

推荐 (维持)

区块链与数字货币：原理、特征和构想

2016年02月01日

相关报告

《VR+时代开启 企业级应用市场同步繁荣》2016-01-26

《CES 展会举行，虚拟现实再成焦点》2016-01-10

《HTC Vive 首届峰会召开，一呼百应 VR 产业正兴起》2015-12-21

分析师：

袁煜明

yuanyuming@xyzq.com.cn

S0190515040001

蒋佳霖

jiangjialin@xyzq.com.cn

S0190515050002

研究助理：

杨墨

yangmo@xyzq.com.cn

钱路丰

qianlf@xyzq.com.cn

马斯劼

masj@xyzq.com.cn

投资要点

- 这篇报告我们针对两个很新、但最近关注度迅速提高、又有关联性的两个概念：区块链与数字货币。我们将试图解析其定义和原理、特征与发展现状、相互的关联性、未来的应用前景。
- **区块链与数字货币受到关注。**1月20日，央行召开数字货币研讨会表示争取早日发行数字货币。此前，多家世界顶级银行加入 R3 组织制定区块链银行标准；纳斯达克完成首个基于区块链平台的交易。金融与咨询机构专家指出运用区块链技术可以提升交易透明度，减少洗钱、逃漏税等违法犯罪行为。国内外金融、证券、会计审计等行业都在加大对区块链技术的研究，并形成初步应用。区块链和数字货币正在向我们走来。
- **区块链：去中心化、去信任化的集体维护数据库技术。**区块链通过集体维护，分布式记录、储存的特征实现去中心化，通过非对称技术加密数学和可靠数据库技术完成信背书，保障区块链系统开源、透明、安全。在中心化、信任缺失的互联网时代具有显著优势。
- **区块链源于比特币，即将应用于多个领域。**比特币是区块链的一个“杀手级应用”，区块链是比特币的底层技术，且作用绝不仅仅局限在比特币上。未来，区块链有望触及金融行业底层架构，革新包括商业银行在内的金融机构基础设施。此外，区块链技术还能在法律、零售、物联、医疗等领域得到应用，使这些行业不再依靠第三方来建立信用和信息共享，提高整个行业的运行效率和整体水平。
- **央行数字货币：极有可能通过区块链技术实现。**数字货币与电子货币、虚拟货币均不同。目前央行尚未明确未来会发行何种形式的数字货币。但根据 2013 年央行曾明确表态的比特币非货币，此次定调推广的数字货币，实现形式必然与比特币不同，但极有可能应用区块链技术。区块链技术可以使整个数字货币体系中所有规则透明化，所有数据内容公开化，无法篡改和操纵，符合央行希望通过数字货币提升经济交易活动便利性和透明度的要求。同时，区块链技术还可以实现“直升机撒钱”政策，直接从央行向个人注入资金，提升货币供给控制力。
- **风险提示：**区块链技术升级速度不及预期，商业模式尚未成型，金融等政策监管风险。



目 录

1、区块链的前世今生.....	- 4 -
1.1、区块链技术近期受到关注.....	- 4 -
1.2、前世：从比特币谈起.....	- 5 -
1.3、区块链：比特币的底层技术.....	- 7 -
2、区块链技术与特点.....	- 10 -
2.1、本质：去中心化、去信任化的集体维护数据库技术.....	- 10 -
2.2、区块链基本特征.....	- 11 -
2.3、去中心化：分布式记录+分布式储存.....	- 12 -
2.4、去信任化：非对称加密数学+可靠数据库.....	- 13 -
2.5、区块链可能遇到的问题.....	- 14 -
3、区块链：现状与发展.....	- 15 -
3.1、区块链发展脉络.....	- 15 -
3.2、应用领域众多，投资火热.....	- 17 -
4、数字货币的定义与现状.....	- 21 -
4.1、数字货币定义：与电子货币、虚拟货币均不同.....	- 21 -
4.2、目前已经出现的数字货币形式.....	- 22 -
4.3、数字货币与传统货币相比的优势与劣势.....	- 25 -
5、央行数字货币：可能的实现形式.....	- 26 -
5.1、央行数字货币与比特币不同.....	- 27 -
5.2、区块链技术可能应用于央行数字货币.....	- 27 -
6、风险提示.....	- 29 -
图 1. 半年内“区块链”百度指数趋势迅速提升.....	- 4 -
图 2. 近 20% 受访者认为区块链技术将在未来 3-5 年内对金融领域产生影响..	- 5 -
图 3. 比特币的属性.....	- 5 -
图 4. 比特币节点全球分布情况.....	- 6 -
图 5. HASH 函数示意图.....	- 8 -
图 6. 全网算力与 HASH 难度同步增长.....	- 8 -
图 7. 比特币的交易过程.....	- 9 -
图 8. 区块链的局部结构.....	- 9 -
图 9. 比特币中的区块链如何工作.....	- 10 -
图 10. DPOS\POW\POS 三种证明方式对比.....	- 11 -
图 11. 传统隐私保护模式与区块链下的新隐私保护模式.....	- 12 -
图 12. 中心化结构与去中心化结构.....	- 13 -
图 13. 私钥、公钥间的关系.....	- 14 -
图 14. 过去两年区块链数据库空间占用情况.....	- 15 -
图 15. 区块链在金融领域的应用.....	- 16 -
图 16. 区块链可以应用在多个领域.....	- 18 -
图 17. 区块链可以使通信更加快捷安全.....	- 18 -
图 18. 尝试应用区块链的金融机构.....	- 19 -
图 19. 飞利浦医疗和 TIERON 合作通过区块链完成病历资料认证.....	- 20 -
图 20. Skuchain，一种新的供应链模式.....	- 20 -
图 21. 数字黄金货币发展史.....	- 23 -
图 22. 排名前五的加密货币市值占比情况.....	- 23 -
图 23. 排名前十的加密货币.....	- 24 -

图 24. 比特币价格波动情况（2012 年 12 月 13 日至 2016 年 1 月 27 日）	- 24 -
图 25. 人们对加密货币的熟悉程度	- 25 -
图 26. 加密货币的使用情况	- 25 -
图 27. 数字货币与传统货币相比的优势与劣势	- 26 -
图 28. 区块链实现“直升机撒钱”	- 28 -
表 1. 比特币发展简史	- 6 -
表 2. 区块链大事记	- 17 -
表 3. 区块链代表性投资事件	- 21 -
表 4. 电子货币、虚拟货币和数字货币的对比	- 22 -
表 5. 央行数字货币和比特币的区别	- 27 -

报告正文

1、区块链的前世今生

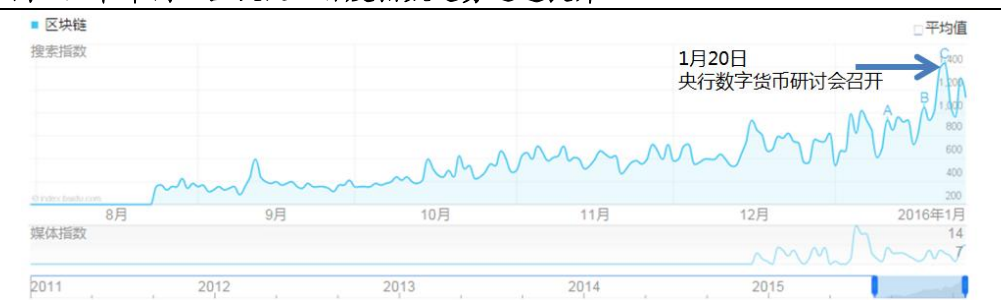
1.1、区块链技术近期受到关注

2016 年 1 月 20 日，中国人民银行数字货币研讨会在北京召开，来自人民银行及国内外知名机构的数字货币研究专家进行了研讨和交流。会后央行表示，将争取早日发行数字货币，以降低传统纸币发行、流通成本，提升经济交易活动便利性和透明度，更好支持经济和社会的发展。

这是继 2013 年 12 月央行等五部委发布关于防范比特币风险的通知之后，第一次对数字货币表示明确的态度。

尽管央行并未明确提出将数字货币将以何种形式发行，但根据与会专家态度和央行“提升交易便利性和透明度”的要求，我们认为，央行未来推出的数字货币很有可能会使用到比特币的核心技术——区块链。区块链（Blockchain）是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案，可以有效提升交易透明度，减少洗钱、逃漏税等违法犯罪行为。在央行的明确表态后，数字货币与区块链技术受到业界更多关注。

图 1. 半年内“区块链”百度指数趋势迅速提升

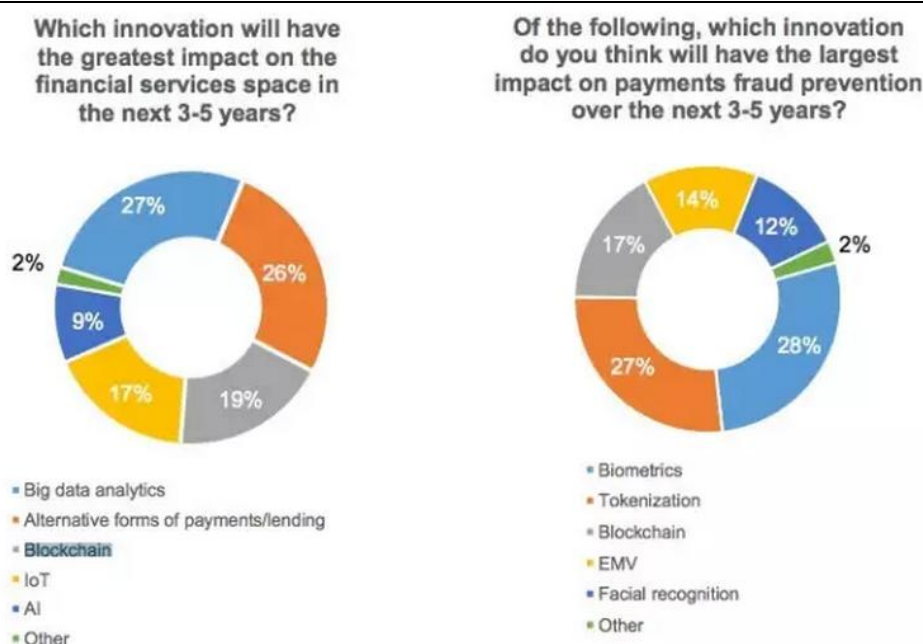


资料来源：百度指数、兴业证券研究所

事实上，在此次央行表态前，区块链技术已经开始进入公众视野，并在世界各国的银行、证券、会计审计、政府政策等领域开始被应用。

2014 年以来，包括巴克莱银行，瑞士信贷银行，摩根大通在内多家世界顶级银行都已经加入了由金融科技公司 R3 领导的组织，着手为区块链技术在银行业中的使用制定行业标准和协议，截止目前全球范围内加入由区块链技术公司 R3 联盟的银行已超过 42 家。一家叫 Magister Advisor 的公司认为，到 2017 年银行在区块链开发的经费将超过 10 亿美元，这个数值是所有企业软件板块发展速度最快的。纳斯达克在 2015 年 12 月 30 日完成了基于区块链平台的首个证券交易，推出基于区块链的数字分类账技术 Lin 进行股票的记录交易与发行，这对于全球金融市场的去中心化有着里程碑的意义。会计审计领域，在继德勤与安永宣布进军区块链之后，普华永道也正式宣布加入区块链行业。公众对区块链的兴趣也在增加，根据 Capital One 对 2015 年拉斯维加斯 Money20/20 会议的 151 名与会者的访问，有近 20% 的与会者认为区块链技术在未来的三到五年内，将会对金融服务领域有着很大的影响。

图 2. 近 20%受访者认为区块链技术将在未来 3-5 年内对金融领域产生影响




资料来源：Capital One、兴业证券研究所

除了在国外备受关注，国内也正在加大区块链的研究和投入。开发区块链应用的井通中国日前受到川财证券、安邦资产、泰达宏利、等十余家国内重量级公私募基金和证券信托的联合调研。全球共享金融 100 人论坛近日也在京宣布成立了“中国区块链研究联盟”，共同谋划区块链未来的发展。相信这一发展趋势在央行数字货币研讨会后将继续下去，区块链技术正在向我们走来。

1.2、前世：从比特币谈起

2008年11月1日，一位化名中本聪（Satoshi Nakamoto）的计算机程序员，在MIT计算机系统安全组的网站上发表了一篇篇幅仅8页的学术论文，《Bitcoin: A Peer-to-Peer Electronic Cash System》，中本聪描述了一种完全基于点对点（Point to Point, P2P）的电子现金系统，该系统使得全部支付都可以由交易双方直接进行完全摆脱了通过第三方中介例如商业银行的传统支付模式从而创造了一种全新的货币体系。2009年1月，第一个序号为0的比特币的区块——创世区块诞生。几天后的1月9日出现序号为1的区块，并与序号为0的创世区块相连接形成了链，标志着比特币区块链诞生。

图 3. 比特币的属性

	去中心化	低交易费用
	全世界流通	无隐藏成本
	专属所有权	跨平台挖掘

资料来源：兴业证券研究所

比特币创始之初，很长时间内只在技术工程师之间以娱乐为目的进行流通，只能属于一种“小众货币”。第一个比特币交易发生于2009年1月12日，中本聪发送了

10比特币给密码学专家哈尔·芬尼。2010年5月21日，佛罗里达程序员用1万比特币购买了价值25美元的披萨优惠券，随着这笔交易诞生了比特币第一个公允汇率。自此以后，比特币与实物的交换以这种间接模式慢慢开始。据Coin Desk估算，目前全球大约有60000个商家接受比特币。在线下世界，大概有4000个经营场所允许使用比特币。随着比特币的被接受性的提高，一些针对主要货币的比特币交易所也陆续出现。截至2013年底，根据Blockchain.info组织的统计，有近14万个网络地址参与比特币交易，交易量为每天6万次，而全球最大的比特币交易平台为比特币中国、Mt.Gox和Bitstamp，所占市场份额分别为32.5%、26%、20.7%。中国成为比特币交易增长最迅速的国家，有超过15家大型的比特币的交易平台处理比特币相关的业务。

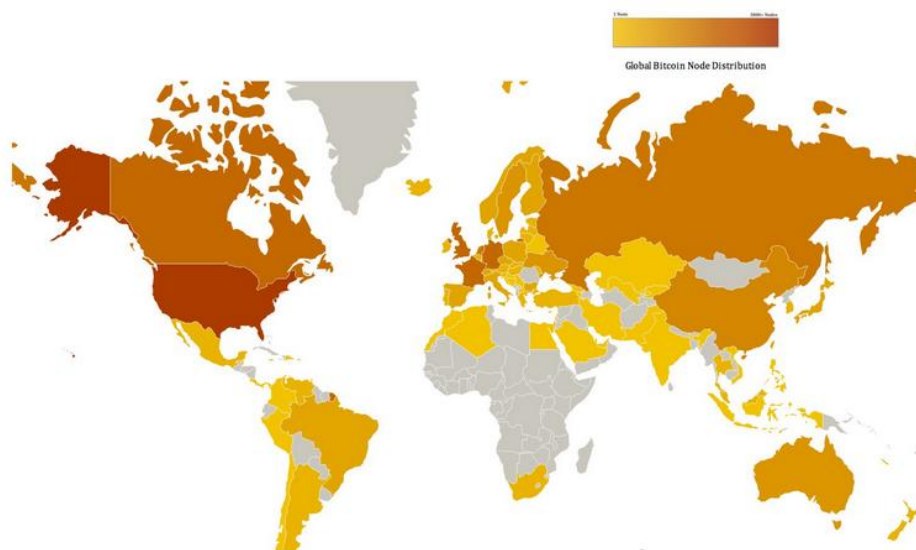
表 1. 比特币发展简史

时间	事件
2008年11月	中本聪发表《Bitcoin: A Peer-to-Peer Electronic Cash System》，提出比特币概念
2009年1月	第一个序号为0的比特币的区块——创世区块诞生，几天后的1月9日出现序号为1的区块，并与序号为0的创世区块相连接形成了链
2009年1月12日	第一个比特币交易发生，中本聪发送了10比特币给密码学专家哈尔·芬尼
2010年5月21日	第一个比特币实体交易发生，佛罗里达程序员用1万比特币购买了价值25美元的披萨优惠券
2010年7月	第一个比特币平台成立，新用户暴增，价格暴涨
2011年2月	比特币价格首达1美元，英镑、巴西雷亚尔、波兰兹罗提汇兑交易平台成立
2013年11月	比特币价格达到历史高峰，盘中高达1242美元
2014年	中国成为比特币交易增长最迅速的国家，有超过15家大型的比特币的交易平台处理比特币相关的业务。
2016年1月	比特币逐渐受到质疑，著名比特币挖掘者套现离场

资料来源：互联网、兴业证券研究所

比特币交易所的出现，鼓励投资者用各国法币进行兑换。在大量投资者参与下，比特币价格一路上升，从最初的零点几美元，到2013年11月29日，仅用了四年时间，就达到历史高峰，盘中高达1242美元，一度超过1盎司黄金。其后，比特币价格有所回落，经过6年的发展，目前比特币总体市值已过100亿美元，节点遍布世界各地。

图 4. 比特币节点全球分布情况



资料来源：Coinviz、兴业证券研究所

然而，时至今日，比特币也出现了许多问题。包括：

比特币加大了金融监管的难度。在金融监管过程中，几乎所有国家都非常依赖银行系统来查验交易的资金进出。而比特币独立的支付网络则有效地躲开了这种追查途径，使得监管资金动向非常困难。比特币由于其匿名特性，比特币成为犯罪资金的主要载体，在许多非法网站上，甚至成为唯一支付手段。

挖矿行为演变为军备竞赛增加了比特币体系的资源消耗。昂贵的专用矿机提高了挖矿的效率，使得传统的采矿技术无法生存，随着时间的推移和竞争的加剧，整个比特币产业链成为极端资本密集型行业。

交易确认的时间限制了比特币的使用范围。因为每个比特币区块的产生需要10分钟，因此每笔交易的验证，也需要10分钟。比特币的优势，仍限于互联网领域，在实体经济中，只有对时间不敏感的消费场所如餐馆等，才会成为比特币使用的理想场所。

2016年1月，著名比特币挖掘者公开表示，比特币基本面已经被打破，其价格无论在短期内还是在长期内都应当并有可能下行，随后将持有的比特币套现离场。比特币在争议中，已失去当年的光芒。

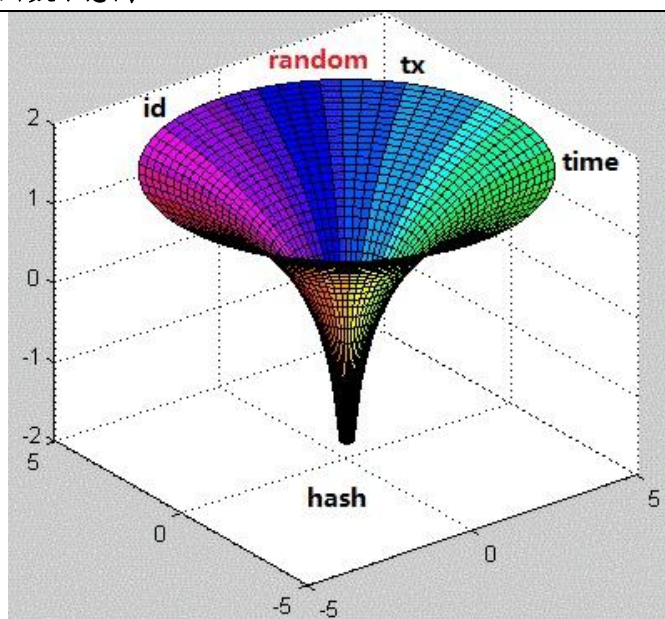
1.3、区块链：比特币的底层技术

在过去的一年中，尽管比特币本身受到质疑，然而人们开始从比特币的支付领域逐渐转移到了比特币底层协议区块链技术上，越来越多投资者及普通民众接受了比特币底层技术区块链的概念。我们可以通过了解比特币的生成与交易等一系列过程，理解区块链技术。

比特币的生成。比特币的产生需要依据特定的算法，通过大量复杂的运算才能生成，俗称“挖矿”。挖矿就是指产生新区块并计算随机数的过程，以解决一项复杂的数学问题来保证比特币网络分布式记账系统的一致性。

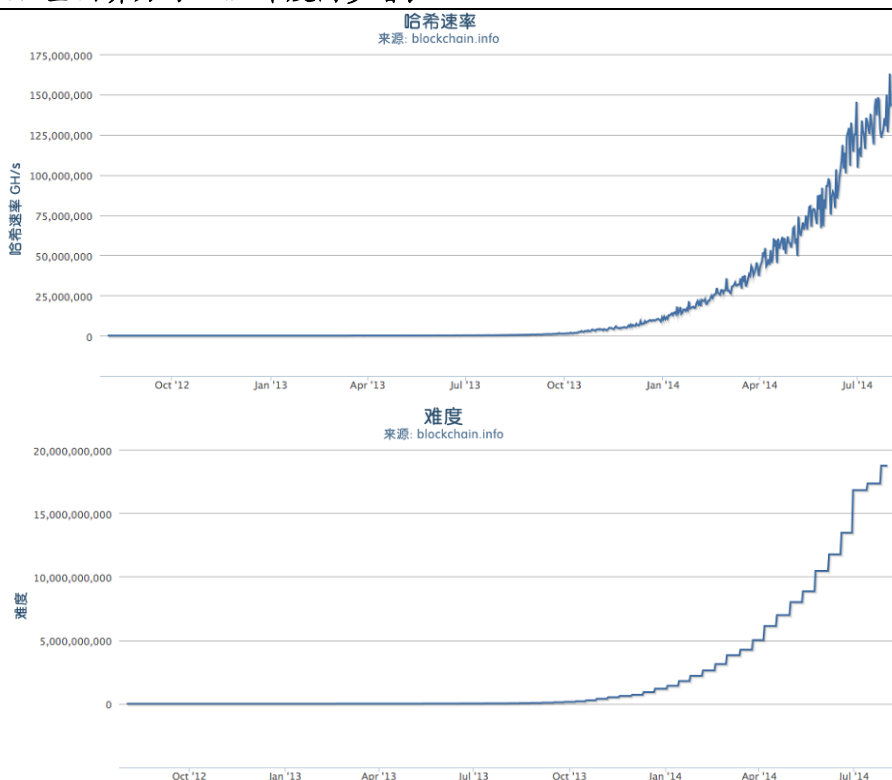
这一项复杂的数学问题为寻找一个**随机数散列值（也称为哈希值）**。散列值由散列函数生成，散列函数的功能是将任意长度的不同信息（例如数字、文本或其他信息）转化为长度相等但内容不同的二进制数列（由0和1组成）。比特币采用的是散列算法中的SH256算法，任意长度的信息输入通过这个函数都可以转换成一组长度为256个的二进制数字，以便统一的存储和识别。256个0或1最多可以组合成 2^{256} 个不同的数，这个庞大的集合能够满足与比特币相关的任何标记需要。且散列还有一个重要特征，若想要生成一个特殊的输出数字，只能通过随机尝试的办法逐个进行正向运算，而不能由输出结果逆向推出输入信息。这个特征是比特币能够顺利运行的重要基石。挖矿就是通过改变随机数来生成不同的散列值，直到符合要求。随着全网算力提高，找到散列值的难度也会提升，从而维持10分钟找到一次的频率。

图 5. HASH 函数示意图



资料来源：《区块链：一种去中心化的公开记录系统》、兴业证券研究所

图 6. 全网算力与 HASH 难度同步增长

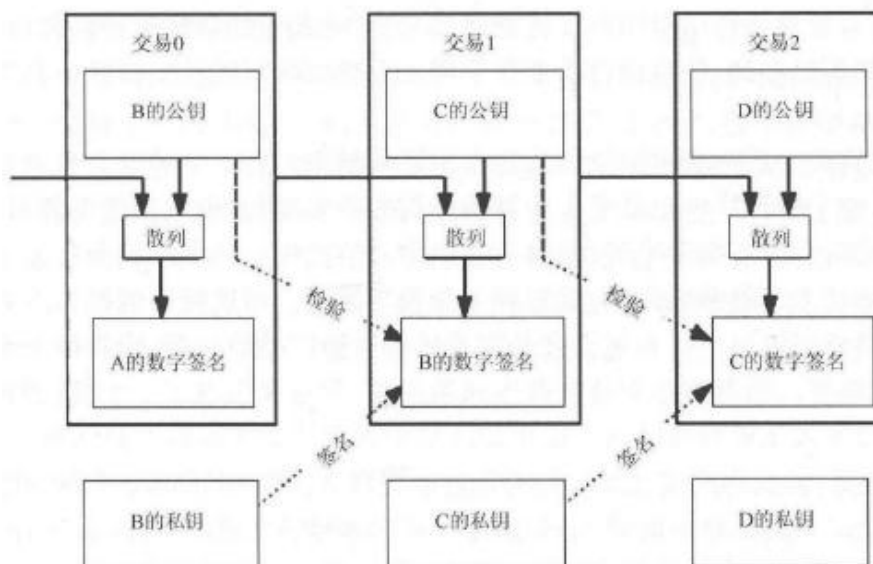


资料来源：blockchain.info、兴业证券研究所

比特币的交易。比特币使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为。在信息传递过程中，发送方通过一把密钥将信息加密接收方在收到信息后，再通过配对的另一把密钥对信息进行解密这就保证了信息传递过程的私密性与安全性。比特币的交易并非简单的支付货币本身。下图中的交易1为例，如果B想支付100个比特币给C,那么不仅B需要在交易单上注明金额，而且需要注明这100个比特币的来源。由于每笔交易单都记录了该笔资金的前一个

拥有者、当前拥有者以及后一个拥有者，我们就可以依据交易单实现对资金的全程追溯。这也是比特币的典型特征之一。最后，当每一笔交易完成时，系统都会向全网进行广播，告诉所有用户这笔交易的实施。

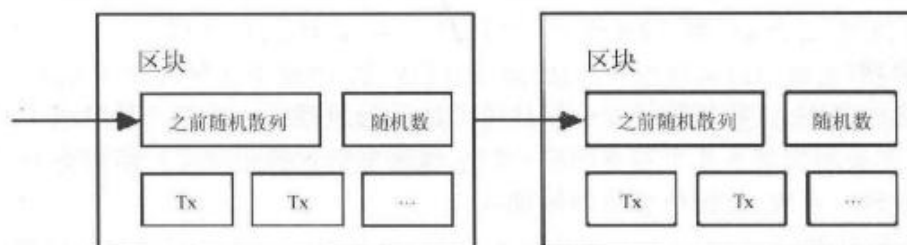
图 7. 比特币的交易过程



资料来源：《Bitcoin: A Peer-to-Peer Electronic Cash System》、兴业证券研究所

区块+链。由于每笔交易是相对分散的，为了更好地统计交易，比特币系统创造了区块这一概念。每个区块均包含以下三种要素：一是本区块的ID（散列）二是若干交易单；三是前一个区块的ID（散列）。比特币系统大约每十分钟创建一个区块，其中包含了这段时间里全球范围内发生的所有交易。每个区块中也包含了前一个区块的ID，这种设计使得每个区块都能找到其前一个节点，如此可一直倒推至起始节点，从而形成了一条完整的交易链条。因此，从比特币的诞生之日起，全网就形成一条唯一的主区块链，其中记录了从比特币诞生以来的所有交易记录并以每十分钟新增一个节点的速度无限扩展。这条主区块链在每添加一个节点后，都会向全网广播，从而使得每台参与比特币交易的电脑上都有一份拷贝。在现实世界里每笔非现金交易都由银行系统进行记录，一旦银行计算机网络崩溃所有数据都会遗失。而在互联网世界里，比特币的所有交易记录都保存在全球无数台计算机中，只要全球有一台装有比特币程序的计算机还能工作，这条主区块链就可以被完整地读取。如此高度分散化的交易信息存储，使得比特币主区块链完全遗失的可能性变得微乎其微。

图 8. 区块链的局部结构



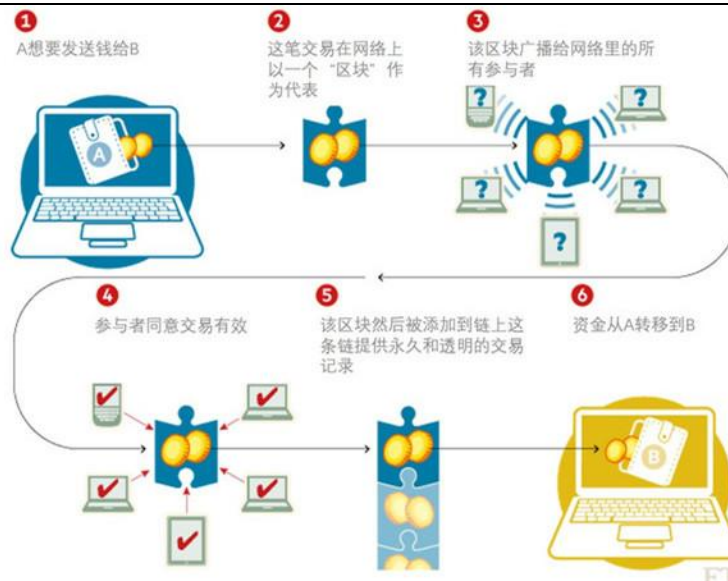
资料来源：《Bitcoin: A Peer-to-Peer Electronic Cash System》、兴业证券研究所

每个人在对交易的有效性进行验证后都可以根据这些交易数据生成新区块。为了避免虚假交易或重复交易，使这一新区块被信任，需要构建**工作量证明机制**。

如果想要修改某个区块内的交易信息，就必须完成该区块及其后续连接区块的所有工作量，这种机制大幅提高了篡改信息的难度。同时，工作量证明也解决了全网共识问题，全网认可最长的链，因为最长的链包含了最大的工作量。

比特币与区块链。综上所述，区块链是一串使用密码学方法相关联产生的数据块。在比特币的应用中，整个区块链就是比特币的公共账本，网络中的每一个节点都有比特币交易信息的备份。当发起一个比特币交易时，信息被广播到网络中，通过算力的比拼而获得合法记账权的矿工将交易信息记录成一个新的区块连接到区块链中，一旦被记录，信息就不能被随意篡改。比特币是区块链的一个“杀手级应用”，区块链是比特币的底层技术，且作用绝不仅仅局限在比特币上。因此，尽管比特币与区块链经常被同时提及，但二者并不能画上等号。

图 9. 比特币中的区块链如何工作



资料来源：FT 中文网、兴业证券研究所

2、区块链技术与特点

2.1、本质：去中心化、去信任化的集体维护数据库技术

区块链是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案让参与系统中的任意多个节点，把一段时间系统内全部信息交流的数据，通过密码学算法计算和记录到一个数据块（block），并且生成该数据块的指纹用于链接（chain）下个数据块和校验，系统所有参与节点来共同认定记录是否真。

区块链是一种类似于 NoSQL（非关系型数据库）的技术解决方案统称，并不是某种特定技术，能够通过很多编程语言和架构来实现区块链技术。并且实现区块链的方式种类也有很多，目前常见除上文提到运用于比特币的 POW（Proof of Work，工作量证明）外，还有 POS（Proof of Stake，权益证明），DPOS（Delegate Proof of Stake，股份授权证明机制）等。

POW 工作量证明。一方（通常为证明者）提交已知难于计算但易于验证的计算结果，而其他任何人都能够通过验证这个答案就确信证明者为了求得结果已经完

成了量相当大的计算工作。现代第一个应用是 Adam Back 于 1996 年提出的以基于 SHA256 的工作量证明为反垃圾邮件手段的“Hashcash”。系统通过要求所有邮件发送时都必须完成大强度的工作量证明，这将使垃圾邮件发送者发大量电子邮件变得很不划算却仍允许用户们在需要时向其他用户正常发送邮件。现在比特币为了同样的目的使用了一个类似它的系统，而 Hashcash 的算法也已经被改造为以“挖矿”为形式的比特币安全的核心。这一方法存在缺陷：工作量证明浪费资源，比特币网络每秒完成 600 万亿次 SHA256 运算，而最终这些计算没有任何实际或科学价值。

POS 权益证明。POS 权益证明法是一种 SHA256 的替代方法，这一方法在最近几年才开始出现：在比特币发明的 2008 年，没有能安全地与密码协议互动的数字财产。POS 法从根本上解决了工作量计算浪费的问题，它不要求证明者完成一定数量的计算工作，而是要求证明者对某些数量的钱展示所有权，通过每一笔交易销毁的币天数（coin days）来实现，币天数代表一个特定的币距最后一次在网络上交易的时间。在给定的时间点，只存在有限的币天数，它们在那些长期持有大量货币结余的人手中持续增加。所以币天数可被视为在网络中权益的代表（proxy）。每当这些币有交易时，币天数即被销毁，因此不能被重复使用。

DPOS 股份授权证明机制。股份授权证明机制（DPOS）是一种新的保障加密货币网络安全的算法。它在尝试解决比特币采用的传统工作量证明机制（POW）以及点点币和 NXT 所采用的股份证明机制（POS）的问题的同时，还能通过实施科技式的民主以抵消中心化所带来的负面效应。一共有 101 位受托人通过网络上的每个人经由每次交易投票产生，他们的工作是签署（生产）区块，且在每个区块被签署之前，必须先验证前一个区块已经被受信任节点所签署。区别于其他保障加密货币安全的算法，DPOS 体系里每个客户端都能够决定谁能够被信任，而不用必须信任拥有最多资源的人。

图 10. DPOS\POW\POS 三种证明方式对比

特征	DPOS	POW	PPC POS
不鼓励权力集中	✓	✗	✗
承载更多的交易量	✓	✗	✗
更快的确认速度	✓	✗	✗
高效节能	✓	✗	✓
鼓励开发	✓	✗	✓

资料来源：中文维基、兴业证券研究所

2.2、区块链基本特征

结合定义区块链的定义，区块链会现实出四个主要的特性：去中心化（Decentralized）、去信任（Trustless）、集体维护（Collectively maintain）、可靠数据库（Reliable Database）。

去中心化（Decentralized）：整个网络没有中心化的硬件或者管理机构，任意节点之间的权利和义务都是均等的，且任一节点的损坏或者失去都会不影响整个系统的运作。因此也可以认为区块链系统具有极好的健壮性。

去信任（Trustless）：参与整个系统中的每个节点之间进行数据交换是无需互相信任的，整个系统的运作规则是公开透明的，所有的数据内容也是公开的，因此在

系统指定的规则范围和时间范围内，节点之间是不能也无法欺骗其它节点。

集体维护 (Collectively maintain): 系统中的数据块由整个系统中所有具有维护功能的节点来共同维护的，而这些具有维护功能的节点是任何人都可以参与的。

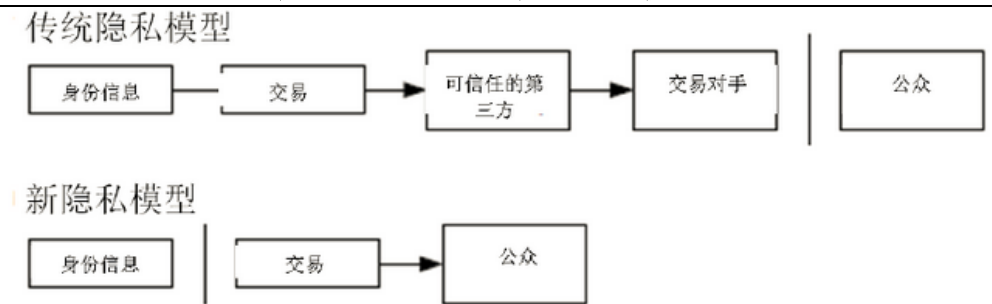
可靠数据库 (Reliable Database): 整个系统将通过分数据库的形式，让每个参与节点都能获得一份完整数据库的拷贝。除非能够同时控制整个系统中超过 51% 的节点，否则单个节点上对数据库的修改是无效的，也无法影响其他节点上的数据内容。因此参与系统中的节点越多和计算能力越强，该系统中的数据安全性越高。

并且由以上四个特征会引申出另外 2 个特征：开源 (Open Source)、隐私保护 (Anonymity)。如果一个系统不具备这些特征，将不能视其为基于区块链技术的应用。

开源 (Open Source): 由于整个系统的运作规则必须是公开透明的，所以对于程序而言，整个系统必定会是开源的。

隐私保护 (Anonymity): 由于节点和节点之间是无需互相信任的，因此节点和节点之间无需公开身份，在系统中的每个参与的节点的隐私都是受到保护

图 11. 传统隐私保护模式与区块链下的新隐私保护模式

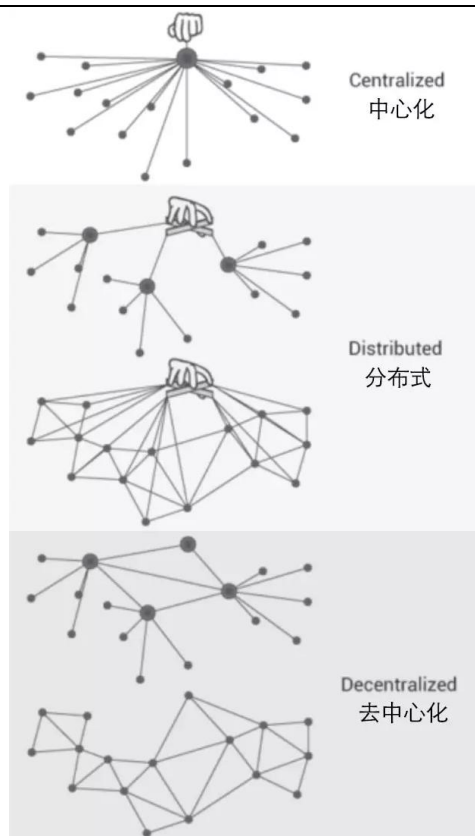


资料来源：《Bitcoin: A Peer-to-Peer Electronic Cash System》、兴业证券研究所

2.3、去中心化：分布式记录+分布式储存

区块链最大的特点为：去中心化。目前传统数据库是中心化记录、中心化储存的，即使是异地灾备、云存储，也只是将存储地从一处变为多处，从本地变为云端，如果中央服务器出现问题，则灾备数据库也将停止更新数据；而区块链数据库则是分布式记录、分布式储存、分布式传播的，每一条信息都由单个节点传播给全网其它所有节点，每个节点都负责数据的记录、储存，没有中心化或第三方机构负责管理，一个节点出现问题，其他节点会继续数据的更新和存储，通过去中心化的方式，维持系统稳定运行，信息完整可靠。

图 12. 中心化结构与去中心化结构



资料来源: okTurtles Foundation、兴业证券研究所

分布式记录。区块链与传统网络记录体系不同，没有设立中心记录者，而是通过建立公开记录体系，使全网每一个节点在参与记录的同时也来验证其他节点记录结果的正确性，在全部参与者确认后完成信息记录，以确保记录结果真实性。

分布式储存。在中心化体系中，每项数据都由中心系统进行记录，一旦中心点计算机网络崩溃所有数据都会遗失。而区块链使得全网全部数据同时储存于系统所有节点中，只要全网有一个节点保持正常运作，这条主区块链就可以被完整地读取。如此高度分散化的交易信息存储，使得主区块链完全遗失的可能性变得微乎其微。

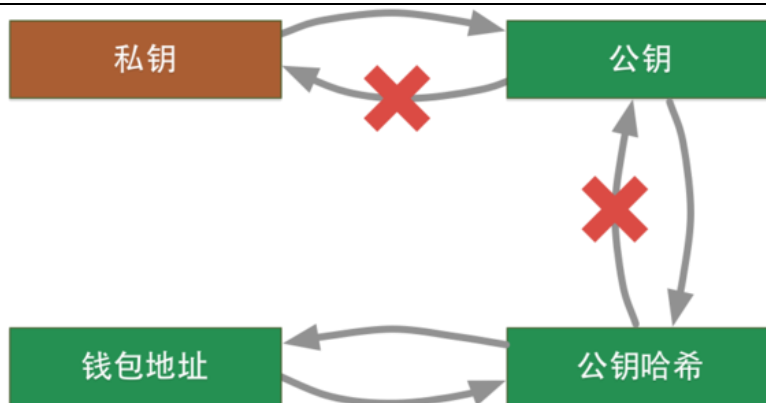
2.4、去信任化：非对称加密数学+可靠数据库

在传统的互联网模式中，是通过可信任的中央节点或第三方通道进行信息的匹配验证和信任积累，这些中央节点或通道是否可信任对整个体系信用影响极大。而区块链，通过数学方解决了信任问题，依靠非对称加密和可靠数据库完成了信用背书，所有的规则事先都以算法程序的形式表述出来，参与方不需要知道交易对手信用度，更不需要借助第三方机构来进行交易背书或者担保验证，而只需要信任共同的算法就可以建立互信，通过算法为参与者创造信用、产生信任和达成共识，完成去信任化。

非对称加密：区块链通过数学共识机制是非对称加密算法，即在加密和解密的过程中使用一个“密钥对”，“密钥对”中的两个密钥具有非对称的特点：一是用其中一个密钥加密后，只有另一个密钥才能解开；二是其中一个密钥公开后，根据公开的密钥其他人也无法算出另外一个密钥。在区块链的应用场景中，一是加密时的密钥是公开所有参与者可见的（公钥），每个参与者都可以用自己的公钥来加

密一段信息（真实性），在解密时只有信息的拥有者才能用相应的私钥来解密（保密性），用于接收价值。二是使用私钥对信息签名，公开后通过其对应的公钥来验证签名，确保信息为真正的持有人发出。非对称加密使得任何参与者更容易达成共识，将价值交换中的摩擦边界降到最低，还能实现透明数据后的匿名性，保护个人隐私。

图 13. 私钥、公钥间的关系



资料来源：巴比特、兴业证券研究所

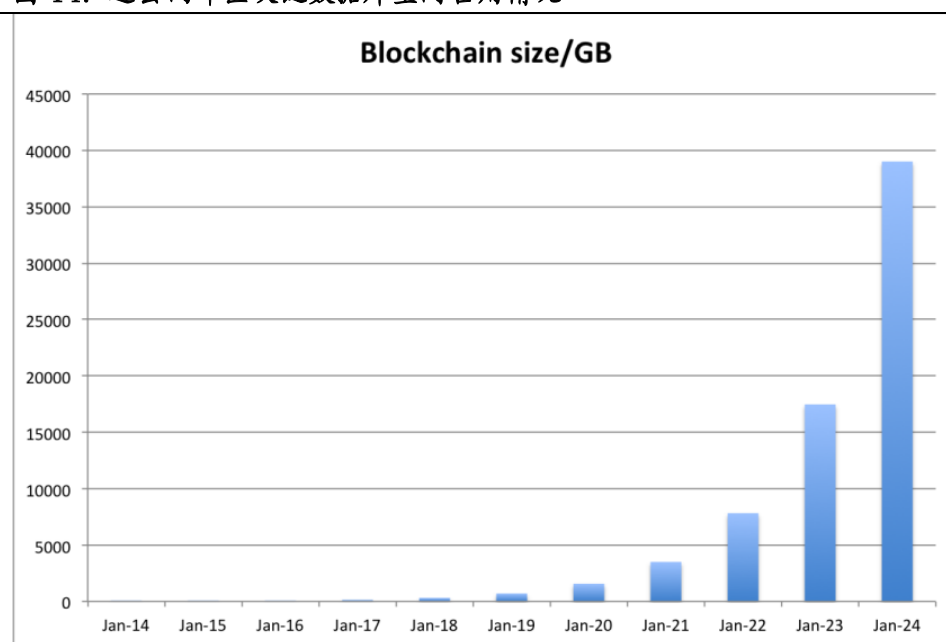
可靠数据库。整个系统将通过分数据库的形式，让每个参与节点都能获得一份完整数据库的拷贝。除非能够同时控制整个系统中超过 51% 的节点，否则单个节点上对数据库的修改是无效的，也无法影响其他节点上的数据内容。而在实际中，发动 51% 攻击是无意义的，为掌握全网 51% 算力所需投入的成本，远远大于成功实施攻击后获得的收益，因此，从理论上来说，区块链技术可以保障数据库安全可靠，且参与系统中的节点越多和计算能力越强，该系统中的数据安全性越高。

2.5、区块链可能遇到的问题

目前，区块链应用还处于初级阶段，面临着诸多问题。以区块链最成熟的应用比特币为例：

首先，技术层面上，网络容量首当其冲。正如我们看到的，每隔 10 分钟便有一个区块增加至账单中。由于区块的容量相当有限（1MB），这个网络每秒钟只能处理 7 笔交易。有关区块容量的争论也在今年浮出水面：部分挖矿者开始将区块的容量增至 8MB。区块的容量每隔两年会增长一倍。由此提出的一个问题是，如果 Bitcoin XT 覆盖了整个网络的 75%，那么这个网络会完全采用新的区块大小。更为普遍的是，这场辩论是围绕一个问题展开，即区块链是应该以较低费率来处理大量交易，还是以较高费率来处理少量交易。

图 14. 过去两年区块链数据库空间占用情况



资料来源：blockchain.info、兴业证券研究所

其次，在安全层面上，许多比特币交易平台或遭到黑客攻击或被迫关闭，使得数以百万计的比特币凭空消失。比如15年一月份，世界第三大比特币交易所 Bitstamp 因一次黑客攻击丢失了 540 万美元的比特币。随后，总部位于斯洛文尼亚的这家公司被迫停止交易。这次攻击大约损失了 19000 个比特币。这一幕同样可能发生在通过区块链交易的资产上。而比黑客攻击更尴尬的是，丢失私钥的用户将无法挽回自己的资产。

再次，政策层面上，“去中心化”让中心化的政府疑虑重重，监管政策不乐观，而对于一个分散式网络来说，监管本身的难度也不小。此外，不少业内人士还抱怨人们对区块链的理解程度和接受意愿不够，这导致新技术及新应用很难推广。

但对于任何新生事物而言，这都是必须跨越的障碍，对于区块链应用也是如此。越来越高的媒体关注度与越来越深入的专业讨论，必然会逐渐加深人们对区块链的理解并提高人们的接受意愿。随着更多相关研究，以上问题很有可能得到解决。

3、区块链：现状与发展

3.1、区块链发展脉络

区块链开始引人关注，与比特币的风靡密切相关。直至今日，莱特币、狗狗币等类比特币层出不穷，人们对于电子货币的关注已经转向了对区块链的深入研究。区块链强大的容错功能，使得它能够在没有中心化服务器和管理的情况下，安全稳定地传输数据。从诞生到现在，区块链专家 Melanie Swan 将区块链发展划分为三个阶段：区块链 1.0、2.0、3.0。

区块链 1.0：以比特币为代表的可编程货币

比特币设计的初衷，是为构建一个可信赖的自由、无中心、有序的货币交易世界，尽管比特币出现了价格剧烈波动、挖矿产生的巨大能源消耗、政府监管态度不明

等各种问题，但可编程货币的出现让价值在互联网中直接流通交换成为了可能。可编程的意义是指通过预先设定的指令，完成复杂的动作，并能通过判断外部条件作出反应。可编程货币即指定某些货币在特定时间的专门用途，这对于政府管理专款专用资金等有着重要意义。

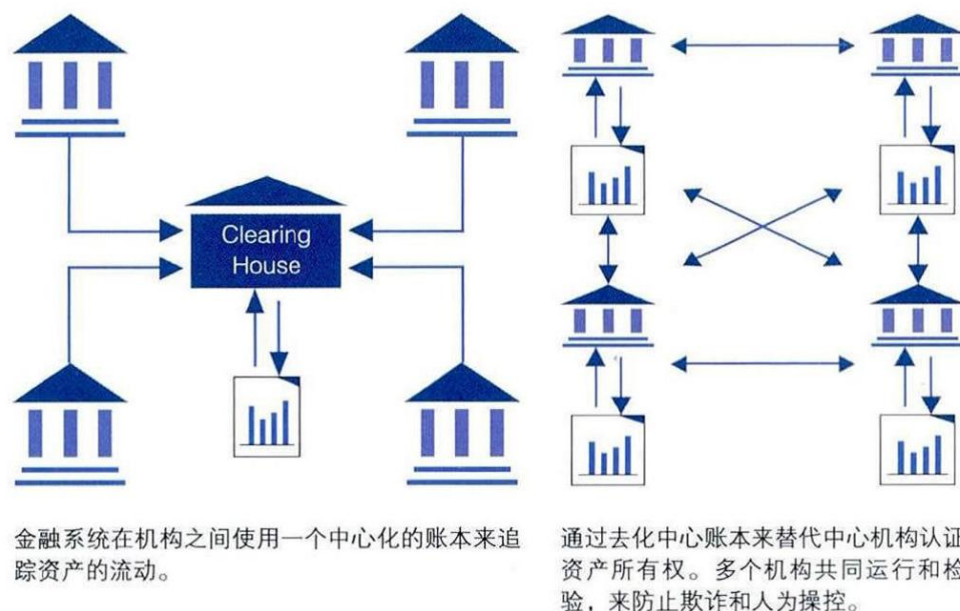
区块链是一个全新的数字支付系统，其去中心化、基于密钥的毫无障碍的货币交易模式，保证安全性同时大大降低了交易成本，对传统的金融体系可能产生颠覆性影响，也刻画出一幅理想的交易愿景——全球货币统一，使得货币发行流通不再依靠各国央行。1.0 设置了货币的全新起点，但构建全球统一的区块链网络还有很长的路要走。

区块链 2.0：基于区块链的可编程金融

数字货币的强大功能，吸引了金融机构采用区块链技术开展业务，人们试着将“智能合约”加入区块链形成可编程金融。目前，可编程金融已经在包括股票、私募股权等领域有初步的应用，包括目前交易所积极尝试用区块链技术实现股权登记、转让等功能；华尔街银行联合想要打造的区块链行业标准，提高银行结算支付的效率，降低跨境支付的成本。

目前商业银行基于区块链的应用领域主要有：一是点对点交易。如基于 p2p 的跨境支付和汇款、贸易结算以及证券、期货、金融衍生品合约的买卖等；二是登记。区块链具有可信、可追溯的特点，因此可作为可靠的数据库来记录各种信息，如运用在存储反洗钱客户身份资料及交易记录上；三是确权。如土地所有权、股权等合约或财产的真实性验证和转移等；四是智能管理。即利用“智能合约”自动检测是否具备生效的各种环境，一旦满足了预先设定的程序，合同会得到自动处理，比如自动付息、分红等。目前，包括商业银行在内的金融机构都开始研究区块链技术并尝试将其运用于现实，现有的传统金融体系正在被颠覆。

图 15. 区块链在金融领域的应用



资料来源：《区块链：金融的另一种可能》、兴业证券研究所

区块链 3.0：区块链在其他行业的应用

除了金融行业，区块链在其他领域也开始应用。在法律、零售、物联、医疗等领域，区块链可以解决信任问题，不再依靠第三方来建立信用和信息共享，提高整个行业的运行效率和整体水平。基于此，人们尝试用区块链颠覆互联网底层协议，把人类的统一语言、经济行为、社会制度乃至生命都写就为一个基础软件协议。统一语将人类各民族自然语言统一为一种低熵值的表达形式并提供了它与计算机

语言的接口；人类经济行为、社会制度体系和生命再生机制统称为时间货币系统。
 区块链 3.0 即是集成了统一语和时间货币的分布式人工智能操作系统。

表 2. 区块链大事记

时间	关键词	事件
2008	《Bitcoin: A Peer-to-Peer Electronic Cash System》	中本聪的人发表了论文《比特币：一种点对点的电子现金系统，提出区块链的概念，区块链进入人们视野
2009	比特币	比特币作为区块链首个应用，在开源区块链上顺利运行
2012	Ripple	瑞波（Ripple）系统发布，跨过转账引入区块链技术
2013	MEC	美卡币（MEC）区块链断裂，交易中断，1 天后美卡币重新接回区块链重生
2014	应用与突破	4 月，Austin Hill 和 Adam Back 在比特币区块链基础上构建侧链 5 月，Storj 采用区块链技术为用户提供服务 6 月，搜索引擎 DuckDuckGo 接入区块链查询 8 月，区块链并购投资火热，区块链服务商 Chain 获 950 万美元投资 10 月，Tilecoin 发布集成物联网实验设备
2015	金融机构	传统银行等金融机构开始测试并尝试使用区块链技术

资料来源：互联网、兴业证券研究所

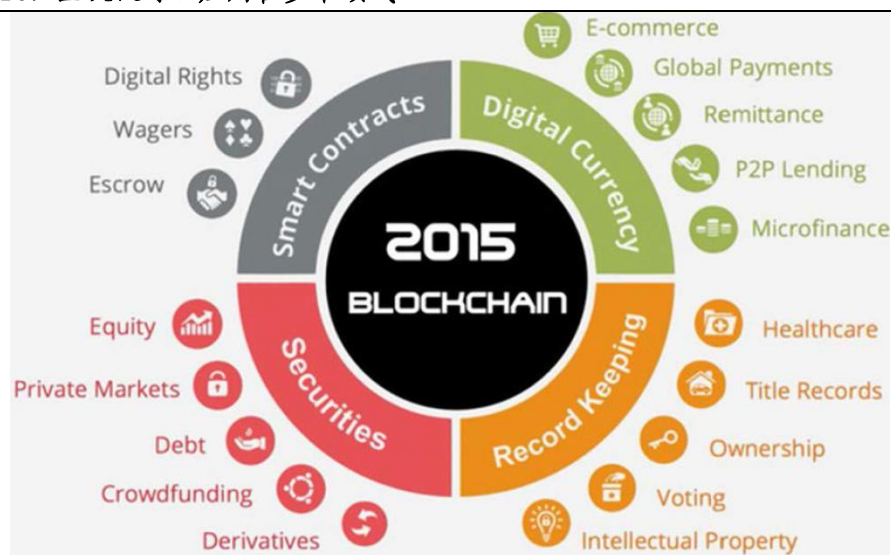
90 年代，信息技术的飞速发展变革了现代社会，数据计算、数据库应用等为互联网技术应用打下基础，从深度和广度方面拓宽了人们的世界观。人们从对比特币的关注，到区块链技术在金融领域大展身手，进入 2015 年，区块链在建立去中心化信用的尝试，已经不限于金融界，而被社会各个领域关注，特别是在中国，目前社会的公信力普遍不足的情况下，区块链更能为社会管理提供一种全新的思路和技术选项。我们认为，区块链技术发展阶段处于 2.0 在 3.0 之间，比特币的成功和金融领域的尝试性运用，社会对区块链的关注度和投资热度急剧提升，区块链技术的发展进入黄金时期。

区块链飞速发展，描绘了世界基于技术的统一愿景，整个社会有望进入智能互联网时代，形成一个可编程的社会。在这个信用已经成为紧缺资源的时代，区块链的技术创新，作为一种分布式信用的模式，为全球市场的金融、社会管理、人才评价和去中心化组织建设等，都提供了一个广阔的发展前景。

3.2、应用领域众多，投资火热

区块链的应用场景大致可分为数字货币、记录保存、智能合约和证券。具体包括跨境支付、电子商务、投票、公证、知识产权保护、证券发行交易、众筹、契约、担保等各类社会事务。无论是公证、医疗、房地产还是物联网领域，只有过多的中介参与，过高的中介成本或者是低追踪成本和高信息安全的需求，都会有区块链技术的用武之地。

图 16. 区块链可以应用在多个领域



资料来源：Coindesk、兴业证券研究所

通信：通信领域是最早的区块链应用之一。传统的通信程序都是考虑如何用最短的时间和路径传送信息，如今，除了速度，安全性成了关注重点，基于区块链的比特信（Bitmessage）应运而生。区别与传统点对点传输方式，比特信不需要信任沟通协议，一份邮件会发送给网络系统中的所有人，只有真正拥有密钥的人才能打开信件，这也避免了被追踪收件方和发件方的风险。由于这种方式对网络带宽和运算能力要求很高，只有在如今具备软硬件基础的情况下，才能承担这种由快到安全的转变。

前已经有很多试图以区块链技术为基础的通信应用开始发展，在基于强大安全和算例的基础上建立全新模型，未来会有越来越多与过去截然不同的网络模型和架构出现。

图 17. 区块链可以使通信更加快捷安全



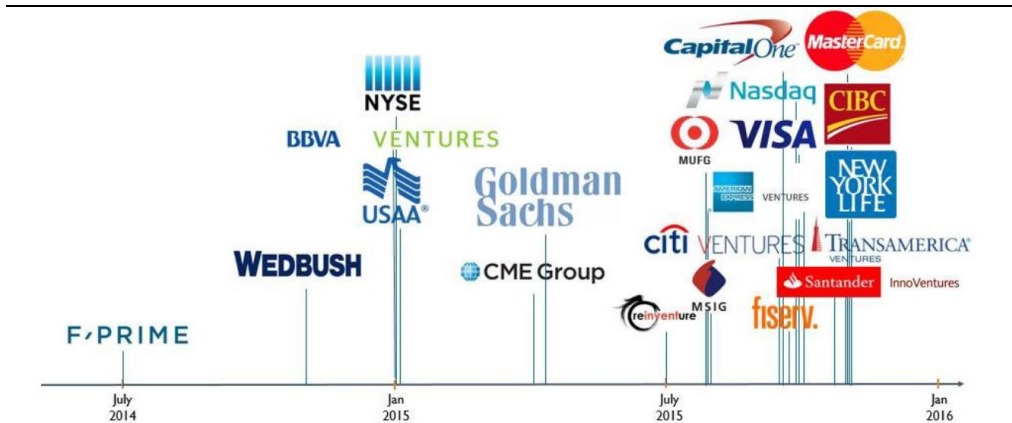
资料来源：互联网、兴业证券研究所

金融：金融领域存在大量诸如银行、证券交易所等中介机构，对区块链技术的巨大需求也形成了目前区块链接入最多的领域，金融系统的去中心化将大大提高系统的运行效率。目前的货币发行由央行控制，以政府为中心，进行集中式货币管理控制，这样的状态下无法实现货币真正的自由交换，比特币的产生也是对这一问题的尝试性解决，为人们提供一种去中心化的数字货币。比特币的成功对传统金融机构产生了巨大影响，各巨头纷纷涉入区块链领域，试图用区块链技术取代传统金融底层协议。金融领域与社会发展密切相关，金融对区块链技术的探索对

区块链发展起了明显推动作用，衍生出侧链、私有链等新概念，加速区块链技术成熟与应用。

由于区块链在金融领域应用前景广阔，全球各大金融机构都积极参与区块链项目的投资，在区块链技术上加强研究，其中包括纳斯达克、高盛、花旗、摩根士丹利、瑞银等。银行等金融机构的基础设施融合底层区块链技术结合，将对现有的支付、交易、结算的方式产生深远的影响，提升其运作的效率。归纳来看，银行的投资有三种途径，一是商业银行成立内部的区块链实验室。比如花旗银行、瑞银、纽约梅隆银行等已相继成立研发实验室，重点围绕支付、数字货币和结算模式等方面测试区块链的应用，有的还扩大到其员工内部系统中测试。二是投资金融科技初创公司。2015 年以来，许多跨国大型金融集团纷纷以创投形式进入区块链领域，比如高盛联手其他投资公司向比特币公司

图 18. 尝试应用区块链的金融机构



资料来源：CBinsights、兴业证券研究所

跨国价值转移。依靠现有技术，建立一个全球性的信用共识体系是很难的，由于每个国家的政治、经济和文化情况不同，对于两个国家的企业和政府完全互信是几乎做不到的，这也就意味着无论是以个人抑或企业政府的信用进行背书，对于跨国之间的价值交换即使可以完成，也有着巨大的时间和经济成本。而区块链技术的信用由数学背书，所有的规则都建立一个公开透明的数学算法（程序）之上可以获得全球大部分国家的共识，从而实现跨国价值转移。

医疗：目前医疗领域是除了金融领域外的区块链第二大应用领域，包括病例在内的很多资料极富隐私性，需要很高的权限保护。尽管目前对与个人信息的管理能基本符合要求，未来技术的发展将获得大量特定基因数据，当前的中心化资料系统也会变得很吃力，容易出现大规模数据泄漏的问题。即使是重视安全、采用闭源系统的苹果，也出现过数次数据库泄漏问题，造成较恶劣的影响。在过去数据泄漏的案例中，往往是由于网络操作的问题引起，让所有的数据暴露在黑客的面前。而区块链技术可以通过多签名私钥和加密技术来防止这种情况的出现。当数据被哈希后放置在区块链上后，使用多签名技术，就能够让那些获得授权的人们才可以对数据进行访问。使用这种技术，将能够制定一定的规则来对数据进行访问，必须获得授权才能够进行，无论是医生、护士或者病人本身都需要获得许可；在某些情况下，可以设定需要 3 个人中 2 个人授权才可以进行。

之前，飞利浦医疗和 TIERON 合作，希望让飞利浦医疗通过区块链技术来完成关于病历资料的认证，或者是病历方面的隐私保护。由于区块链是高冗余的系统，部分损失不会也不会造成任何问题，所有的数据都无法被篡改，或者无法随意的阅读，可以设立复杂可编程的权限保护，这种可编程、匿名性特征能更好的在去中心化的环境中保护病人的隐私，其应用前景非常广阔。

图 19. 飞利浦医疗和 TIERION 合作通过区块链完成病历资料认证



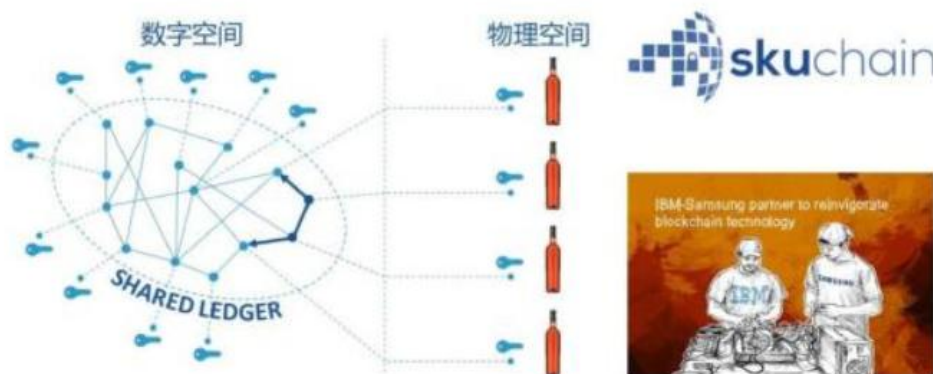
资料来源：互联网、兴业证券研究所

供应链和物联网：由于传统物联网模式是由一个中心化的数据中心收集所有已联接设备的信息，但这样一来，在生命周期成本、收入方面有严重缺陷，如果设备的运行环境可以去中心化，彼此相连，形成分布式云网络，整个网络的生命周期就可以变得非常长，同时运行成本可以显著降低。

在传统的中心化系统中，信任机制比较容易建立，毕竟存在一个中央机构来管理所有设备和各个节点的身份，但对于潜在数量在百亿级的联网设备而言，这种做法难度极大。而区块链技术解决了闻名已久的拜占庭将军问题——它提供一种无需信任单个节点，还能创建共识网络的方法。比特币使用算法工程保证整个网络的安全，借助它，设备能在金融市场中完全独立于任何人工干预。一套算法会生成自己的比特币钱包，从而允许它与别的算法（别的钱包）进行交易。物联网中，所有日常家居物件都能自发、自动地与其它物件、或外界世界进行金融活动。

市场上比较知名的是 IBM 和三星提出的以太坊物联网解决方案，并融资约 1800 万美元。IBM 工程师认为，区块链是解决物流系统中信息传输不确定性问题的理想方案，对供应链中的物流信息提供认证服务，并通过区块链数据库追踪问题所在，解决各类高端消费品的仿制问题。高容错性的物联网区块链技术，具有广阔的发展前景。

图 20. Skuchain，一种新的供应链模式



资料来源：互联网、兴业证券研究所

公证：公证作为当前社会的重要需求，具有较高的成本并严重依赖政府机关和权威单位的信用，也造成了国内知识产权保护不够的问题。利用区块链去中心化的特点，使用数学信用背书完成全自动化公证。如果从重要信息到生活痕迹都能够

证明所有权，且数据永久保存并随时可追溯源头，微信息和微知识产权将形成体量惊人的交易市场。当前也有不少公司在公证领域做出尝试。Bitproof 专注于学校学历证书认证，MONEGRAPH 试图把艺术品进行区块链登记，Factom 提供对所有文书、文件的数据资料公证服务。区块链技术可自动、便捷的完成无可辩驳的全球公证，有望让公证领域进入一个全新的阶段。

当前，区块链技术蓬勃发展，投资公司对区块链技术抱有极高的期待。微软公司的 Azure 区块链服务项目 (MSFT)，与多家区块链初创公司合作，为用户、合伙人和开发者提供技术和服务支持，推进区块链技术的应用场景落地，其成员包括 ConsenSys、Ripple、CoinPrism 和 Factom 等；区块链支付初创公司 Align Commerce 获得了由硅谷投资公司 KPCB 领投的 1250 万美元 A 轮融资，区块链技术初创公司 Chain 也筹集了 3000 万美元的风险投资。技术的发展和前景的广阔带来了创业的黄金期。区块链技术在公证、医疗、通信等领域寻求更深层次的应用。据报道，2015 年初至今，投资到区块链相关初创公司的总金额，已经突破了 10 亿美元。

表 3. 区块链代表性投资事件

投资者	投资公司	事件
Andreessen Horowitz	Coinbase (数字货币交易及钱包服务提供商)	Coinbase 于 2015 年 1 月获得 C 轮 7500 万美元融资。在此之前，Coinbase 完成了对区块链信息浏览服务商 Blockr.io 的收购。
--	Gem (医疗健康)	目前已经获得了 700 万美元的投资，和健康行业内多个不同利益相关方进行合作来评估是否需要区块链技术
Khosla Venture	Chain (为使用区块链的金融机构提供基础设施)	Chain 于今年 9 月成功融得 3000 万美元资金，纳斯达克与 Chain 合作，就比特币用于私企股票交易开展试运营
Boost VC	Mirror (区块链智能合约初创公司)	Mirror 已经完成了 A 轮 880 万美元的融资，目标是提高国际市场的流动性以及金融系统的民主化
雨云创投公司	Blockcypher 和 ShoCar	Blockcypher 是区块链网络服务公司，ShoCard 提供区块链身份解决方案
光速创投	blockchain、BlockScore 和 Melotic	Blockchain 是比特币钱包提供商，BlockScore 是身份验证服务公司，Melotic 是数字资产交易所以
RRE Ventures	Mirror 和 Chain	Mirror 是区块链智能合约初创公司，chain 是区块链技术公司
数贝投资	专业投资区块链领域的应用公司	数贝投资目前已投区块链领域 1.8 亿元。其中，1 亿为天使基金，用于孵化具有应用前景的区块链项目，以及提高区块链安全性的矿机芯片行业。5 亿为产业基金，投向有明晰商业模式的中后期区块链应用项目。

资料来源：互联网、兴业证券研究所

随着区块链技术的蓬勃发展，更多的领域开始引入区块链技术，并展示了对该技术的强烈需求。艺术品领域需要可靠认证作品真实性，审计领域需要区块链的数据库功能来保证审计数据的真实性与可追踪性，智能资产领域需要区块链的数据自动处理功能来帮助资产实现智能化、自动化。从比特币到社会领域的全方面，区块链技术正逐步以去信任环境下的大规模协作工具的形式扩展到全社会，互联网的价值转移也变得有可能。

4、数字货币的定义与现状

4.1、数字货币定义：与电子货币、虚拟货币均不同

接下来我们再介绍另一个有关联性的另一个概念：数字货币。

随着信息技术的发展和在金融领域的应用，多种非货币形式的货币出现。主要的非法定货币主要有三种：电子货币、虚拟货币和数字货币。

电子货币是纸币在银行或其它相关金融机构将法定货币电子化和网络化存储和支付的形式。当在账户之间划拨资金时，实质上只是资金信息的传递。人们对电子货币的信任来自对政府法定货币和银行金融体系正常运转的信心。电子货币本质上是法定货币的一种电子化，常以磁卡或账号的形式存储在金融信息系统内，以方便储藏和支付为主要目的，货币的价值与法定货币等值。按照发行主体的不同又可分为银行卡（借记卡、贷记卡等）、储值卡（公交卡、饭卡、购物卡等）和第三方支付方式（Palpal、支付宝、财付通等）。

广义的“虚拟货币”，没有实物形态的货币，包括以上提到的电子货币和下文介绍的数字货币等。但狭义的虚拟货币却是基于网络的虚拟性，由网络运营商提供发行并应用在网络虚拟空间的类法币，即它是真实世界货币体系的一种映射模拟，又被称为网络货币。例如腾讯公司发行的Q币，各大网游公司发行的游戏币，论坛为奖励网民参与贡献而设计的积分等等，通常被称为狭义的虚拟货币。拟货币最大的特点是发行主体为互联网企业，使用范围也常常限定在该企业经营领域之内，目的是方便网民衡量、交换、享用互联网服务。政府出于稳定金融体系的要求规定虚拟货币不可双向流通；同时，拥有虚拟货币发行权的企业也没有激励提供虚拟货币等价兑回现金的服务。这种单向流通的特性决定了虚拟货币无法充当真实世界里的现金或电子货币，它只能是互联网企业用来服务于自身用户的一种商务模式。人们对虚拟货币的信任完全来自对互联网发行企业的信心。

数字货币可以认为是一种基于节点网络和数字加密算法的虚拟货币。数字货币与电子货币最大的不同在于数字货币不会有物理钞票的存在，它本身就是财富的表现形式。数字货币的核心特征主要体现在三个方面：①由于来自于某些开放的算法，数字货币没有发行主体，因此没有任何人或机构能够控制它的发行；②由于算法解的数量确定，所以数字货币的总量固定，这从根本上消除了虚拟货币滥发导致通货膨胀的可能；③由于交易过程需要网络中的各个节点的认可，因此数字货币的交易过程足够安全。

表 4. 电子货币、虚拟货币和数字货币的对比

特性	电子货币	虚拟货币	数字货币
发行主体	金融机构	网络运营商	无
使用范围	一般不限	网络企业内部	不限
发行数量	法币决定	发行主体决定	数量一定
储存形式	磁卡或账号	账号	数字
流通方式	双向流通	单向流动	双向流通
货币价值	与法币对等	与法币不对等	与法币不对等
信用保障	政府信用	企业信用	网民信念
交易安全性	较高	较低	较高
交易成本	较高	较低	较低
运行环境	内联网、外联网、读写设备	企业服务器与互联网	开源软件以及 P2P 网络
典型代表	银行卡、公交卡、支付宝等	Q 币、盛大币、各论坛积分等	GDCs 共享币、比特币、莱特币等

资料来源：互联网、兴业证券研究所

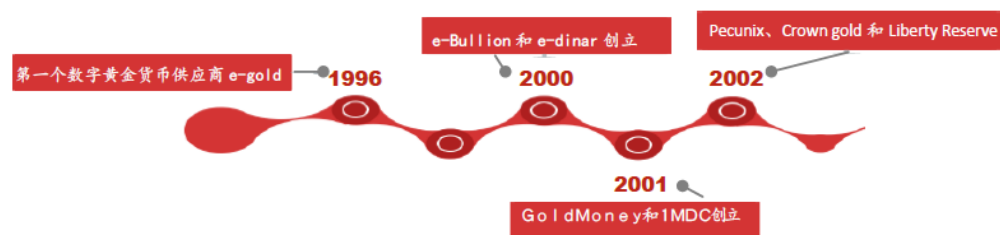
4.2、目前已经出现的数字货币形式

数字货币(Digital currency)分两类指非 **Cryptocurrency 货币**（即数字黄金货币，如 e-gold，以及公司发行的货币，如 xrp）和 **Cryptocurrency 货币**（即比特币 Bitcoin 类加密货币）。

- **数字黄金金币** (Digital Gold Currencies，简称 DGCs)是一种以黄金重量命

名的电子货币形式。这种货币的典型计量单位是金衡制克或者金衡制盎司，尽管有时候也使用黄金迪纳尔做单位。数字黄金货币通过未配额或者分散配额的黄金存储来资助。到 2006 年 1 月，数字黄金货币供应商持有超过 8.6 公吨的黄金作为储备，价值大约 1.54 亿美元。数字黄金货币由很多供应商发行。每个竞争供应商都发行独立的数字黄金货币，基本都以他们的公司名字命名。e-gold 和 Liberty Reserve 是应用最流行的数字黄金货币供应商，拥有最大数量的用户。在黄金储备总量方面，GoldMoney 是领导供应商。

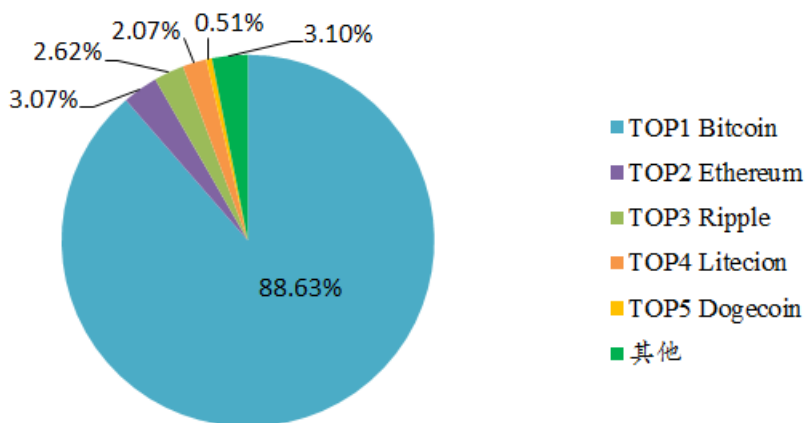
图 21. 数字黄金货币发展史



资料来源：兴业证券研究所

- **加密货币** 指不依托任何实物，使用密码算法的数字货币。是一种依靠密码技术和校验技术来创建，分发和维持的数字货币。密码货币的特点在其运用了点对点技术且每个人可以发行。截至 2016 年 1 月 26 日，全世界共有 666 种加密货币，总市值达 6,750,110,160 美元。

图 22. 排名前五的加密货币市值占比情况



资料来源：coinmarketcap，兴业证券研究所

绝大多数加密货币的体量都很小，目前的加密货币市场仍以比特币(Bitcoin)为主，但以太币(Ethereum)、瑞波币(Ripple)和莱特币(Litecion)也占据了一定的市场份额。其中,只有 46 家加密货币的市值超过 100 万美元，仅最大的 8 种加密货币市值超过 1000 万美元。前三大加密货币的市值占总市值的 94.32%。

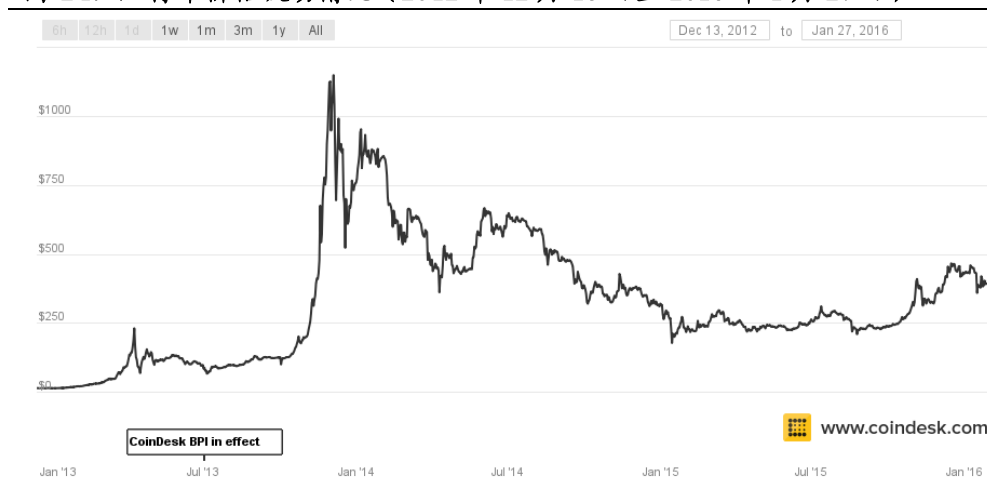
图 23. 排名前十的加密货币

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	\$ 5,973,580,035	\$ 394.75	15,132,450 BTC	\$ 54,780,900	-0.12 %	
2	Ripple	\$ 202,945,780	\$ 0.005983	33,920,177,761 XRP *	\$ 1,863,280	14.96 %	
3	Ethereum	\$ 186,946,510	\$ 2.44	76,572,545 ETH	\$ 12,270,600	-12.08 %	
4	Litecoin	\$ 142,749,588	\$ 3.23	44,234,223 LTC	\$ 4,171,360	2.35 %	
5	Dogecoin	\$ 46,918,918	\$ 0.000456	102,831,025,445 DOGE	\$ 6,348,870	37.81 %	
6	Dash	\$ 26,995,366	\$ 4.37	6,173,304 DASH	\$ 392,015	7.49 %	
7	Factom	\$ 11,715,814	\$ 1.34	8,753,728 FCT *	\$ 1,924,520	23.26 %	
8	Peercoin	\$ 10,817,328	\$ 0.471525	22,941,154 PPC	\$ 284,767	12.74 %	
9	MaidSafeCoin	\$ 10,469,257	\$ 0.023134	452,552,412 MAID *	\$ 209,683	23.23 %	
10	VPNCoin	\$ 10,066,623	\$ 0.025145	400,339,746 VPN *	\$ 2,993,360	14.26 %	

资料来源: coinmarketcap, 兴业证券研究所

加密货币的价格往往波动剧烈。以最主要的加密货币——比特币为例：2010 年 4 月比特币的单价还不到 14 美分，而 2013 年 11 月 24 日达到了 1242 美元的历史高位，2015 年 1 月，其单价下跌至 200 美元左右，但 3 月初又反弹至接近 300 美元。其他加密货币也波动剧烈，往往一天之内波幅就超过了 10%，极端情况下更是超过 100%。

图 24. 比特币价格波动情况（2012 年 12 月 13 日至 2016 年 1 月 27 日）



资料来源: coinmarketcap, 兴业证券研究所

加密货币尚未普及。当消费者对加密货币更了解，并且加密货币的可获得性和安全性大大提高、能够可靠兑换为现金时，人们才会广泛接受并使用加密货币。阻碍加密货币广泛使用的最大制约因素为人们对加密货币的认知度。经调查，调查者中只有约 6% 的人对加密货币非常了解；而 83% 的人都对加密货币稍有了解或者完全不了解。

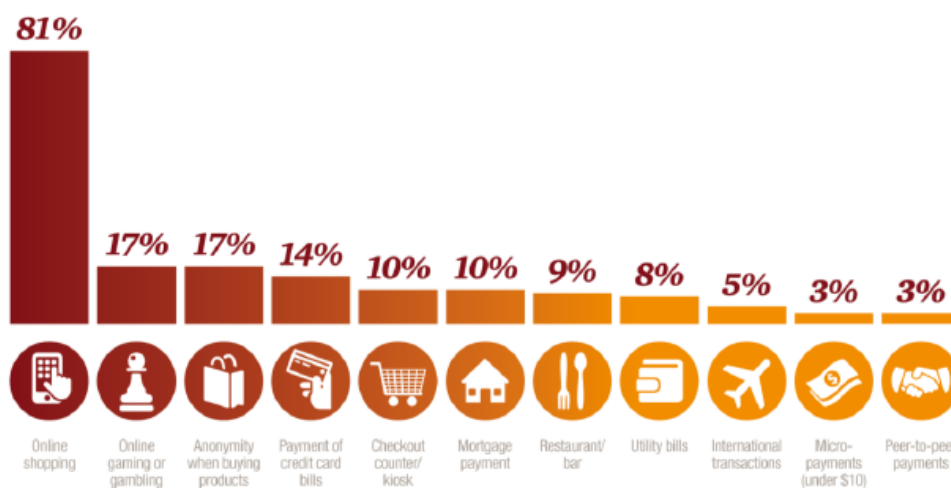
图 25. 人们对加密货币的熟悉程度



资料来源：普华永道咨询，兴业证券研究所

加密货币的用途。在过去的一年里，将加密货币用于网上购物人数占加密货币使用者总数的 81%，而用于网游和匿名购买的人数均占 17%，用于信用卡还款的人数占 14%。除此之外，人们还将加密货币用于柜台结账、住房抵押、餐饮消费、水电费支付、跨国交易、小额支付以及对等支付。

图 26. 加密货币的使用情况



资料来源：普华永道咨询，兴业证券研究所

4.3、数字货币与传统货币相比的优势与劣势

数字货币在互联网的“问世”创造出其他电子货币或虚拟货币无法企及的“神话”，源于其拥有以下六个“不俗”的优点：

其一，去中心化：整个网络由用户构成，没有中央银行。

其二，世界流通：任何人都可以挖掘，购买、出售或收取，并可以在任何一台接入互联网的电脑上管理。

其三，交易费用低：几乎是实时交易且无手续费。

其四，无隐藏成本：知道对方比特币地址就可进行支付，没有额度与手续限制。

其五，专属所有权：操控私钥可以被隔离保存在任何存储介质，除了主人之外无人可以获取。

其六，跨平台挖掘：软件挖掘过程中可以在众多平台上发掘不同硬件的计算能力。

数字货币在近几年兴起，作为“新生儿”，发展不成熟，仍然具有诸多缺陷：

其一，种类过多，存在消费上不便利：比如，进行小额现金交易时，从与 Cyber Cash 合作的商场买东西就得用 Cyber Cash，而到与 Digicash 合作的商场买东西又得先换 Digicash 的钱。消费者的钱包里放着不能通用的各种货币，如果钱包里某商场承认的钱不够了，只好放弃从该商场买东西的念头，因此很不方便。从 Internet 电子商务愈演愈烈的情况来看，统一数字货币是大势所趋。但如果数字货币能在

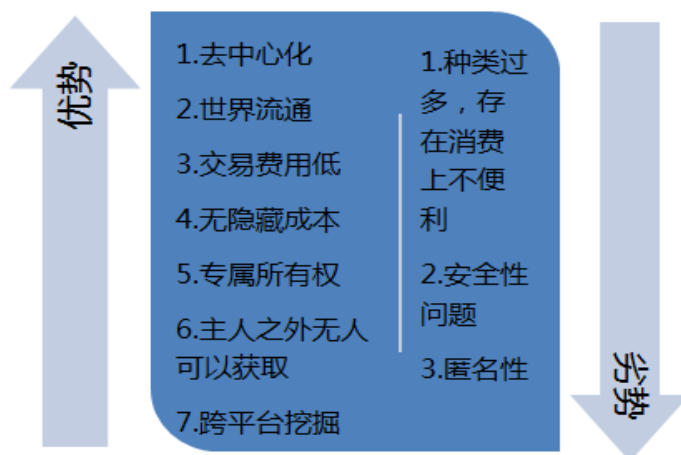
未来实现统一，则该问题也将随之迎刃而解。

其二，安全性问题：迄今为止，安全性一直是制约数字货币发展的最重要的瓶颈因素之一。数字货币的使用者一般将其储存在移动设备、计算机或在线钱包中。如果其设备丢失或损坏，用户就会丢失其拥有的数字货币。英国《卫报》就曾报道，一名男子因误扔其存有比特币的硬盘而损失了 7500 个比特币。此外，存放在在线钱包中也有可能被黑客攻击而窃取，交易平台也有卷款跑路的风险。日本最大的比特币交易平台 Mt.GoX 于 2014 年 3 月宣称受到黑客攻击，损失了超过 75 万枚比特币，当时市值约 3.65 亿美元，但据日本《读卖新闻》2015 年 1 月 2 日报道，这很有可能是其 CEO 监守自盗。

其三，匿名性：数字货币因其匿名性和不受地域限制的特点还可能被用于恐怖融资和洗钱活动。比特币为代表的“去中心化”数字货币实际上不是完全匿名的，它的每一笔交易的参与方的信息都被记录在总账上，但交易参与方所提供的信息类似于“笔名”，无法将其与在现实中的真实身份一一对应，这就使得数字货币有可能被用于洗钱和恐怖融资。目前，已有观点认为 ISIS 可能利用数字货币进行融资。

其四，危及金融稳定：其理论上可能会对传统货币体系造成冲击，不仅影响中央银行的宏观调控能力，还影响到政府的财政收入。仍以比特币为例，如果数字货币被广泛使用，因为其货币供给的总规模不变且货币供应速度不断降低，将不可避免地引起通缩。

图 27. 数字货币与传统货币相比的优势与劣势



资料来源：普华永道咨询，兴业证券研究所

5、央行数字货币：可能的实现形式

1 月 20 日，央行数字货币研讨会在北京召开。会议要求，央行数字货币研究团队要积极吸收国内外数字货币研究的重要成果和实践经验，在前期工作基础上继续推进，明确发行数字货币的战略目标，做好关键技术攻关，争取早日推出央行发行的数字货币。来自人民银行、花旗银行和德勤公司等国内外科研机构，及重要金融机构和咨询机构的金融机构专家参加了会议。针对未来如何建立数字货币的发行、流通和结算体系，国家如何发行加密电子货币等专题进行了研讨。在移动支付领域、与银行体系关联较为紧密的产业链上下游领域及数字货币与其他支付工具的无缝衔接领域，央行将积极结合全球趋势进行创新升级。

5.1、央行数字货币与比特币不同

此次央行提出“数字货币”，使人很容易联想到最广为人知的数字货币比特币，尽管比特币具有自由流通，保护隐私等优点，但事实上，**央行数字货币与比特币之间，必然存在极大区别。**

早在 2013 年底，包括央行在内的五部委就发布通知明确了比特币的性质，认为比特币不是由货币当局发行，不具有法偿性与强制性等货币属性，并不是真正意义上的货币。从性质上看，比特币是一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。比特币缺乏政府信用作担保，因此它并不是货币。一旦出问题政府不承担责任，风险非常大。在这一次定调后，比特币价格在 1 天内暴跌 2000 元。

现在，中国宣布将推出自己的数字货币来取代比特币。中国最终发行的数字货币跟比特币将大不一样：

首先，它将是为中国政府特制的，以便跟踪交易，而且将处于中国央行的保护之下，能方便政府机构监管，加强货币流通透明性，而不是像比特币一样没有发行方，任何人都可以开采购买，虽然拥有加密和匿名的优点，但也因此用于黑市交易而受人诟病。比特币需要通过挖矿解码生成，矿工大多有 IT 知识储备，而央行数字货币面向大众，在获取上必然无法使用“挖矿”系统。比特币币值由于挖矿难度提升和政策变化等原因，在近年来波动剧烈，而央行在推出数字货币时为了维持其价格的稳定，不可能根据获取的难易程度定价。

此外，央行数字货币应当能满足最大范围的支付需求，尤其是随着移动互联网、云计算、区块链等技术的演进，全球支付方式发生巨大变化的背景下，央行的数字货币需要满足全球支付需求。而不是如同比特币，只能在小范围内使用。央行的数字货币和比特币的区别主要如下：

表 5. 央行数字货币和比特币的区别

	央行数字货币	比特币
发行方	由央行统一印制、发行	没有发行方，基于一种算法随机生成，任何人都可以开采、购买、出售或收取比特币。
获取方式	面向普通群众，普通群众都可获得	IT 高手通过反复解谜密与其他淘金者相互竞争，为比特币网络提供所需的数字，获得相应的比特币。
定价	央行力保数字货币价格稳定，不可能根据获取的难易性定价	随着“挖掘”难度不断增加，比特币的价格也不断增加。
使用范围	需要满足全球的支付需求，在全球范围内使用	小范围，各个国家尚未承认比特币的货币属性。

资料来源：兴业证券研究所

5.2、区块链技术可能应用于央行数字货币

中国人民银行认为：数字货币将会增强其控制中国货币的能力。央行发行的数字货币可以降低传统纸币发行、流通的高昂成本，提升经济交易活动的便利性和透明度，减少洗钱、逃漏税等违法犯罪行为，提升央行对货币供给和货币流通的控制力。未来，数字货币发行、流通体系的建立还有助于我国建设全新的金融基础设施，进一步完善我国支付体系。

央行希望通过数字货币提升交易透明度，而区块链技术，正可以满足这一需求。区块链技术具有去中心化性，整个系统没有中心化的管理机构和硬件，同时，还

具有去信任化性，系统中任何节点间进行数据交换都不需要相互信任，因此，通过区块链技术，整个数字货币体系中所有规则都是透明的，所有数据内容都是公开的，没有人有能力去篡改和操纵。

■ 减少洗钱、逃漏税等违法犯罪行为。

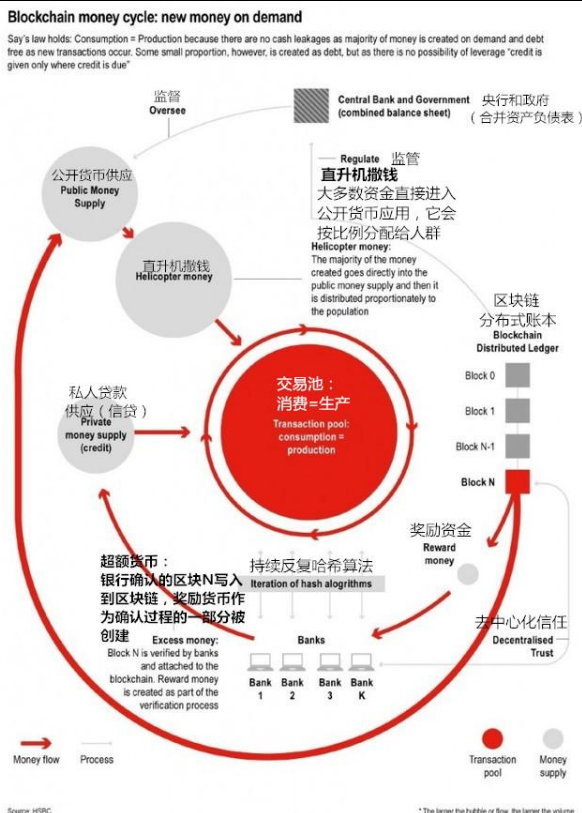
目前分散的金融机构都有很多内部账本，而未来随着区块链技术的应用，将建立全国统一账本，让每一笔钱都可以追溯，每一次交易行为都可以追溯，逃漏税、洗钱行为会在监管范围内，甚至有可能实现在刷卡机上自动扣税。

■ 解决信用问题，降低基础设施建设成本。

金融的本质是信用，从某种意义上讲，金融机构存在的意义，就是解决信用问题。比如第三方支付，如果交易双方相互信任，何必需要这个中介？而区块链技术一个革命性的突破就是去信任。也即网络中的两个任意节点(可以理解为任意两个人)，不需要相互信任，就能够精确且公平地完成价值转移，比如转账。任意一方都没有能力去篡改数据或者操控交易。所以，区块链技术一旦成熟起来，将会重构金融行业的底层逻辑，解决信用问题，降低信用维持的成本。目前刷卡消费正在成为习惯，未来数字货币推广后，从社会信用积累的角度，企业和消费者都会倾向于使用数字货币、刷卡消费，因为电子交易有数据痕迹，可以据此积累企业和个人的信用，这会成为获得银行等金融服务的依据。

而在提升货币供给控制力方面，区块链技术也有与之相对的应用。据汇丰银行发布的一份报告表示，央行可以将区块链技术用于一种政策，这甚至比量化宽松更标新立异。它可以让央行到家庭的“直升机撒钱”政策，变得更为容易。“直升机撒钱”将是外部货币(outside money)：直接从中央银行注入资金，而不是代表私营部门其他地方的债务。

图 28. 区块链实现“直升机撒钱”



资料来源: HSBC, 兴业证券研究所

总体而言，区块链的技术特点与央行推行数字货币的目的相符合。未来，区块链技术很有可能会被应用于央行数字货币中。

6、风险提示

区块链技术升级速度不及预期，商业模式尚未成型，金融等政策监管风险。

投资评级说明

行业评级 报告发布日后的 12 个月内行业股票指数的涨跌幅度相对同期上证综指/深圳成指的涨跌幅为基准,投资建议的评级标准为:

- 推 荐: 相对表现优于市场;
中 性: 相对表现与市场持平
回 避: 相对表现弱于市场

公司评级 报告发布日后的 12 个月内公司的涨跌幅度相对同期上证综指/深圳成指的涨跌幅为基准,投资建议的评级标准为:

- 买 入: 相对大盘涨幅大于 15% ;
增 持: 相对大盘涨幅在 5% ~ 15% 之间
中 性: 相对大盘涨幅在 -5% ~ 5% ;
减 持: 相对大盘涨幅小于 -5%

机构销售经理联系方式

机构销售负责人			邓亚萍	021-38565916	dengyp@xyzq.com.cn
上海地区销售经理					
姓名	办公电话	邮箱	姓名	办公电话	邮箱
罗龙飞	021-38565795	luolf@xyzq.com.cn	盛英君	021-38565938	shengyj@xyzq.com.cn
杨忱	021-38565915	yangchen@xyzq.com.cn	王政	021-38565966	wangz@xyzq.com.cn
冯诚	021-38565411	fengcheng@xyzq.com.cn	王溪	021-20370618	wangxi@xyzq.com.cn
顾超	021-20370627	guchao@xyzq.com.cn	李远帆	021-20370716	liyuanfan@xyzq.com.cn
胡岩	021-38565982	huyan@xyzq.com.cn	王立维	021-38565451	wanglw@xyzq.com.cn
地址: 上海市浦东新区民生路 1199 弄证大五道口广场 1 号楼 20 层 (200135) 传真: 021-38565955					
北京地区销售经理					
姓名	办公电话	邮箱	姓名	办公电话	邮箱
朱圣诞	010-66290197	zhusd@xyzq.com.cn	郑小平	010-66290223	zhengxiaoping@xyzq.com.cn
肖霞	010-66290195	xiaoxia@xyzq.com.cn	陈杨	010-66290197	chenyang@xyzq.com.cn
刘晓浏	010-66290220	liuxiaoliu@xyzq.com.cn	吴磊	010-66290190	wulei@xyzq.com.cn
何嘉	010-66290195	hejia@xyzq.com.cn			
地址: 北京市西城区武定侯街 2 号泰康国际大厦 6 层 609 (100033) 传真: 010-66290200					
深圳地区销售经理					
姓名	办公电话	邮箱	姓名	办公电话	邮箱
朱元贱	0755-82796036	zhuyy@xyzq.com.cn	李昇	0755-82790526	lisheng@xyzq.com.cn
杨剑	0755-82797217	yangjian@xyzq.com.cn	邵景丽	0755-23836027	shaojingli@xyzq.com.cn
王维宇	0755-23826029	wangweiyu@xyzq.com.cn			
地址: 福田区中心四路一号嘉里建设广场第一座 701 (518035) 传真: 0755-23826017					
海外销售经理					
姓名	办公电话	邮箱	姓名	办公电话	邮箱
刘易容	021-38565452	liuyirong@xyzq.com.cn	徐皓	021-38565450	xuhao@xyzq.com.cn
张珍岚	021-20370633	zhangzhenlan@xyzq.com.cn	陈志云	021-38565439	chanchiwan@xyzq.com.cn
曾雅琪	021-38565451	zengyqi@xyzq.com.cn	申胜雄		shensx@xyzq.com.cn
赵新莉	021-38565922	zhaoxinli@xyzq.com.cn			
地址: 上海市浦东新区民生路 1199 弄证大五道口广场 1 号楼 20 层 (200135) 传真: 021-38565955					
私募及企业客户负责人			刘俊文	021-38565559	liujw@xyzq.com.cn
私募销售经理					
姓名	办公电话	邮箱	姓名	办公电话	邮箱
徐瑞	021-38565811	xur@xyzq.com.cn	杨雪婷	021-20370777	yangxueting@xyzq.com.cn
唐恰	021-38565470	tangqia@xyzq.com.cn	韩立峰	021-38565840	hanlf@xyzq.com.cn
地址: 上海市浦东新区民生路 1199 弄证大五道口广场 1 号楼 20 层 (200135) 传真: 021-38565955					

港股机构销售服务团队

机构销售负责人			丁先树	18688759155	dingxs@xyzq.com.hk
姓 名	办公电话	邮 箱	姓 名	办公电话	邮 箱
郑梁燕	18565641066	zhengly@xyzq.com.hk	阳烜	18682559054	yanghan@xyzq.com.hk
王子良	18616630806	wangzl@xyzq.com.hk	周 围	13926557415	zhouwei@xyzq.com.hk
孙博轶	13902946007	sunby@xyzq.com.hk			
地址: 香港中环德辅道中 199 号无限极广场 32 楼 3201 室 传真: (852)3509-5900					

【信息披露】

本公司在知晓的范围内履行信息披露义务。客户可登录 www.xyzq.com.cn 内幕交易防控栏内查询静默期安排和关联公司持股情况。

【分析师声明】

本人具有中国证券业协会授予的证券投资咨询执业资格并注册为证券分析师，以勤勉的职业态度，独立、客观地出具本报告。本报告清晰准确地反映了本人的研究观点。本人不曾因，不因，也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

【法律声明】

兴业证券股份有限公司经中国证券监督管理委员会批准，已具备证券投资咨询业务资格。

本报告仅供兴业证券股份有限公司（以下简称“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。客户应当认识到有关本报告的短信提示、电话推荐等只是研究观点的简要沟通，需以本公司 <http://www.xyzq.com.cn> 网站刊载的完整报告为准，本公司接受客户的后续问询。

本报告并非针对或意图发送予或为任何就发送、发布、可得到或使用此报告而使兴业证券股份有限公司及其关联子公司等违反当地的法律或法规或可致使兴业证券股份有限公司受制于相关法律或法规的任何地区、国家或其他管辖区域的公民或居民，包括但不限于美国及美国公民（1934 年美国《证券交易所》第 15a-6 条例定义为本「主要美国机构投资者」除外）。

本公司的销售人员、交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。本公司没有将此意见及建议向报告所有接收者进行更新的义务。

本公司的资产管理部门、自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

本公司系列报告的信息均来源于公开资料，我们对这些信息的准确性和完整性不作任何保证，也不保证所包含的信息和建议不会发生任何变更。我们已力求报告内容的客观、公正，但文中的观点、结论和建议仅供参考，报告中的信息或意见并不构成所述证券的买卖出价或征价，投资者据此做出的任何投资决策与本公司和作者无关。

在法律许可的情况下，兴业证券股份有限公司可能会持有本报告中提及公司所发行的证券头寸并进行交易，也可能为这些公司提供或争取提供投资银行业务服务。因此，投资者应当考虑到兴业证券股份有限公司及/或其相关人员可能存在影响本报告观点客观性的潜在利益冲突。投资者请勿将本报告视为投资或其他决定的唯一信赖依据。

若本报告的接收人非本公司的客户，应在基于本报告作出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。

本报告的版权归本公司所有。本公司对本报告保留一切权利。除非另有书面显示，否则本报告中的所有材料的版权均属本公司。未经本公司事先书面授权，本报告的任何部分均不得以任何方式制作任何形式的拷贝、复印件或复制品，或再次分发给任何其他人，或以任何侵犯本公司版权的其他方式使用。未经授权的转载，本公司不承担任何转载责任。