，标志着国内首个区块链跨境领域项目成功落地应用，在国内区块链金融应用领域具有里程碑意义。

机构联盟：传统企业联合研究区块链技术，推动区块链应用发展。目前最受关注的联盟是超级账本项目联盟。详情见“区块链相关应用”部分。

3. 区块链公司

底层技术公司：此类公司注重对区块链底层技术的开发，目的是通过新建或不断优化区块链平台，为各类 DAPP 开发提供良好的环境。如以太坊、EOS。详情见“区块链相关应用”部分。

区块链应用公司：此类公司注重对区块链特性与功能的利用，并用以解决当前市场存在的问题，相关企业有区块链初创公司 R3，Ripple 网络。详情见“区块链相关应用”部分。

4. 投资机构

股权投资机构：此类公司着眼于对区块链技术相关企业的投资和指导。如国内的分布式资本，该公司由比特股团队创始人之一沈波，万向控股副董事长肖风以及以太坊创始人 Vitalik Buterin 共同运作，目前已投资包括 Gem、EOS、Zcash 在内的众多企业。此外，还有包括中国比特币首富李笑来的团队 Inblockchain，传统 VC 公司 Boost VC(该公司近几年开始转投区块链公司)，国外区块链公司专投机构 Blockchain Capital 在内的众多股权投资机构。

数字资产对冲基金：此类公司着眼于资产分配，主要业务为构建数字资产市场组合以及投资 ICO 项目。如 Hyperchain Capital，该公司资产组合包括比特币、以太坊、EOS、Zcash、Q-tum 在内的三十余种数字资产。

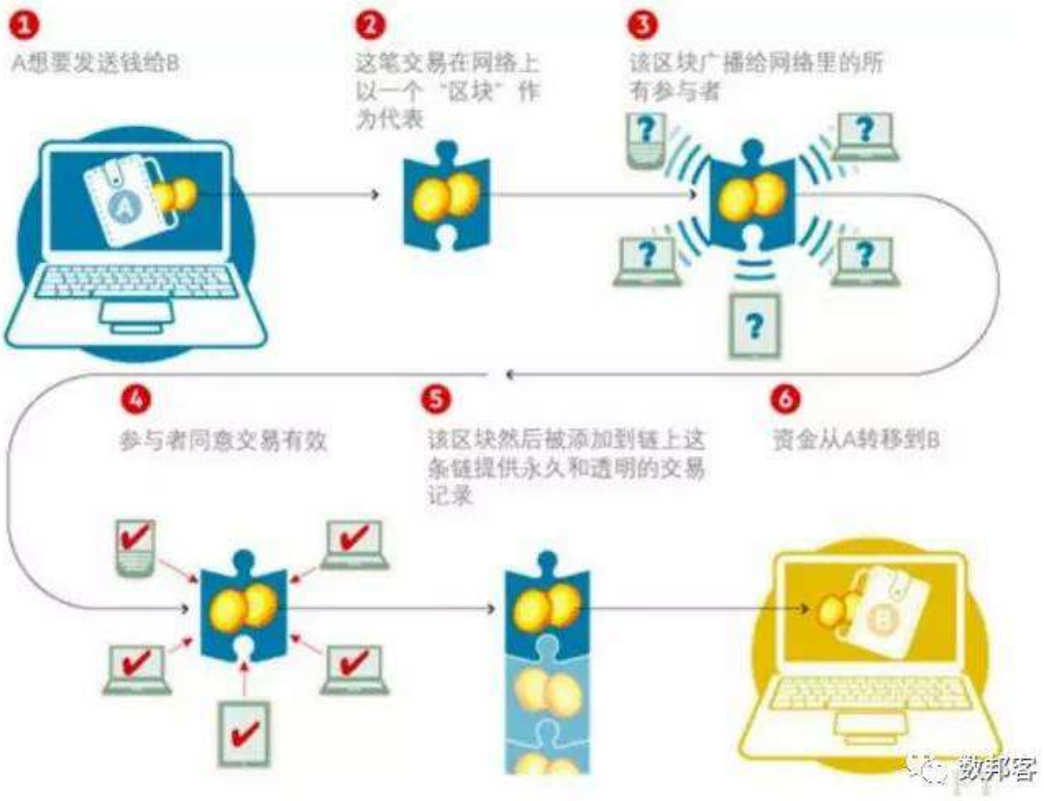
七、区块链相关应用

1. 支付手段

比特币(Bitcoin，BTC)：2008 年中本聪（Satoshi Nakamoto）发表论文《比特币：一种点对点的电子现金系统》，宣告比特币的正式诞生。2009 年 1 月 3 日区块链技术的第一个成熟应用——比特币网络上线。比特币通过“挖矿”的方式产生，当“矿工”(自然人或群组，他们自愿进行计算机处理来解开区块方程并验证发生的一系列数据交换)解开一个新的加密区块时，会得到这个区块内包含的比特币和解密时间段内发生的交易的手续费作为奖励。区块内的代码参数会自动调节区块难度，使得全网节点解出一个区块的时间约为 10 分钟，区块包含的比特币每四年会发生减半，所以总量恒定为 2100 万枚。比特币自 2009 年诞生后价格持续上涨，2011 年币价达到 1 美元，2013 年最高达到 1200 美元，超过 1 盎司黄金价格，目前已上涨至 2000 多美元。

通过比特币，任意节点之间可以在互相不认识，完全无信任的情况下互相转账，因此现被用于跨境贸易、支付、汇款等领域，在这些

领域采用比特币支付将大大减少手续成本和时间成本。同时，比特币已经用来购买现实世界的一些产品，2010 年有人用 10000 比特币购买了两个匹萨，这是历史上最早的一笔比特币与实物的交易，现在，包括捐款、购买数字音乐专辑、购买汽车、搭乘出租车在内的众多领域方面许多公司都已经接受了比特币作为支付工具。比特币解决了支付方式去中心化的问题。下图为比特币区块链支付流程：



资料来源：Financial Times

2. 匿名支付手段

Zcash(ZEC)：Zcash 诞生于 2011 年 11 月 9 日，是首个使用零知识证明机制的区块链系统。该系统整体结构和运作模式与比特币十分类似，但是通过对交易记录的编码化实现了节点信息的完全匿名，从匿名性角度上来讲，比比特币更能保证资金安全和身份保密性。

3. 底层基础链

以太坊(Ethereum,ETH)：底层基础链是一种平台化的、程序化的区块链。在基础链上可以实现 DAPP 的开发，并应用到众多领域之中。

我们可以将其类比为编程语言和软件之间的关系。

以太坊是最早的，也是目前最成功的底层基础链应用。提及以太坊就不得不先介绍智能合约。智能合约是一套以数字形式定义的承诺和执行承诺的协议，是 1995 年由尼克·萨博提出的理念。事实上智能合约是一段计算机程序，在合约参与方满足一定的条件后即可准确的自动执行。信用卡的自动还款功能是该技术在传统行业的应用。然而由于缺乏应用平台该想法一直未能大面积普及。自比特币诞生后人们认识到区块链可以为智能合约提供可信的执行环境，真正实现智能合约的去信任化。以太坊团队首先看到了区块链和智能合约的契合机会，并于 2015 年 7 月 30 日发布以太坊项目。在以太坊平台，众多的开发者可以编写各式各样的智能合约来创建应用，满足用户需求。就智能合约本身来讲，其使用主要分为三个步骤：

1) 合约被多方用户共同制定

i. 用户在区块链注册得到自己的私钥、公钥、和地址。

ii. 多个用户共同商定一份数字化合约，合约包含用户的权利和义务，各用户使用私钥对合约进行签名保证合约的有效性。

2) 合约存入区块链

i. 合约通过 P2P 的方式在网络中传递给每一个节点并被保存。

ii. 各节点在共识时间里将保存的合约打包成一个合约集合(set)，计算其哈希值并将此值构建为一个区块发布到其余节点，各节点对收到的信息与保存的信息进行验证并发送一份认可的信息到其他节点。各节点通过多轮验证最终对合约内容达成一致。

iii. 验证的主要目的是确认合约参与者的私钥签名是否匹配其账户。

3) 智能合约自动执行

i. 智能合约系统会自动检测每一条合约的触发条件，当条件满足时便会开始进行验证。

ii. 当大部分节点验证成功达成共识后该合约便被执行。

iii. 已完成的合约将留存在旧区块中，进行中的和未被执行的合约将加入到新的区块中等待下一轮处理。

量子链(Q-tum)：量子链是一个通过合并改进版本的比特币核心基础架构和可以相互兼容的以太坊虚拟机版本的底层平台，旨在成为开发可信的去中心化应用的最重要工具，并且适用于现实世界商业环境。量子链平台希望建立一个智能合约枢纽，将智能合约标准化并应用到商业当中。同时量子链平台也计划推出移动端产品。

Enterprise Operation System(EOS)：EOS 是一个基于全新架构的底层区块链平台。据 EOS 白皮书所述它采用了石墨烯架构技术，因而具备众多老式区块链不具备的优势，如具备商业应用级处理速度，每秒钟可处理百万次的交易记录。石墨烯架构使用 DPOS 共识算法，出块速度在 1.5 秒左右因此其交易确认时间将会大大提高，同时在该算法下版本更新不会引发硬分叉后双链并行的问题。EOS 还包含一个冻结和处理破坏性应用程序的机制，类似 DAO 事件发生时该应用会被冻结而不会影响到整个区块链，也就避免了因为技术问题而造成的硬分叉。从发展前景看该项目可能将区块链技术与相关应用带到一个新的高度，但实际成果还未落地。

4. 汇款

瑞波(Ripple,XRP)：瑞波网络是一个实时网络全额清算系统，用于货币交换和汇款并支持跨境交易，运营公司为 Ripple Labs。该网络基于区块链技术开发，但是是一个基于熟人信任的网络系统，严格意义上并不完全属于区块链系统，加之跨境交易存在灰色地带，所以应用实则有所局限。但是不可否认的是该网络依然是目前市场上较为成熟的一个区块链应用因而其代币瑞波币也具有一定的投资价值。

5. 分布式存储

SiaCoin(SC):Sia 是一个基于区块链技术的支持云存储的平台，

我们可以借助常见的百度云来理解。从存储角度讲，类似于百度云等的存储平台是一种中心化的，无隐私性的平台，Sia 则可以保证自己上传的资源不被删除，下架，封禁；从下载角度讲 Sia 借鉴了 BT 传输机制,下载时可从多个节点读取,保证了下载速度;从应用角度讲，Sia 可能是目前为止应用目的最为清晰的一个平台,其前景值得期待。

6. 电子存证

小蚁(AntShare,ANS)：小蚁区块链是国内第一条原创公有链。小蚁项目致力于将现实世界的资产和权益进行数字化,通过点对点网络进行登记发行、转让交易、清算交割等金融业务。小蚁使用电子合同(e-contract)来记录数字资产的流转。在小蚁中，电子合同所产生的数字凭证(digital token)作为一种通用的底层数据，可以用于记录股权、债权、证券、金融合约、积分、票据、货币等各种权利和资产，用于股权众筹、股权交易、员工持股计划、P2P 借贷、积分、基金、供应链金融等领域。目前，小蚁区块链已为“法链”项目提供技术支持。

7. 数据交易

公信宝(GXS)：公信宝是一个基于区块链实现的去中心化数据交易所，旨在打通各平台数据源信息，实现各个机构之间的数据能够进行点对点交易和共享。公信宝声称该平台具有数据造假控制机制和双向匿名机制，可确保企业的隐私不被泄漏，获得的数据真实有效。其数据爬虫维度目前涉及全国社保、通信服务运营商、学信网、京东、支付宝、微信等众多平台。公信股(GXShares)是公信宝 ICO 过程中向用户发行的权益证明资产，拟发行总量为 1 亿股(100,000,000)，享有公信宝数据交易所佣金10%的分红权。

8. 股权交易

Linq：2015 年 NASDAQ 在 SEC 的监管允许下推出了基于区块链的股权交易平台 Linq。Linq 运用分布式、电子化的记账方式使股份发

行人可以看到股票期权比例，每一轮投资以后已发行股票的价格以及估值情况。区块链创业公司 Chain 成为了平台第一个使用者。

9. 产权公证

Ascribe：初创企业 Ascribe 利用区块链技术为知识产权进行时间标记，为艺术品和其他数字媒介创建可持续所有权结构，目的是通过去中心化数据库为创作者的作品提供信息公证和所有权追踪。

10. 技术联盟

超级账本：Linux 基金会在 2015 年发起的一个多方合作的开源项目，旨在共同打造基于区块链的企业级分布式账本底层技术。超级账本将提供多种区块链技术框架和代码，包含开放的协议和标准，不同的公式算法和存储模型，以及身份认证、访问控制和智能合约等服务。此商业化联盟链的成员有包括英特尔、摩根大通和 IBM 在内的众多大型企业。截至 2017 年 1 月，该联盟共计划开发 5 个项目：Fabric(区块链底层基础框架)，Sawtooth Lake(时间消失证明和法定人数投票共识算法)，Iroha(移动应用开发)，Blockchain Explorer(查询区块链交易数据的网页应用)和 Cello(管理区块链生命周期)。

R3CEV：一家专注发展联盟链的区块链创业公司，截至目前它已经吸引了 47 家金融机构加盟，其中中国的平安保险集团和招商银行也在联盟之中。2016 年 3 月，R3CEV 宣布其 40 家银行成员已经测试了 5 种不同的区块链技术并将用于发行、交易和赎回固定收益产品。

11. 四大会计师事务所

2014 年德勤推出提供咨询服务的区块链应用 Rubix 并于 2016 年在柏林和纽约分别建立了区块链实验室。

2016 年普华永道推出了 Vulcan 数字资产服务，通过与 BloqLibra 和 Netki 公司的合作使数字资产能够用于日常银行业务和商业中。

2016 年 9 月毕马威推出了数字账本服务，旨在帮助金融服务公

司更好的运用区块链技术。

2017 年起安永的客户可以选择用比特币支付发票审计和咨询服务，另外安永在 2017 年 4 月推出 Ops Chain 来促进区块链技术在企业中的商业使用。

八、区块链技术及应用面临的问题

1. 51%攻击

区块链技术面临的潜在威胁。只要某个节点拥有全网总算力的 51%或总币龄的 51%，理论上即可对区块记录进行修改，实现多重支付并获取收益。

2. 数据处理速度有限

当前的区块链技术水平有一定的局限性，只适用于低流量低频次的交易环境。在比特币区块链中，每个区块确认时间大约需要 10 分钟，目前全网每秒实际只能确认 3 笔左右的交易，进而一笔交易的平均最终确认时间实则已经超过 1 小时，数据处理效率非常低。虽然诸如瑞波币和以太坊的许多新平台已经优化了区块链技术使得交易速度有了一定的提升，但距高效解决问题和大规模普及还有一定的距离。

3. 安全存在隐患

2014 年，当时世界上最大的比特币交易所运营商 Mt.Gox 遭受黑客攻击，损失 85 万枚比特币；2016 年去中心化自治组织 The DAO 遭受黑客攻击，损失近 6000 万美金。这两次事件都和区块链技术的安全漏洞有关。由于目前区块链技术仍处于早期发展阶段，资产管理平台或技术开发平台的技术问题可能会给参与者带来巨大损失；某种数字资产的价值可能会因为技术缺陷而丧失；使用区块链技术的传统行业或政府部门若因技术故障而使重要数据受到影响，其后果也可能是灾难性的。

4. 与固有系统不兼容

1) 区块链技术的快速发展不免会对许多现有行业造成极大冲

击。当前世界

大部分主流金融机构无法接纳公有区块链，对于他们而言需要的是一个自主可控的系统，区块链技术显然无法实现这一点。

2) 区块链技术的应用会降低行业手续费和佣金收入。

3) 数字资产市场成熟度和稳定性远不及金融市场，容易暴涨暴跌，行业参与者良莠不齐，投资者可能无法认可或承受市场波动。

5. 监管政策难以确立

区块链去中心化的特点意味着系统内没有一个明确的主体，因而监管对象难以明确，导致目前监管政策并不明朗。目前该行业存在一些不规范行为，但是其技术的价值和前景值得肯定，需辩证看待。过度的监管会限制区块链技术的发展，但监管不足会破坏当今社会金融结构的稳定性。

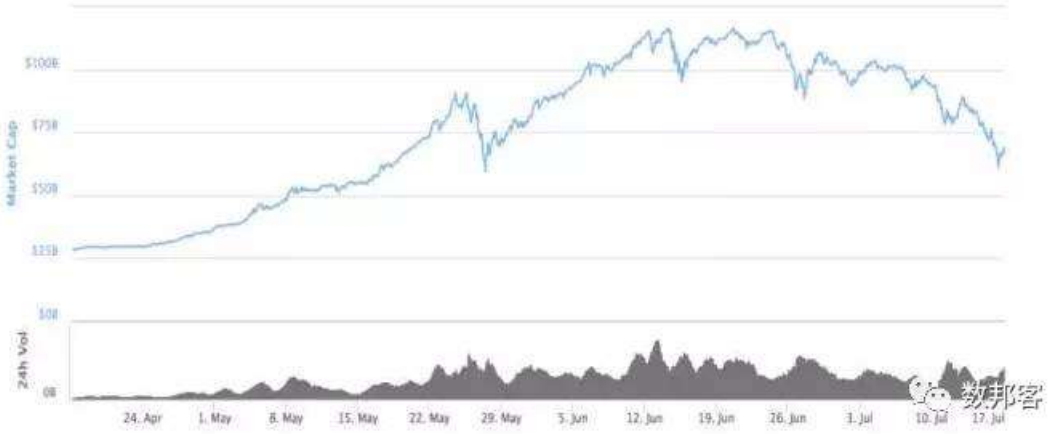
九、数字资产市场行情

1. 数字资产

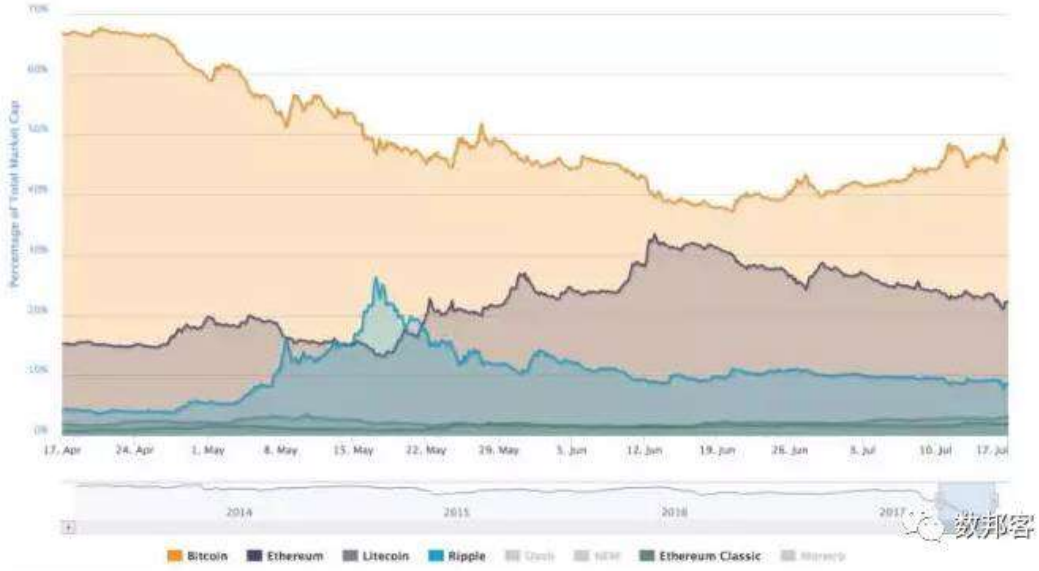
资产数目：截至 2017 年 7 月 17 日已有 978 种数字资产。

交易量：目前比特币与以太坊每周交易量均在 55 亿美元左右，莱特币约为 25 亿美元，以太坊经典约为 15 亿美元，瑞波币约为 10 亿美元。

市值：目前各类数字资产的总市值约为 850 多亿美元，其中比特币约占 45%，以太坊约占 25%，瑞波币约占 10%，其余 900 多种共同占有 20%。下图为近三月数字资产总市值



下图为部分数字资产市值占比。



资料来源：CoinMarketCap

动态：2013 年 8 月，德国将比特币设立为合法货币，同年 12 月，比特币价格最高达到 1200 美元。

2017 年 4 月 1 日起以比特币为首的各数字资产迎来一波极大的上涨。短短两个月时间比特币价格增长为过去的三倍达到近 3000 美元，以太坊则增长为过去的 10 倍达到 300 多美元。截至目前比特币价格仍接近上涨前三倍，以太坊约为过去价格的 5 倍。原因如下：

1） 4 月 1 日日本宣布比特币和以太币成为合法支付方式。

2） 俄罗斯最大电商“Ulmart”5 月表示将于 2017 年 9 月开始接受比特币支付。

3） 5 月 24 日来自全球 21 个国家的 56 个数字资产公司就比特币扩容达成共识，将在 7 月使用“Segwit+2x”技术将比特币区块大小扩容至 2Mb，并采用新的审核交易方式“隔离验证”(Segregated Witness)。这一共识意味着比特币区块链的交易塞车问题将获缓解，比特币转帐可更快被确认。

价值：数字资产具有价值是因为其数学特性(持久性、可携带性、可互换性、稀缺性、可分割性和易识别性)而非依赖于物理特性(比如

黄金和白银)或中央权力机构的信任(比如法定货币)。简而言之，数字资产是由数学支持的，要具有价值所需要的就是信任和使用。

价格决定因素:数字资产价格由供需决定。需求增加,价格上涨。目前大部分数字资产以一个可预见的逐步下降的速率发行。这表示需求必须遵循这一通胀水平才能保持价格的稳定。

数字资产是不是泡沫：价格的快速上涨并不会构成泡沫。人为的高估将会导致一个突然向下的修正才会构成泡沫。基于成千上万的市场参与者个体行为的选择导致数字资产价格的波动是市场决定价格的结果。

2. 首次代币发行(Initial Coin Offering,ICO)

ICO 是一个区块链行业术语，源自股票市场 IPO 概念。是指区块链项目首次发行代币募集比特币、以太坊等通用数字资产的行为。有明文记载的首个 ICO 项目是万事达币(MSC)；第二个 ICO 项目是未来币(NXT)，由于这是第一个完全使用 POS 机制的数字资产，其资金的募资程度比较成功。

以太坊 ICO 是较大的且十分成功的 ICO 项目之一，以太坊的建立也是区块链历史的一座里程碑。EOS 的 ICO 项目打破了首日募资额度的历史记录，成为目前最大的 ICO 项目。

ICO 是一种具有高效性的融资方式，省去了包括人际交流、协议签署等在内的大量的时间成本。但也因其高效性、极为高涨的市场热情和监管的缺失导致了许多 ICO 项目本质上只是泡沫，只为了炒作、圈钱。目前要想证明整个 ICO 市场和项目价值的合法性是十分困难的，他们的价值完全基于投机，不能通过真实的市场数据进行评估，因为自始至终都没有部署可行的产品或者软件。

参与 ICO，首先应该弄清这个问题：这个项目提供的解决方案是否切实可以解决现实问题且是不可替代的，即该问题的解决必须通过区块链技术达成，如果可以解决，那么是否具有效率和经济性的优势？

在理解 ICO 项目的基础上再考虑是否参与。这样至少保证了项目本身的可靠性。项目能否成功落地，市场是否接受，则依然充满不确定性，因而 ICO 需谨慎投资。

十、政策与监管

目前德国、以色列、美国加州、日本、印度已认可了加密数字资产，但就全球市场而言，数字资产管理仍处于监管空白地带。尽管目前中国和不少国家都对数字资产行业持较为开放和包容的态度，但实际监管风向并不明朗。

1. 中国

1） 2013 年中国人民银行、工业和信息化部、中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会联合印发了《关于防范比特币风险的通知》，通知规定禁止各金融机构为客户提供比特币登记、交易、清算、结算等服务；禁止接受比特币或以比特币作为支付结算工具；禁止开展比特币与人民币及外币的兑换服务；禁止开展比特币的储存、托管、抵押等业务等等。

2） 2016 年 1 月 20 日中国人民银行召开数字货币研讨会，提出争取早日推出央行发行的数字货币。

3） 2017 年 2 月中旬央行检查组对多家交易平台进行约谈，令几大交易平台着手自律与自查。几家平台带头开始收取 0.03%-2%的交易费、停止融资融币并宣布为升级反洗钱系统暂停提现比特币。

4） 2017 年 3 月 7 日央行召集北京数家比特币交易所召开通气会并下发了一份监管草案以征求意见。草案要求比特币交易所必须建立三项制度——反洗钱反恐怖融资制度、反洗钱上报制度和客户识别制度。另据《华尔街日报》3 月 17 日消息，央行的这份草案除了将比特币交易所纳入反洗钱法的监管范围还要求交易所确认客户身份并遵守银行业监管规定。此外交易所还将安装用于收集可疑交易活动并向有关部门汇报的系统，央行将负责处理比特币交易所的违规行为。

5) 7月央行数字货币研究所所长姚前表示对ICO的监管政策框架可以从现行的IPO与股权众筹监管法规中寻找合法性依据，但不能完全简单套用。他建议宽容对待ICO，根据区块链技术行业的特性在上市审批、投资者限制、项目公开宣传和推介上给予一定的包容性豁免。他还强调注意以下五点：

i. 额度管控与白名单管理。

ii. ICO 融资计划管理。

iii. 对发行人施予持续、严格的信息披露要求、强调反欺诈和其他责任条款。

iv. 强化中介平台的作用。监管部门保留监管干预和限制权力。

v. 加强国际监管合作与协调。

2. 英国

2015 年 3 月提出了“监管沙盒”概念。在沙盒中企业将在英国金融行为监管局 FCA 制定的大框架内测试区块链创新型产品和商业模式并且不会将不良影响直接带给处于正常监管机制下的企业。

3. 欧盟

1) 欧盟近期创建了TITANIUM联盟，计划在三年内开发出一种可行的科学解决方案来减少犯罪分子使用数字资产和暗网进行犯罪活动(如恐怖主义、诈骗、洗钱和敲诈)带来的挑战。

2) 欧盟议会提议建立一个中央数据库来登记用户的身份信息、钱包地址、加密数字资产申报表。欧盟表示国家金融情报机构应该将数字资产地址和数字资产所有者的身份相关联，以此来减轻匿名性带来的风险。

4. 美国

1) 2017年7月初美国大宗商品期货交易委员会CFTC首度将比特币衍生品交易纳入监管。

2) 2017年7月14日美国统一法律委员会在年度会议上对《加

密货币经济统一监管法案》进行投票。该法案的目的是“创建一个法律监管结构对向法律制定州的居民提供服务或产品的‘虚拟数字资产商业活动’进行监管”。本草案第 103 条规定银行及政府等某些主体可免于获取营业执照。

5. 韩国

韩国中央银行经调查认为“双重货币制度”是可行的，即法定货币和加密数字资产共存。

6. 日本

2017 年 4 月 1 日，日本宣布比特币和以太坊成为合法支付方式，允许金融机构参与电子货币交易。7 月 1 日宣布新版消费税法正式生效，比特币和以太坊交易不再需要缴纳 8%的消费税。

十一、发展前景

区块链发展到今天早已超越了“币”的范畴进化为“链”与“链”的竞争。区块链在目前的状态，正如 20 世纪 90 年代的互联网，虽然不被大部分人理解和接受，虽然产生过泡沫，但是可以肯定的是其技术前景是十分诱人的。

很多人持有数字资产是泡沫，是庞氏骗局的论调。我们知道，十七世纪初，郁金香经历了从普通到价值数亩田地又跌落至归零的大起大落，郁金香泡沫便是一种典型的破灭型泡沫。然而数字资产不同。从历史价格来看，数字资产在多次的动荡中保持了上涨的大趋势。即便 13 年比特币曾有过 10 倍的增长并且半年后发生大跌，最终也依然稳定在了 200 美元的节点并且逐年增长。数字资产中一定存在泡沫但是这更多的是一种挤出型泡沫，在市场的一次次反馈中挤出泡沫虽然导致了价格的波动，但是实质上是逐渐证明了自身的价值。比特币已经诞生 8 年之久，各类主流数字资产也基本存在了 3 年以上，有理由相信数字资产价格的上涨是基于价值的肯定而非市场的炒作。

而更底层的区块链技术，则可能带来下一次技术的革命性进展。

当下，区块链技术已经在不少机构和行业里开始运作，本研报已经列举了很多金融行业相关的应用。实际上，在其他行业，如法律、媒体、游戏等等，都也已经有所进展。可以预见到未来区块链技术一定会给我们的生活带来更多的便利甚至是翻天覆地的变化。

诚然，区块链在传统机构中的应用充满争议，因为一方面降低了信用成本和手续成本，另一方面也冲击了现有稳定结构和行业利益。在发展的过程中有优秀的技术公司，也不乏有炒作热点试图骗取利益的幌子公司。但是对于区块链技术本身，我们应该持有开放包容的态度，应该相信他们是可以带来实质性进步的。而对于具体的应用，也不能一概而论，只有在充分了解企业和项目之后才有权做出理性的判断。

十二、投资建议

部分数字资产价格在整个市场中波动性是相对较低的，对应的应用具有相当的稳定性或是其目的明确、可操作、可实现，对应的平台在技术上有一定的优势，可以支持、帮助整个区块链生态系统良好运作，其背后的团队在技术能力、营销水平、口碑等方面均具有一定的优势。对于该类数字资产，建议长期持有。

部分数字资产在整个市场中波动性是相对较高的，因而其投机性更强，对应的应用有一定的实际价值，但鉴于政策或技术的限制其前景不明朗，对应的平台可能缺乏技术的革新，存在较大的重叠性，其背后的团队技术能力一般或者存在不良背景。对于该类数字资产，建议短期投资。

部分数字资产在整个市场中的波动性是相当高的，且流动性较差，对应的应用和平台基本没有实际价值，前景十分一般，无论从技术上还是团队上都不具备优势。对于该类数字资产，不建议介入。