

前言 要么拥抱颠覆，要么被颠覆

说起区块链，就不得不从比特币说起。2008年，一个化名中本聪的神秘组织发表了比特币的白皮书——《比特币：一种点对点的电子现金系统》。2014年开始，比特币的行情波动让“区块链”这个概念逐渐进入了一部分人的视野。

区块链究竟是什么？一言以蔽之，区块链是一种能够大幅降低商业社会信用成本的技术。区块链作为一个分布式的账簿，其数据一旦记录下来，就是永久保存且不可更改的。过去，当你和一个陌生人进行一个商业行为的时候，你无法百分之百地相信他，他也无法百分之百地相信你，为了解决这个问题，我们不得不需要第三方来做信用背书以证明这个交易的公平性和真实性。但是第三方信用背书就是完全没有问题的吗？有没有可能通过技术的手段，不需要信任第三方，彼此就能达成信任，从而可以直接促成交易？区块链就是为了解决这个问题而生的，通过代码和数字，不可篡改，达成了信任的基础。通俗地说，我想和你做生意，我知道 $1+1=2$ ，你也同意 $1+1=2$ ，那我们就有了信任的基础。我们的交易会在全网广播，所有人都来作证，这样不需要第三方，我们就可以完成交易了。这是一个非常了不起的发明！商业社会发展的基石便是信用！而区块链居然大幅地降低了信用的成本。

目前，我在硅谷所认识的大多数人都把注意力集中在了人工智能上，他们认为这是最有前景的技术革命。我也被他们的热情深深感染了！人工智能将颠覆行业，并赋予我们从前只敢在超级科幻小说中想象的能力。诚然，人工智能拥有改变世界的的能力，而区块链也可以。一个社会的发展，一方面是生产力的发展，另一方面是生产关系的发展，生产力和生产关系相互作用。在我的认知判断里，以人工智能为代表的新技术，代表着先进的生产力，一定有非常好的前途，可以提升很多工作的效率，而区块链则代表着先进的生产关系，把信用的成本降低到忽略不计，大幅提升了交易的效率。人工智能和区块链的结合，一定是未来最有前途的产业。

有人说，现在区块链数字货币资产涨得这么快，肯定有很多泡沫！“当主流媒体还在忙于猜测加密货币价格及其黑市阴谋时，其遗漏了这一切的本质事实。那就是，密码学家们悄然发明了一套全新的技术原型。” Haseeb Qureshi在其文章《区块链：一场始料未及的革命（Blockchain: The Revolution We're Not Ready for）》中指出，“区块链将颠覆整个社会，它使得仅存在于乌托邦和哲学家白日梦中的治理体系得以实现。”文中，他不仅饶有趣味地将区块链技术于20世纪震惊物理学界的弦理论进行了类比，还举出1995~2001年互联网泡沫危机以警醒盲目跟风的投机者。

正如我所提及的，如果你也相信区块链是未来的趋势，那么这个行业还是非常早期的阶段，泡沫也许真的存在，大潮退去才知道谁在裸泳。我坚信，当尘埃清理干净以后，那些兢兢业业的真正想要改变世界的区块链创业者，一定会有所建树。

十年以后，可以预见，区块链+和今日互联网+一样寻常，所有不透明、低效的行业，都会被区块链颠覆；大部分的生活问题都可以被区块链解决，而加密数字货币作为区块链分布式的记账单位与区块链紧密结合，成为一种新型的资产，资产代币化成为一种新的趋势。

朋友们，现在有一个链接未来的机会摆在大家的面前，以往无数次的技术革新告诉我们，要么选择去拥抱颠覆，要么只能被颠覆。

魏久胜

于澳大利亚墨尔本

引言 一个真正信任时代的到来

人类社会的进步与信息的发展息息相关，在大众传播时代，信息传播是中心化的，信息掌握在少数人手中。而在“点对点”的信息传播中，人类一直无法解决“共识”的问题，互联网实现了信息互联，却无法解决互信的问题——直到区块链出现，这些问题才有了完美的解决方案。

人类的一切活动都离不开“信用”两个字。数学家邓巴认为，人与人之间点对点的信任，其极限也就是150人。因此，当前人类活动中凡是涉及“信用”的问题，都由一个中心（第三方机构）来做信用背书。但是区块链可以通过算法建立智能信任，它公开透明、成本低、速度快、分布广泛，没有权威可以篡改、伪造记录，意味着一个真正信任时代的到来。

技术的发展都是为了创造更美好的生活，人类历史上一切技术革新，无不带来效率的巨大提升，例如从手工制作到蒸汽机的出现，从马车到汽车再到高铁。区块链也是这样一种技术，它的去中心化，必将影响各行各业，极大地提升效率和降低成本，便捷人们的生活。

信用机制的发展与区块链的诞生

一个人能记住多少张脸？数学家邓巴在研究中发现，人与人之间点对点的信任，150人已经是极限，这得到科学界广泛的认同，这个数也被称为“邓巴数”。因此，过去的信任机制一直都是“中心化”的，需要一个中间机构来做信用背书。这不仅影响了效率，增加了成本，还存在中心“大到不能倒”、中心故障会导致系统整体瘫痪等缺陷。区块链的出现，可以在任意两个人之间建立点对点的信任，不需要中心机构的参与，甚至不需要监督。

英国《经济学家》杂志2015年10月份的封面文章《信任的机器：比特币及其背后的区块链技术是如何改变世界的》^[1]中提到：区块链是一台制造信任的机器，可以说区块链的核心问题就是解决信用共识的问题。

[1] 文章英文名为The Trust Machine: How the Technology behind Bitcoin Could Change the World。文中还提到，区块链本质上是一个可共享的、可信的、每个人都可以检查的公开账本，但是没有任何单一用户能够控制它。

区块链技术创造智能信用

信用、信任对人类社会有多重要，答案是不言而喻的。很多时候，商业活动中的一切曲折和难题，都是信任的问题，而其中无数的低效行为和资源浪费，也都是为了解决信任的难题。

一个人能记住多少张脸

有一个人类学家，他研究部落的时候，发现每一个部落都控制在150人左右。因为人再多一些的话，就记不住了，记不住脸就感受不到亲近，连亲近都没有，信任就更无从谈起了，没有信任，部落之间的战斗和争端就永远不会停止。

人与人之间点对点的信任，其极限也就是150人——这个理论由数学家邓巴提出，也称邓巴数。

虽然这个世界上有一些人，他们的社交范围特别广，但总体来说，一旦一个群体的人数超过150人，成员之间的关系就开始淡化。邓巴写道：“150人似乎是我们能够建立社交关系的人数上限，在这种关系中，我们了解他们是谁，也了解他们与我们自己的关系。”

一个人能够信任的人是非常有限的。所以，在过去的经济活动中，第三方信任背书是必不可少的。

区块链创造智能信任

区块链可以通过算法建立智能信任——机器和机器间的信任，从而创造一种全新的信用共识机制，不需要第三方参与。

区块链全面颠覆了过去的那一套信任机制：用技术信任取代权威中心和情感信任，以此建立一种网络结构，所有人都可以参

与成为无数节点之一，进行认证、确权、交易、追溯和调整等一系列动作。它公开透明，成本低，速度快，分布广泛，没有权威可以篡改、伪造、取缔记录。简而言之，区块链体系下的信任机制，不再是人与人之间的信任，而是机器与机器之间的信任，这就是智能信任。更确切地讲，区块链是用代码构建的信任，在区块链的系统里，“代码即法律”^[1]。

[1] 《区块链：比特币底层技术如何改变货币、商业和世界》一书对“机器信任”做了如下描述：诚信被编码到流程的每一个环节中，它是分布式的，而不依赖于任何一个成员，参与者能够直接进行价值交换并可以期望另一方以诚信的方式行事。

区块链是技术创新的产物

从互联网到移动互联，我们可以清楚地看到技术创新是如何服务商业社会的。

信息的互联以及由此带来的技术创新，造就了网络化社交软件的诞生。当QQ问世时，多少人感到欣喜和不可思议：我们可以在同一时间跟五湖四海的陌生人交流，这在网络问世之前是不可想象的。

电商发展起来后，人们渴望能够看到其他消费者对商品的评价，技术的创新实现了人们的想象，并且颠覆了过去的商业模式：以前商家重广告，现在则重口碑。

当我们感受到互联网带来的种种便利时，人们开始想象：能否把这网络随身携带，不用坐在电脑前也能感受到网络带来的种种便利？安卓技术的出现使之变成了现实。移动互联网给人类生活带来了前所未有的便利，也带来了商业格局的再次颠覆。

.....

区块链也同样是技术创新的产物。

首先，互联网上信息爆炸，却难以辨别真伪，以至于人们有了对信息溯源的诉求。如何让信息能够不被篡改并且可以溯源？对于这一领域的技术探索从未停止过，区块链则让它成为现实。

其次，互联网上我们的信息很容易被一些平台收集、获取乃至贩卖，还有大量的网络黑客存在，可以说，人们对互联网安全的忧虑从未停止过。因此，对密钥技术的探索，可以说从互联网诞生之初就开始了，而区块链，实际上也是密钥技术发展的产物。

最后，最重要的，我们的一切商业活动都处在中心化的网络下。不仅需要消耗大量的中间成本，还会影响效率，最可怕的是一旦中心本身不可靠，带来的后果将非常严重！商业社会一直都有去中心化的构想，互联网的出现对商业的一个最基本的颠覆就是：中间环节越来越少，渠道越来越短，“消灭一切中介”的口号一直在喊，区块链通过技术的创新在“去中心化”的道路上又前进了一大步，它是意义深远且具有颠覆性的。

区块链让“消灭一切中介”真正成为可能

我们当前的大部分商业活动都是中心化的，细数一下，几乎各行各业都有中介的存在。尤其是在各种金融活动中，如股权变更。在类似房地产这样的大宗交易中，以及结婚、毕业登记等重要的事项中，一个中间人（中介、监督人、证明人等）是不可缺少的，这个中间人往往还承担着信用中介的职能，必须具备权威性。因此正如我们上文所讲，往往是大到不能倒，因为一旦中心本身不可靠，带来的后果是极其严重的。

互联网在出现之初就提出了消灭一切中介的口号，但实际上，互联网只是信息共享，起到了缩短中间环节的作用，并且把一部分中介搬到了互联网上，并没有真正“消灭中介”。传统的互联网技术也不可能真正做到消灭中介，因为互联网无法制造信用，信用共识永远都是最大的障碍。

以近几年很火爆的“互联网金融”为例，互联网金融之所以问题频发，就是因为大部分的互联网金融平台只能起到“信息中介”的作用，却在实际上承担了“信用中介”的职能，而绝大多数平台的信用值和实力根本不足以担当此重任，因此出现问题是必然的。为了解决这一问题，让互联网金融能够健康发展，行业和政府都想到了各种方法，但根本上，所有方法的出发点只有一个：找到一个更可靠的“中心”来作为“信用中介”。资金托管也好，政府部门监督也好，都是为了让无序的互联网金融行业能够“中心化”，其争议只是在于到底由谁来担当这个“中心”。

例如，我们在网上交易，两个陌生人之间如何达成互信？必须有一个强大的中心来承担“信用中介”的职能，否则交易无法达成。支付宝就是这样一个中介：我们买A的物品，钱不是打到A的账户上，而是打到支付宝账户上，当我们确认收货后，支付宝再把钱返给A。这样就保证了交易的安全。但是这当中也存在一些问题：首先，中心太重要了，大到不能倒，哪怕是主机出现一点故障都会导致交易无法正常进行；其次，钱需要隔很长一段时间才能打给A。

有没有更好的方法能够解决由“信任危机”所引发的一系列的麻烦？区块链技术为我们提供了另一种可能：由技术信任（智能信任）取代人工信任，可以在不需要任何中心的前提下实现互信。

区块链最终不仅会颠覆传统的金融系统，还会颠覆人们记录股票、合同、产权证、专利和结婚证的方式。换句话说，基本上就是所有需要一个值得信赖的中间人进行确认的事宜，因为区块链的参与，这个中间人将不再需要。

目前，关于区块链的融资项目越来越多。为什么风投这么看好区块链领域的投资？一个重要的原因就是它的去中心化。科斯拉创投的一位合伙人曾经这样说：“公司的投资是基于这样的信念——区块链会改变社会对交易的观念，无论是金融，还是其他交易。只要有经纪人的领域，只要是需要专家来证明某样东西有效性的地方，都有可能用区块链绕过去。”

PeerNova公司首席执行官纳维德·沙瓦尼说：“我们整个合同系统的基础是一个可信赖第三方。但是有了区块链，第三方就没必要存在了。”^[1]

以房地产交易为例：

传统上，一桩典型的居住地产买卖要涉及很多相关人士，交易非常复杂：土地登记处、买方和卖方、抵押贷款提供者（通常是银行）、抵押贷款调查人员和房地产经纪人。在传统的交易中，这个过程中可能出现不必要的拖延，因为不同的利益相关者需要知道，在每一个阶段，交易当中的哪一方需要做些什么，才能继续推进。同时，无论是买方还是卖方，都严重依赖中介。

英国主管土地所有权登记的政府机构——英国皇家土地登记处日前宣布，开始尝试利用区块链技术进行英国房产登记注册的项目。

一旦有了区块链的参与，这个过程就可以透明化，增加各方的信任，减少官僚作风。自动执行合同（或“智能合同”），区块链技术可以保证已经完成所有必需的步骤之后，款项才开始转移或所有权才会转移。区块链的分布性使交易中任何一方不再依赖唯一的“真相来源”（中介），增加各方的信任，降低成本，加速交易。

不难想象，如果买卖双方能够更清楚地看到和批准对方的举动，中间商就不再是唯一的掌握关键信息的人，一些中介角色就会减少甚至消失。

除了商业交易，区块链还可以应用于生活中的其他领域。举一个例子：

通常人们结婚要举行一个婚礼，在婚礼上双方说出誓言，亲朋好友都是证明人，婚礼上还有一个证婚人。

一对名为蒙德鲁斯·戴和乔伊斯·巴约的夫妇可能是第一对用比特币来纪念彼此结合的夫妇。他们当着大约50位客人的面，利用一台比特币自动柜员机记录下了自己的书面婚誓。他们的誓言将会保存在区块链里，也就是一个可以永久存储信息的开放账簿里。

在这个案例里，区块链技术可以承担证婚人的角色，人们可以把结婚数据储存在区块链里，以一种只能回顾却无法修改的方式储存起来。

尽管目前关于区块链的相关应用还在探索之中，但是我们不难想象，一旦区块链的去中心化能在各个领域全面开花，其对整

个世界将会带来多么大的改变，“智能信任”将给人类生活带来怎样的便利。

[1] 最早出自《纽约时报》的一篇文章《区块链有望消灭一切中间人》（Data Security is Becoming the Sparkle in Bitcoin），方小华译。<http://www.8btc.com/the-sparkle-in-bitcoin>。

1 从零开始，认识区块链

我们可以把区块链看成是一个分布式的总账本，而每一个区块相当于这个总账本中的一页。它通过算法解决了“点对点传输”中的“共识机制”问题，实现了“点对点数据传输”的去中心化。此外，它还具有开放性、自治性、数据不可篡改、可追溯性、匿名性的优势。

区块链技术的发展分三个阶段或领域：区块链1.0、2.0和3.0^[1]。区块链1.0对应的是货币，区块链2.0对应的是智能合约，区块链3.0则延伸到一切领域。

区块链是通过“共识机制”来达成一致的，比特币的共识机制为PoW，即“工作量证明”，区块链是比特币的底层技术。

[1] 区块链1.0、2.0、3.0的概念由美国区块链科学研究所创始人梅兰妮·斯万在他的《区块链：新经济蓝图及导读》一书中首次提出，后被业内广泛使用。

区块链的发展之路：从1.0到3.0

区块链1.0时代主要是指区块链诞生之初，其技术探索主要是货币和支付领域的去中心化，其主要应用就是比特币。因此，也可以简单地认为，区块链1.0就是指比特币系统。

如果说区块链1.0实现了比特币交易中的去中心化，那么区块链2.0就是将这种去中心化延伸到其他的资产领域。比特币是一种资产，在比特币网络中，去中心化运转得很安全，那么能否把这项去中心化的技术应用到其他资产的交易和转换中呢？

这就有了区块链2.0，伴随着区块链2.0的是智能合约的诞生。主要指通过智能合约的方式将去中心化技术应用于注册、确认、转移各种不同类型的资产及合约。所有的金融交易都可以通过智能合约的方式在去中心化的情况下实现交易和转移，包括股票、私募股权、众筹、债券、对冲基金和所有类型的金融衍生品（如期货、期权）等。

区块链2.0超越了货币范畴，延伸到所有的资产，包括有形资产（股票、基金等），也包括无形资产（知识产权等）。

什么是智能合约呢？

传统合约是指双方或者多方协议合作或者交易时，每一方必须信任彼此会履行义务，还需要第三方监督的参与（通常是法律或者仲裁）。而智能合约无须彼此信任，因为智能合约不仅是由代码进行定义的，也是由代码强制执行的，完全自动且无法干预。到了约定的时间，机器就自动执行。

在这个基础上衍生出了智能资产这个概念。

使用区块链编码的资产通过智能合约就成为智能资产。智能资产是指所有以区块链为基础的可交易的资产类型，包括有形资产和无形资产。智能资产通过区块链控制所有权，并通过合约来符合现有法律。比如，预先建立的智能合约能够在某人已经偿还全部贷款后，自动将车辆所有权从财务公司转让到个人名下，这个过程是全自动的。

区块链2.0时代，人们对区块链应用的构想，除了智能资产，还包括无需信任的借贷。

让不认识的人在互联网上把钱借给你，而你可以将你的智能资产作为抵押，这必然大幅降低借贷成本，让借贷更具竞争力。非人为干预的机制也让纠纷率大大降低。

以太坊也是区块链2.0的产物，它是一个开放的智能合约完整解决方案。^[1]比特币是区块链1.0最重要的运用，很好地完成了货币和支付交易。但是当我们需要记录和转移更多复杂的资产类型时，我们就需要第三步——更强大的脚本系统——最终实现图灵完备（能够运行任何货币、协议和区块链）。以太坊就是一个区块链为基础的项目，旨在提供一个图灵完备脚本语言和图灵完备平台。

区块链1.0主要是指比特币，区块链2.0延伸到一切资产，而区块链3.0则超越了货币，超越了金融领域，甚至超越了商业领域，延伸到一切领域，渗透到我们生活的方方面面，包括政治、社交、教育、医疗等。按照行内人士的预测和构想，区块链3.0时代在未来5年将会得以实现，那时，区块链将变得和互联网一样被所有大众认知和接受，从而全面颠覆我们的生活。

麦肯锡公司向美国联邦保险咨询委员会提交了一份区块链技术报告，报告把2009年至2016年称为“黑暗时代”，认为此期间所有区块链解决方案都基于比特币，而区块链的新时代将从2016年开始。届时，区块链的应用将变得空前广泛。应用麦肯锡报告中的一句原话：基于区块链目前的发展速度，我们认为区块链解决方案也许会在未来5年实现全部潜力。^[2]

[1] <http://www.8btc.com/blockchain-2-ethereum>.

[2] <http://www.8btc.com/mckinsey-sees-blockchain-technology>.

区块链的共识机制

区块链系统会选取记账最快、最好的那个节点，以这个节点的账目为准，并发送备份给所有节点。那么，系统是凭什么来认定最快、最好的节点的？最快、最好的标准是什么？其他节点为什么会同意某个节点的记账？人人都参与记账，那么如何保证他们的账目都是正确的？会不会有些节点出于私利伪造或者篡改信息，会不会有节点恶意搞破坏？靠什么来保证节点数据的一致性和正确性？换句话说，靠什么达成共识？这就涉及区块链的共识机制。

去中心化的共识难题

在一个中心化的系统里，因为有权威化的中心存在，要达成共识是很容易的。例如，A跟B借10万元钱，传统的操作方式是双方去公证处公证，或者请一个颇具权威的中间人来进行担保。这样，想赖账就不可能了。

那么，在一个去中心化的系统里，没有权威中心的存在，没有公证人，没有担保公司，也没有中间人，A如果借了B的10万元钱，最后不承认不还钱怎么办？

为了方便大家对去中心化的理解，依然以刚才的借贷为例，我们来建一个最简单的去中心化模型。

如果A借了B 10万元钱，他们既不找公证，也不找中间人，其操作方法是：A在人群中喊一声，“我是A，我找B借了10万元钱！”B也公开承认，“我是B，我借了10万元钱给A！”此时整个系统里的人都听到了这个消息，大家各自在账本上记下“A找B借了10万元钱”。需要指出的是：在这个系统中，所有人都能收到A的信息，却不知道其他人的存在。

这就是一个去中心化的系统，我们会发现，在这个系统中不需要公证，不需要证明人，甚至连借贷协议都不需要，也不需要人与人长久的信任关系。倘若A赖账，系统里的其他人就会翻出账本：××时间，A找B借了10万元钱。

看起来是不是很简单？去中心化的记账是一个公开透明的系统，完全不需要第三方监督或者证明。但是，这当中存在两个致命的问题：

(1) 由于是点对点的沟通，系统中有那么多人，他们都能接收到A的信息，但是所有节点之间却并不认识，也无法交流，

如何能够保证所有人的记账都是同步的呢？

(2) 假如有的人没有听清楚，把账记错了，或者包庇A，故意做假账，怎么办？

一个账本中，假如出现时间和账目不一致的情况，那它就是无效的。例如，上述例子中，C记载的是“A找B借了10万元钱”，D记载的是“A找B借了1万元钱”，后面记的账更是五花八门。那么这个账本就无效了，B完全可以赖账。

这就是去中心化系统所面临的两大难题：同步性问题和一致性问题。

同步和一致，在过去的技术下是做不到的。因为是点对点的通信，双方不可能在这种情况下达到信息的一致性。严谨一点，就是“在分布式计算上，试图在异步系统和不可靠的通道上达到一致性是不可能的”。

PoW的缺陷以及其他共识机制

工作量证明使得区块链系统在没有中心的情况下也能达成共识，但是对工作量证明也有一些批判，一个常见的指责就是“浪费能源”，因为节点计算需要耗电，挖矿已成为能源密集型产业。

出于对消耗能源的担忧，也有科学家在探索和实践新的共识机制。

PoS (proof of stake)：权益证明机制

一个典型的共识机制就是权益证明机制，以节点持有币的数量和实践来选择记账权。

如果把PoW理解为“干得越多，收获越多”，那么PoS就是“持有越多，获得越多”。

它的优点是：相对于PoW，一定程度上减少了数学运算带来的资源消耗。同时，它根据每个节点所持有的数字货币的比例和时间，等比例地降低挖矿难度，从而加快了寻找随机数的速度，在一定程度上缩短了共识达成的时间。

它的缺点是：还是需要挖矿，且所有的确认都只是一个概率上的表达，而不是一个确定性的事情，理论上有可能存在其他攻击影响。例如，以太坊的DAO攻击事件造成以太坊硬分叉。

DPoS：股份授权证明机制

它类似于董事会投票，持币者投出一定数量的节点，代理其进行验证和记账。它与PoS原理相同，只是选了一些“代表”。与PoS的主要区别在于节点选举若干代理人，由代理人验证和记账。

该模式可以每30秒产生一个新区块，并且在正常的网络条件下区块链分叉的可能性极其小，即使发生也可以在几分钟内得到解决。

其缺点是必须是在该区块链系统有一定影响力的人才资格获得记账的权利。

还有燃烧证明、沉淀证明等。

不过，这些并没有从本质上达到节省能源的目的，当前工作量证明仍然是最可靠和最有效的去中心化共识机制。

区块链的技术基础

区块链是一种“点对点”的数据传输和储存，它在最基础的数据层中，会用到哈希函数、密钥技术（主要是非对称加密）、Merkle树、时间戳、数字签名等技术手段。在传输层中，会涉及P2P网络、传输机制、验证机制。在共识层面会运用到PoW、PoS等各种共识机制。传输层相对容易理解，共识层前面已经讲过，因此在这里，我们仅介绍它在数据层所运用的相关技术。

哈希函数

哈希函数 (Hash Function)，也称为散列函数或杂凑函数。哈希函数是一个公开函数，可以将任意长度的消息M映射成为一个长度较短且长度固定的值H (M)，称H (M) 为哈希值、散列值、杂凑值或者消息摘要。

哈希函数满足三个特性：

- (1) 消息M的任何改变都会导致哈希值H (M) 发生改变。
- (2) 在给定某个哈希函数H和哈希值H (M) 的情况下，得出M在计算上是不可行的。

所谓的“在计算上不可行”，依据计算复杂度理论的说法，是指对于该运算不存在一个多项式时间算法，例如大数分解和离散对数问题。上述计算不可行是哈希函数安全性的基础。如果把一段消息比作一个人，这段消息的哈希值就是这个人的指纹，是这个人独一无二的特征。

作为区块链技术基础的哈希函数，还需要具有以下特征。

免碰撞

其实这个特点在理论上并不成立，比如，比特币使用的SHA256算法，会有 2^{256} 种输出，如果我们进行 $2^{256}+1$ 次输入，那么必然会产生一次碰撞；甚至从概率的角度看，进行 2^{130} 次输入就会有99%的可能发生一次碰撞。不过我们可以计算一下，假设一台计算机以每秒10000次的速度进行哈希运算，要经过10~27年才能完成 2^{128} 次哈希。因此，发生碰撞的几率是极其小的。

隐匿性

也就是说，对于一个给定的输出结果H (M)，想要逆推出输入M，在计算上是不可能的。以上特点是比特币的工作量证明系统可以正常运行的基石。

难度值 (difficulty) 是矿工们挖矿时的重要参考指标，它决定了矿工大约需要经过多少次哈希运算才能产生一个合法的区块。比特币的区块大约每10分钟生成一个，为了让新区块的产生基本保持这个速率，难度值必须根据全网算力的变化进行调整。

哈希函数通过调整难度值来确保每个区块挖出的时间都大约在10分钟，哈希函数计算的难度值对保证区块链系统的安全意义重大。正如美国的几位计算机科学家在共同所著的书中所写的：“哈希密码是密码学中的瑞士军刀，它们在众多各具特色的应用中找到了一席之地，为了保证安全，不同的应用会要求不同的哈希函数特点。事实已经证明，要确定一系列哈希函数以全面达成可证安全极度困难。” [1]

工作量证明需要有一个目标值。比特币工作量证明的目标值 (target) 的计算公式如下：

目标值 = 最大目标值 / 难度值

其中，最大目标值为一个恒定值：

0x00000000FF

目标值的大小与难度值成反比。比特币工作量证明的达成就是矿工计算出来的区块哈希值必须小于目标值。

我们也可以简单理解成，比特币工作量证明的过程，就是通过不停地变换区块头（即尝试不同的随机值）作为输入进行SHA256哈希运算，找出一个特定格式哈希值的过程（即要求有一定数量的前导0）。而要求的前导0的个数越多，代表难度越大。

[1] 阿尔文德·纳拉亚南，约什·贝努，等. 区块链：技术驱动金融[M]. 林华，王勇，帅初，等译. 北京，中信出版社，2016.

密码学基础

区块链采用密码学的方法来保证已有数据不可能被篡改。

这个部分的两个核心要点是：①密码学哈希函数，②非对称加密。两个都是密码学的基础概念。

可以说，区块链的诞生得益于密码技术的发展，数字货币正是在密钥技术的发展过程中产生的。

我们来看看密码朋克们对密钥技术的探索过程。

1976年，Whitfield Diffie与Martin Hellman在开创性论文《密码学的新方向》（New Directions in Cryptography）中，提出公开钥匙密码学的概念。他们俩发明的Diffie-Hellman算法是一种密钥交换方法，交换密钥后还需要其他算法来进行加密和解密。这个算法是今天互联网安全的基础。他俩的成就在于，告诉世人非对称加密以及公钥加密是可行的。

Hellman在20世纪70年代险些被美国军方关进监狱，要知道加密技术一直都是政府和军方的重要武器。密码科学家们要么为军方和政府工作，要么就要面对来自政府的威胁。密码学和区块链的很大一部分这种去中心化的理念常常被认为是无政府主义和过度自由主义。中本聪至今还匿名，聪明且谨慎啊。

1982年，大卫·乔姆提出不可追踪的密码学网络支付系统。他发明了乔姆盲签名，可以说他是密码货币的始祖，这个不可追踪的密码学网络支付系统，就是今天比特币的老祖宗。1900年，大卫·乔姆成立了数字现金公司，并试验了一个数字化的货币系统，名字为Ecash，这应该是世界上的第一种电子现金，当时风头很劲，包括微软、维萨等大公司都要收购Ecash。不过，中本聪对Ecash不屑一顾，认为它依然是传统的中心化系统，必须依赖中心化的信用。大卫·乔姆的数字现金公司于1998年宣告破产。其失败的主要原因就是这个系统对个人之间的交易无法起到很好的支持作用，而银行和商家也不愿意使用。

1985年莱斯利·兰伯特等人提出了拜占庭难题。这真是区块链、比特币最重要的核心问题，就是如何解决公开网络上的信任问题。1982年，Leslie Lamport把军中各地军队彼此取得共识、决定是否出兵的过程，延伸至运算领域，设法建立具容错性的分布式系统，即使部分节点失效仍可确保系统正常运行，可让多个基于零信任基础的节点达成共识，并确保资讯传递的一致性。

1992年，蒂莫西·梅成立了密码朋克^[1]，这个组织里有一大批跟区块链技术的发明息息相关的大人物，包括大卫·乔姆、Phil Zimmerman (PGP)、阿桑奇、亚当·贝克、戴伟（名字是中文，不知道人是不是华裔，他在圈子中地位尊崇）、哈尔·芬尼、Tim-Berners Lee爵士（万维网发明者）、John Perry Barlow（赛博自由主义政治活动家）、尼克·萨博（BitGold发明人，智能合约的发明人），等等。

在互联网刚刚兴起的时候，很多天才都打起了电子货币的主意，如Beenz和Flooz都是当年的电子货币，但是全都死翘翘了。正如中本聪所说：中心化的电子货币都是垃圾，必死无疑。若是还依赖中心机构的信用来发行电子货币，那么与网银有何区别？

另一个对区块链技术贡献很大的人就是亚当·贝克，他发明了哈希算法，其中用到了工作量证明系统。他的本意，是实现电子邮件的可信。发送电子邮件之前，需要运算一个数学题，这样发送大量垃圾邮件就会成本巨大。这个思想，被哈尔·芬尼借鉴用来做可重复的工作量证明机制，随后，又被中本聪用到比特币中，完美地解决了拜占庭难题。

哈伯和斯托尼塔在1997年提出一个用时间戳的方法保证数字文件安全的协议。这个技术用简单直白的话语来解释就是：用时间戳的方式记录文件创建的先后顺序，协议要求在文件创建后其时间戳不能改动，这就使文件被篡改的可能性为零。这个协议后来成为比特币区块链的原型。

1998年，另一名密码朋克戴伟提出了匿名的、分布式的电子加密货币系统——B-money。B-money的设计在很多关键技术特质上与比特币非常相似，但是不能否认的是，B-money有些不切实际，其最大的现实困难在于货币的创造环节。

在B-money系统中，要求所有的账户持有者共同决定计算量的成本并就此达成一致意见。但计算技术发展是日新月异的，而且有时并不公开，计算量的成本这类信息并不准确、及时，也难以获得，因而B-money很难成为现实。戴伟为此设计了复杂的奖惩机制以防止节点作弊，但是并没有从根本上解决问题。戴伟的很多设计被中本聪所借鉴，二人有很多邮件交流。

2004年，哈尔·芬尼推出了自己的电子货币，在其中采用了可重复使用的工作量证明机制（RPoW）。同时，他也是第一笔比特币转账的接收者。

此外，区块链的诞生，还要感谢肖恩·范宁和肖恩·帕克点对点网络技术的开发。关于点对点技术，即P2P协议，一个大家很熟悉的例子是我们所用的迅雷，我们的一切种子，都是一种点对点的传输。有了P2P协议，才有了后来的比特币。

[1] 密码朋克是1992年筹备成立的，但密码朋克这个术语于1993年在Eric Hughes 的A Cypherpunk's Manifesto 中首次正式出现。

侧链技术

侧链是一种特殊的区块链。它使用一种叫作“SPV楔入”的技术实现与其他区块链之间的资产转移。

本质上来说，一个SPV证据是由一系列演示证据的模块头和建立在其中的一个模块的输出组成的。这就允许检测者检查一些委托输出的存在工作。这样的证据可能因为另一个以更多工作强调的链（不包括创建输出的模块）变得无效。

使用SPV证据去确定历史，假装相信最长的模块链也是最长的正确的模块链，是由比特币中所谓的SPV客户端决定的。只有当不诚实的勾结拥有了超过50%的分散权利时，才可能欺骗SPV客户端。[1]

侧链协议是可以让比特币安全地从比特币主链转移到其他区块链，又可以从其他区块链安全地返回比特币主链的一种协议。实质上，侧链是一个类似于比特币的独立的、开放的分布式网络，它不是特指某个区块链，而是指遵守侧链协议的所有区块链，该名词是相对于比特币主链来说的。除比特币主链外，所有现存的区块链，如以太坊、莱特币等区块链都属于侧链。

由于侧链是一个独立的、隔离的系统，侧链中出现的严重问题只会影响侧链本身，这极大地降低了比特币主链创新的风险和成本。

它的原理是通过“双向锚定”机制实现主链货币（也就是比特币）价值向侧链系统转移，由主链货币提供信用背书可以产生和发行侧链货币。简单地讲，侧链技术就是由比特币做信用背书而创造出来的旁链，在这些链上发行的数字货币被称为“山寨

币”。

[1] <http://www.wanbizu.com/baike/201411133449.html>, <http://www.blockstream.com/sidechains.pdf>.

区块链的几种类型

区块链根据技术手段、开放程度的不同，可分为公有区块链、联盟（行业）区块链、私有区块链。公有区块链是所有人都参与记账的，被认为是“完全去中心化”的，几乎所有的数字货币都是基于公有区块链。联盟区块链是由某个群体（联盟）参与记账的，被称为是“多中心化”的，当前市面已有不少知名的联盟链。私有链是由某个团体、企业或者个人独享记账权限的，被认为是部分“去中心化”，私有链目前还处于尝试和探索阶段。

公有区块链

公有区块链是指，世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与它的共识过程。公有区块链是最早的区块链，也是目前应用最广泛的区块链，几乎所有的数字货币都是基于公有区块链，每一个币种，世界上仅有一条与之对应的区块链，比特币区块链是公有区块链的始祖。

公有区块链的特点是：

- (1) 公有区块链通常被认为是“完全去中心化”的。
- (2) 在公有区块链中程序开发者无权干预用户。
- (3) 进入门槛低，几乎只要有一台能联网的计算机就可以进入。
- (4) 链中的所有参与者都是隐藏身份的，但链上的所有数据则是公开的。

私有区块链

私有区块链指的是仅使用区块链的总账技术进行记账，可以是一个公司，也可以是个人，独享该区块链的写入权限。读取权限是否对外开放，由该私有链的所有者决定。

私有链的特点是：

- (1) 交易速度非常之快。
- (2) 给隐私更好的保护。
- (3) 交易成本大幅度降低，理论上可以为零。
- (4) 如果说公有链是“完全去中心化”，联盟链是“多中心化”，那么私有链是“部分去中心化”。

关于私有区块链，当前也有一些争论，例如有些人认为区块链为企业所私有，用处不大，因为私有链让用户依赖管理区块链的企业，实际上形成了“中心化”，因此也有很多人认为私有区块链不属于区块链。

目前，私链的应用产品还在摸索当中。

区块链在金融业的应用

信用是金融业的基础。为了解决信用问题，金融业的发展催生了大量的中介机构，包括托管机构、第三方支付平台、公证人、银行等。区块链是一个制造信用的机制，它可以实现信用机制的“去中心化”，从而大大提升效率和降低成本。可以说，区块链和金融的结合度非常高，金融也是区块链除数字货币以外最早的应用领域。这里，我们仅从数字资产管理、跨境支付与结算、证券发行交易及客户征信，以及反诈欺、反洗钱、透明度等方面来讲述区块链在金融领域的应用。

区块链打造智能资产，将改变资产管理的方式

由于区块链把比特币管理得很好，很多人就想到，能否用类似的机制来管理其他的资产呢？这个想法，几乎是每个学习、研究区块链的人都会想到的。按照理想化的设想，把区块链技术搬到其他资产管理领域，不需要中介，也不需要更多的技术创新，就可以打造一个去中心化、更安全、防篡改、可追溯的智能资产管理平台，这个前景是多么诱人。

按照业内人士的构想：区块链可以将所有资产都变成智能资产，用数字化的方式管理。未来这一技术有可能会全面改变人们的资产管理方式。

基于区块链技术的智能资产

如何用区块链技术打造智能资产呢？

区块链可以用于任何资产的注册、交易，包括房产、汽车等有形资产，也包括股票、知识产权等无形资产，很容易进行所有权的确权。

而智能资产的核心就是控制所有权，一旦确权，对于在区块链上注册的数字资产，能够通过私钥来随时使用。

是否还有点抽象？举个例子，一旦将资产变成智能资产，并且用区块链来管理，那么，可以做到：当一个人偿还全部贷款后，自动将汽车从财务公司名下转到个人名下（这个过程可能需要多个相关方的智能合约共同执行）。

区块链打造智能资产的优点

基于区块链的智能资产，是一个去中心化的资产管理系统，在这个系统里，机器信任取代了人工信任，只要物权法能跟上智能资产的发展，运用区块链，在资产本身上记录所有权，确权十分容易，将极大地提升资产管理的效率。

同时，区块链对资产的智能化管理，也可以避免纠纷。

区块链打造智能资产的广阔前景

未来，我们的房产、车库、门禁系统等都会植入一个识别芯片，运用主人注册在区块链的数字身份可以立即识别。

区块链还可以让我们的资产产生更多的价值。

例如，用区块链来管理自己的车，在自己不用的时候可以将它“共享”出去，获取收益。因为有区块链的确权和智能合约，

不用担心车辆遗失，也不需要租车行等相关中介的参与，对于租车方来说，也不需要那么高昂的押金。即便是租来的车，也可以在闲置时作为“二车主”把使用权短租给同事。

可以说，用区块链来打造智能资产，其想象空间是无限的。未来十年智能资产将快速发展，会在某些领域快速得到运用，而区块链在确权方面的优势，加上智能合约的便捷性，将会成为智能资产的底层架构。

当然，区块链打造智能资产要大面积投入应用还需要相当长的时间，首先人们适应用代码来控制资产的方式需要一个过程，其次还有法律、监管层面的问题。

区块链大大简化证券清算结算的流程

中国股民数量已超1亿人，支持如此庞大数量的股民完成交易的是一个非常复杂的系统。传统的证券交易需要经过中央结算机构、银行、证券和交易所四大机构之间的协调，效率低、成本高。

近年来，越来越多的金融机构开始探索将区块链技术应用用于股权交易领域。例如，纳斯达克开发基于区块链的证券发行与交易管理系统，澳大利亚证券交易所探索利用区块链升级证券结算系统等。

以往的证券清算和结算

清算和结算是指什么呢？

通俗地讲，客户买股票是从交易所买的，但是不能直接买，必须在证券公司营业部通过证券公司的席位或者交易单元来买。在购买的时候，登记公司负责对客户的股票进行登记，其间客户转钱还需要通过银行。所以一个完整的证券交易有客户、证券公司营业部、交易所、登记公司、银行等多个主体的参与。

清算将客户、证券公司营业部、登记公司、交易所和银行产生的数据分别进行计算和核对。

与清算相关的还有一个概念叫交收，交收指的是根据清算的结果在事先约定的时间内履行合约：买方支付一定款项获得所购证券，卖方交付一定证券以获得相应价款。

清算加上交收，就构成了结算。

当前，证券交易平台的惯例和趋势是交易平台与结算平台前后分离。

从我国的实际情况来看，证券市场已经形成“两所两网”的局面，大家互相独立，而市场参与者却是共同的。基本上券商都会同时拥有“两所两网”的交易席位，但交易清算结算机制又互相独立，加重了券商的成本负担，增加了资金周转风险。

另外，传统清算登记系统过分依赖场内交易，对清算登记系统的发展不利。

还有，资金清算依赖于银行体系，尤其是人民银行电子联行系统。因此，银行系统的效率直接影响证券市场资金交收效率。

区块链大大简化清算结算流程，实现交易即结算

区块链是一个跨领域、全球性的数据库，它有别于过往的去中心化，是一个相互独立的系统。

区块链具有的安全透明、数据不可篡改、数据可以追溯等特点，可以在证券登记、股权交易、证券发行等方面发挥其作用，

更高效、更安全。

传统的上市流程中，需要先审核，再发行和交易。由于区块链可以追溯数据和交易，它在证券清算结算的过程中能够省略清算所、市议员去验证交易的步骤，不再需要托管人员去验证投资者股票持有的真实性。

更深入地讲，区块链技术实际上是在交易系统中省略了中间人和后台，降低了第三方市计、记账和验证交易的高额成本。

区块链的点对点交易，意味着清算结算过程可以做到交易即结算，与传统的“T+3”和“T+2”清算时间相比，区块链技术提高了资产的流动性，让交易者持有股票等同于手持现金。

区块链技术还带来了高透明度的权益市场，由于每个交易参与者都有完整的交易记录，因此暗箱操作将会很难实现。同时，区块链的数据不可篡改的特性，可以避免伪造、篡改交易记录等不良现象。

区块链技术也将改变证券发行的规则，基于区块链技术的智能合约，在最理想的情况下，可以实现任何人以自己设定的方式自行发行资产凭证。

应用实例

案例一：美国在线零售商Overstock曾和创业公司Counterparty合作共同开发了一个名为美第奇（Medici）的项目，后来因为种种原因，美第奇项目没有开发成功，但双方推动区块链技术在证券市场应用的努力却没有停止。在此之后，Counterparty与MathMoney f(x)公司合作开发了瞄准证券市场的symbiont.io，而Overstock也继续开发自己的区块链项目并在2015年4月率先公布了名为0的部分项目信息，该平台的目标是基于区块链技术实现股权的交易和结算功能，发挥区块链“交易即结算”的优势。

2015年8月，Overstock在纳斯达克的一次活动上正式推出了区块链交易平台项目1.0，设计目标是基于区块链技术建立可实现证券交易的实时清算结算功能的全新系统，该系统同时包括了证券的发行功能。

2015年10月底，纳斯达克宣布要推出基于区块链技术而建立的新平台Linq，该平台以在私募证券市场建立一种全新的股票发行、转让和出售方式为目标，将可能彻底改变资本市场基础设施系统的核心，尤其是对于交易结算和行政审批等过时的管理功能的颠覆。

案例二：澳大利亚证券交易所（ASX）也在认真考虑使用区块链技术作为其清算和结算系统的升级方案。ASX已经认购了区块链技术开发商DAH公司的1500万美元股份，主要就是为了优先使用区块链技术升级ASX的股票系统，DAH将与纳斯达克一起为澳大利亚证券市场设计结算系统。

ASX正在寻求新技术以提高终端之间的效率，大量削减来自投资银行和交易后端的管理成本，而这正是区块链的潜力所在。

此外，澳大利亚政府也将对区块链是否适合在证券清算行为上应用进行评估，如果可行，ASX将会积极推进研究。

区块链让知识产权保护更容易

传统知识产权一直面临确权耗时长、时效性差，用权变现难、流通不顺畅，维权难、溯源难这三大难题。由于侵权严重，原创作者生存艰难，创新乏力，进而导致抄袭篡改的作品长期霸占屏幕，无法获得优质内容。

区块链通过程序算法自动记录信息，移除了第三方，将知识产权的信息储存在互联互通、共享的全球网络系统中，无法被任意篡改，极大地提高了维权的效率，也许会彻底改变目前全球知识产权保护的格局。

区块链与知识产权的应用实例

当前，区块链技术应用于知识产权交易大致有两个方向：一是利用区块链进行确权维权，二是在线的知识产权交易。

案例一：法链

这一领域最著名的应用案例，就是小蚁、微软和法大大合作成立的法链。

“法链”的成立，有望开创出电子文件的全新存储模式。目前，法大大平台电子合同的日均签署量在当前10万份的基础上保持着持续的增长。根据“法链”相关人士的介绍，未来将有更多的司法鉴定机构、公证处、在线仲裁机构、律师事务所等权威第三方机构加入“法链”，构建一个

全新的知识产权保护模式。

线下的知识产权交易文件也可以保存在法链上，如果合同中明文要求所有交易记录都必须在法链上签署并保存的话，法链则可以提供完整的交易证明。

案例二：Left Gallery

区块链可以将我们的资产变成数字资产、智能资产，知识产权也是数字资产的一种。因此，可以利用区块链技术，让知识产权像股票一样在线交易。Left Gallery就是一个著名的应用案例。

这是一个数字展览馆，它是由荷兰柏林艺术家Harm van den Dorpel创立的。这个项目可以帮助艺术家以“下载对象”的方式，出售他们的作品。Left Gallery使用比特币作为付款方式。

它的基本原理是，数字资产的发行方，通过抵押价值150%~250%的数字货币发行数字资产。数字资产与实际资产可兑换。实际专利的持有者可兑换成数字专利，从而获得数字交易的好处，可以像比特币一样分成很小的份额与他人交易，和企业股票一样交易，但是在比特股或者以太坊这样的区块链平台上公开透明地自动化进行。数字专利的发行方与数字专利的持有者约定可以自由兑换，保证数字专利与真实专利的等值。

当数字资产升值，或者基础数字货币贬值导致抵押物价值低于给定阈值时，系统将自动实际清算，卖出抵押物平仓。

案例三：IkonoTV

IkonoTV是第一个高清艺术电视广播频道，这一频道和超过1000位艺术家进行了合作，IkonoTV使用了区块链技术，这项技术适用于加密签约，能使著作权始终清晰，该频道的收看观众超过3亿人。

案例四：Cointemporary

Cointemporary是一个用于展示和出售艺术品的在线平台。在该平台上，单件艺术品的出售时间为10天，在展出期间，它以固定的比特币价格出售。当这件艺术品售出或10天出售时间过去时，平台会展出另一件艺术品。Cointemporary由两位维也纳艺术家Valentin Ruhry和Andy Boot共同创立。

案例五：N3uro

N3uro是一个出售想法的市场。从字面上来讲，该平台抓住了人的脑电波，并出售这些有限的数字版本脑电波记录。N3uro官方网站指出：“这些有限的数字版本，是版权和合同的组合方法，而比特币区块链则作为所有权登记的方式。”

案例六：Plantoid

Plantoid是一个区块链机器人，它使用了比特币捐款来复制自己。它聘用艺术家来对它复制和进行改善。基本上，它是一个横跨电子和物理世界的DAO，并提出了有关版权和所有权的问题。它是一项相当有趣的发明，能使艺术品变得“具有生命，能够自我复制和进行创造”。

案例七：Blockai

Blockai宣布他们在种子轮融资中已经筹集到了547000美元来重启区块链版权服务。

在2015年成立之初，Blockai被设想为“比特币的Netscape浏览器”，当时Blockai尝试将区块链变成一种社交媒体流，允许用户发送信息和鉴证产品。现在Blockai致力于打造一种新工具，允许艺术家证明或声明自己对图片拥有版权。

有专业人士认为这是美国国会图书馆注册版权和不作为之间的方法。从技术上看，任何作品一旦完成就可以进行版权注册。只是，如果想要告别人侵权，必须先注册账户。但是在对旧金山湾区作家的采访中发现，只有10%的人在美国国会图书馆注册版权，其余的人觉得没有必要注册。Blockai的目的就是提供优于费时费钱的正式注册的公共数据库注册方式，也就是在区块链上注册版权来证明著作权。

在Blockai平台上，你只需要简单的一个鼠标拖动动作就可以进行作品注册，并获得对应的版权证书。如果之后有人未经允许复制你的作品，你就可以给他发送一份版权证书来警告他。

案例八：Mediachain

Mediachain打造图片数字库—通过拖拽、复制粘贴等手段，图像是最容易在互联网上分享的媒体类型。图像会像病毒一样传播，但是其创造者和内容所有者却很难从中受益。Mediachain试图运用区块链技术解决这一难题。

区块链让物联网真正链接万物

传统的物联网模式依然由一个中心化的数据中心（服务器）来负责处理信息，依然依赖中心化的代理通信模式，当接入的节点成数十亿、百亿、千亿计算时，中心化的云服务器恐怕难以承受其负担，且维护的成本很高。同时，节点越多，可能出现漏洞的环节就越多，安全性令人担忧。区块链与物联网结合，则可以为物联网提供安全保障，并起到降低成本的作用。可以说，区块链让物联网真正链接万物。

区块链技术可以作为物联网下的基础设施建设

区块链与物联网也是当前炒得很热的一个话题，那么区块链和物联网到底是怎么结合在一起的呢？区块链在物联网领域可以有哪些作为？

首先，我们来认识一下物联网。

什么是物联网

先普及一下什么是物联网，物联网这个词我们可以说是如雷贯耳，可是很多人对这个概念依然模糊。

物联网是新一代信息技术的重要组成部分，其英文名称是The Internet of Things。顾名思义，物联网就是物物相连的互联网。物联网的核心依然是互联网，是在互联网的基础上进行延伸的网络。它和互联网的差别在于：物联网的链接范围更广泛，互联网的客户端，最开始是PC，后来是智能手机，而物联网的客户端可以延伸至万物，任何物品之间都可以相连。举几个简单的例子：

在饭桌上装上感应器，饭桌可以接收信息，可以上网，可以作为通信工具；医院可以远程监控和调节病人的病情；工厂可以自动化处理生产线的问题；酒店也可以根据客人的喜好调节室内的温度和照明等。

随着信息技术的发展，低成本的信息设备将进入千家万户，连接在互联网上的设备呈几何级数增加。2009年互联的设备全球是25亿台，现在是100亿台，而据IBM预测2020年互相连接的设备将超过250亿台。^[1]

那么，区块链和物联网到底有什么关系呢？

物联网可能存在的问题和缺陷

传统的物联网模式依然是由一个中心化的数据中心（服务器）来负责处理信息，依然依赖中心化的代理通信模式，不然就是服务器/用户端模式。所有的设备都是通过云服务器验证连接的，该云服务器具有强大的运行和存储能力。设备间的连接将会仅仅通过互联网实现，即使这只是在几米的范围内发生的。

虽然用这样的模式连接计算机已经有几十年的历史了，支持小型的物联网网络也没什么问题，但却满足不了日益增长的物联网生态体系的需求。随着物联网技术的飞速发展，当万物都可以连接时，可想而知这个网络有多庞大，仅仅靠一个中心化的云服务器来控制所有数据，问题自然而然就出现了。

第一个问题是成本的问题：当前的物联网解决方案非常昂贵，因为在庞大的网络下，对中心化云服务器的要求非常高，而大型服务器和网络设备的基础设施和维护成本是非常高的，一旦物联网设备的数量增加到数百亿甚至千亿时，成本可想而知。

第二个问题是安全的问题：物联网的安全性存在缺陷，缺乏设备与设备之间相互的信任机制，所有的设备都需要和物联网中心的数据进行核对，一旦数据库崩塌，会对整个物联网造成破坏。

区块链技术可以作为物联网下的基础设施建设

物联网是非金融领域与区块链联系最为密切的应用，如果把区块链的优势与物联网相结合，就可以保证设备网络的真实性，节省一些繁杂的环节，降低成本。

区块链具有去中心化、公开透明、安全通信、难以篡改等特点，为物联网提供直接互联的方式来传输数据，降低了中心化架构的高额运维成本。

同样，区块链分布式的网络结构可以提供一种机制，使得设备之间保持共识，无须与中心进行验证，这样即使一个或多个节点被攻破，整体网络体系的数据依然可以运行，是可靠安全的。

[1] <http://iot.ofweek.com/2016-12/ART-132209-8120-30081350.html>.

区块链确保物联网信息安全，保护用户隐私

首先，物联网的安全问题一直都是行业内外非常关心的问题。

物联网可能存在的安全隐患

当前的物联网整体还是中心化的，所有的监测数据和控制信号都由一个中央云服务器存储和转发。云服务器收集的信息十分广泛，不仅包括文字和图片信息，还包括所有的摄像头传输过来的视频信号、麦克风录制的通话记录，甚至用户的奔跑节奏、心跳和血压等。不仅如此，根据物联网行业的构想，未来，通过中央服务器转发的信号还可以控制家庭门窗、电灯和空调等设备的开启，甚至远程控制医疗检测等。当万物互联时，节点越多，网络中的薄弱环节就越容易被黑客利用，安全隐患就越多。

为了能让大家有一个更直观的认识，我们不妨用一些案例来说明：

在万物互联网的状态下，一个家庭会有自己的家庭网络，在这个网络内，所有的物品，包括门窗、空调、锁、桌椅、衣柜等，都可以接收网络信号，并且由一个中心化的服务器来控制。那么，不法分子可以通过攻击家庭网络设备中的某些薄弱环节来侵入家用网络，进而侵入计算机来盗取个人数据。想一下，假如有黑客入侵了你的冰箱，获得了你的日程安排表，以及工作、亲友等相关信息，然后入侵网络云盗取你和家人的照片，甚至还能打开你家的门窗，这将是一件多么可怕的事。

在物联网系统中，就算你拥有最好的加密技术、最好的防火墙，也不能说你的系统是100%安全的。因为总是存在比你更聪明的人破解这些加密技术的可能性。另一大问题是用户，并不是每个人都精通技术，也不是所有人都懂得经常更换密码的重要性，由于接入物联网系统的设备太多，用户总有疏忽的时候。非技术型用户就是系统中的弱点，这也会成为黑客的切入点。

另一挑战就是当有很多节点时，就会存在兼容性问题，这也会成为黑客可以入侵的漏洞。

由于网络里的节点多，一旦遭受攻击，要查出问题节点都是很大的难题。以前对于中心化的数据库来说，由于网络里的节点较少，因此中心能够很容易找到出问题的节点。而物联网由于链接万物，对于一个数以亿计的网络而言，这是很大的工程量，几乎不可能不出错。

同时，用户隐私问题也是很大的挑战。

政府安全部门可以通过未经授权的方式对存储在中央服务器中的数据内容进行审查，而运营商也很有可能出于商业利益的考虑将用户的隐私数据出售给商业机构进行变现。在互联网环境下，这些问题都已经出现端倪。在互联网环境下，由于虚拟和现实的界限很明显，用户暴露在互联网上的隐私可能还不是很彻底，一些重要的隐私可能存在于线下，互联网无法捕捉和泄露。而一旦在物联网环境下，由于万物都互相连接了，虚拟和现实的界限将越来越模糊，人们大量的信息、数据（包括隐私）都将记录在互联网上，一旦被泄露，那将是十分可怕的。因此，人们对隐私安全的忧虑也会影响物联网的发展。

区块链的解决方案

物联网的安全隐患，其核心就在于它的中心化。所有的设备都要依赖中心化的服务器来传送数据，都需要和物联网中心的数据进行核对，一旦中心数据库崩塌，会对整个物联网造成很大的破坏。为什么说区块链能够为物联网提供安全保障呢？

首先，区块链可以有效地狙击一些黑客攻击。

黑客是怎么样攻击的呢？在传统的互联网网络里，黑客只要攻击中心化的总服务器成功就可以实现入侵，就好比是办公大楼外的警卫，在人员进入大楼之前会先检查ID，一旦警卫作弊，可以很轻松地进入。当下物联网中所采用的，也是这种中心化的系统，所以存在黑客入侵的安全隐患。

而在使用区块链的情况下，由于是一个点对点的系统，不存在中心化的服务器，所有节点都是平等的，因此就算成功地攻击任何一个节点，都无法入侵整个网络，除非达到51%以上的攻击。类似于进入一栋大楼时，不需要警卫站在楼外，而是需要楼内大部分用户对该人员的身份进行确认，确认无误后该人员方能进入大楼。这种方式显然更加安全，在这种情况下，收买任何一个人，都无法达成进入大楼的目的。

其次，就算有黑客搞破坏，由于区块链分布式的网络结构提供一种机制，使得设备（节点）之间可以达成共识，无须与中心进行验证，即使一个或多个节点被攻破，整体网络体系的数据依然是可靠、安全的。例如，即使黑客侵入了家庭网络中的冰箱，他也只能得到与冰箱相连的那个节点的相关信息，无法得到整个家庭网络中的全部信息，因此带来的破坏性不会太大。

再次，区块链便于溯源。因此，即使某个节点遭到攻击和破坏，通过区块链系统可以很快找到此处问题的节点，并能够及时处理。这既提升了维护的效率，也节省了成本，还可以最大限度地减少损失。

最后，区块链的匿名性，可以有效地保障物联网生态系统内的用户隐私。

总之，区块链在物联网安全这一环节大有可为，很多企业和机构也开始注意到这一点。2017年9月，Bosch、纽约梅隆银行、思科等多家企业与机构建立信任物联网联盟，此外还将设立开源区块链协议的标准，来加强物联网安全性。

区块链在人工智能领域的应用

区块链可以在人工智能的安全性方面发挥作用，通过区块链的方案，可以在一个分布式的物联网建立信用机制，利用区块链的记录来监控、管理智能设备，同时利用智能合约来规范智能设备的行为。可以说，人工智能可以解决机器人有多大能力的问题，而区块链解决有多大责任的问题。同时，将区块链和人工智能相结合，也可以大大拓展人工智能领域的广度和深度。

区块链解决人工智能的信任问题，且可以降低成本

如同区块链可以降低物联网的运营成本，在物联网系统内建立信任一样，区块链和人工智能的结合，也能发挥类似的相关作用。

人工智能也依赖数据，所以数据的来源、质量、隐私都是急需解决的问题。区块链可以保障数据的准确度，亦可以确定数据的归属权，同时还能保障数据的隐私。通过智能合约，可以将数据的提供方和使用方隔离来实现隐私保护。当训练数据时不知道数据在什么位置，也无法将这些数据转卖给别人，且训练模型也是去中心化的，并非在自己的服务器上训练，最后只能看到训练出来的数据模型。

通过区块链，可以建立机器与机器之间的信任，人工智能的使用范围将会扩大。例如，未来有一天，当我们需要跟其他人交换物品时，可以让彼此的机器人代为跑腿，甚至机器人可以帮我们收快递、付款、收款等。

在算力层面，像GPU等各种各样的人工智能芯片，更新换代非常快。人工智能高性能服务器很贵，且更新换代的速度非常快，对于所有人工智能企业都是巨大的成本。而区块链中的去中心化和分布式技术能完美地解决算力方面的问题，能够让人工智能企业的成本大幅度降低。

区块链与新零售的结合

数据在新零售中的意义重大。但是对于商家来说，要获得真实的数据并不容易，区块链去中心化、可追踪、可溯源、永久无法篡改的特性，既可以保证数据的真实性，又可以保护消费者隐私。因此，区块链可以为新零售的实现插上翅膀。

在零售业中，假货泛滥和供应链腐败一直是两大难题，而区块链的数据不可篡改和可追溯性，则可以很好地解决这两大难题。

区块链为新零售插上翅膀

当前，新零售是一个非常火爆的话题。那么到底什么是新零售呢？市面上众说纷纭，但有几点是公认的：新零售是由产品中心转变为“消费者中心”，以前是先有产品再去寻找消费者，现在则是根据消费者的需求去生产产品，消费者的地位变得前所未有的重要；此外，新零售要打破线上线下的边界，让线上和线下的数据共享。

那么，在这个过程中，区块链将起到怎样的作用呢？

首先，数据在新零售中的意义重大。但是对于商家来说，要获得真实的数据并不容易，区块链去中心化、可追踪、可溯源、永久无法篡改的特性，既可以保证数据的真实性，又可以保护消费者隐私。

其次，消费者在零售行业中的地位越来越重要。如今，口碑效应甚至超过了广告。流量经济时代，要吸引消费者的注意是一件很困难的事。因此，消费者的分享、转发和推荐，有时往往比广告的效果要好得多。如何让更多的消费者愿意分享？这个话题在零售界已经探讨很多年了。然而，在消费分享领域创业成功的，寥寥无几。

事实上，商家很愿意为消费者分享付费，消费者也很愿意去分享商品获得报酬，这样两相情愿的事，为什么就是无法顺利开展呢？

其实就是一个诚信和透明度的问题。传统的技术手段下，数据无法溯源，因此，商家很难准确监测消费者分享的频率和效果，也就无法给出相应的报酬，消费者也就失去了分享的动力。

而一旦加入区块链技术，所有数据登记在链上，无法伪造、无法篡改且可以溯源，那么上述问题就迎刃而解。商家完全可以让消费者在获得高性价比消费体验的同时，还能分享消费红利，从而让“厂家、商家、消费者”真正成为利益攸关的铁三角，成为利益共同体。这必将极大地改变零售业生态，挖掘消费潜能，促进消费需求的大爆发！

再次，区块链还可以通过智能合约为零售提供诚信保障。

随着零售业的发展，线上线下的界限将会越来越模糊，越来越多的交易将在线上进行，越来越多的合同将在线上签订。这个时候，诚信和安全就是一个问题。而一旦引入智能合约，就容易得多了。同时，区块链系统由于是一个去中心化的系统，任何一个节点被破坏都不会影响到整个网络，所以还可以保证合同的安全。

2017年5月，国内最大的B2B平台阿里巴巴1688大企业采购平台与第三方电子合同平台法大大（区块链相关企业）达成合作，在1688大企业采购平台正式上线第三方电子合同服务。

引入电子合同后，1688用户能够在线签署电子合同，通过电子合同智能管理企业采购全流程，从而提升1688平台交易效率。

不仅如此，在大宗商品交易过程中，交易各方可借助电子合同立即进行交易，合同的制定、调整、签订等均可在线进行，交易效率能够得到极大提升，并且确保了交易的安全、可靠，从源头上避免了因电子协议、口头协定等法律效力低下的传统模式带来的法律风险。

最后，理想状态下，区块链可以做到一切数据记录在链上，互链互通，点链直达，高效透明，从生产到流通到仓储所有信息清晰明朗，并且可以追溯，从而有望打通整个零售环节，让用户、终端、企业、市场等全产业链都实现互信。这无疑是一个令人激动的伟大构想。

用区块链追溯产品来源，杜绝假货

曾经，百度试图介入农业，其中一个概念是通过网络直播的方式养鸡。这个概念的核心思想就是：人们其实愿意为优质产品买单，只要商家能让他们相信，那确实是优质产品。当前，很多消费者都活在一种“假冒伪劣产品”的恐慌之中，从国外代购奶粉之所以这么火爆，与当前零售领域特别是食品领域的诚信问题有关。

“百度养鸡”这个概念最终水花不大，这其中一个原因恐怕是：视频直播一只鸡的生产全过程，用这样的方式去取信于消费者，这个成本未免太高了！而且，即使采用这样的手段，也并不能让消费者完全信任。消费者依然有顾虑：我如何知道我不在线的这段时间里，鸡到底吃了什么呢？我如何知道你在打包的时候甚至是在打好包之后到底有没有调包呢？通过视频直播从鸡出生到送到消费者手里这个全过程，几乎是无法操作的。

而一旦加入了区块链，通过区块链去溯源，这个问题就变得简单了。

微软以及许多其他技术公司目前正努力研究将区块链应用于产品溯源。从理论上讲，一旦这项技术能够成熟化并且落地应用，消费者能够使用他们的智能手机来扫描特定商品，然后查看这件商品从出厂到上架销售所经历的所有历程。例如，消费者可以查看“新鲜水果”从农场采摘后到上架销售的全过程，以及它们是否曾经冷冻保藏过。再例如，利用区块链技术，可以展示一件商品（例如T恤）是在哪里、何时以及如何生产并运输到你面前的。

当前，有机蔬菜、散养鸡、无饲料养猪等概念都有人炒作，事实上很多消费者也愿意为了优质产品付出合理的价值，但是涉足这些领域的商家却无法获取消费者的信赖。而这正是区块链技术发挥作用的地方。

区块链作为一种分布式账本，让伪造变得非常困难。从供应商、制造商到运货商，为每一个产品清单来源添加可验证记录，区块链给供应链中这些操作的合法性提供了可能。

在奢侈品领域，区块链溯源的意义就更为重大。它将会让爱马仕、LV等名牌的以假乱真变得困难，同时也让原产地标注和 product 安全追踪变得更容易。

不仅如此，区块链还可以改变整个二手交易市场。

人们在交易二手物品时，最担心的就是诚信问题：电脑、手机是否是原装的？车子的重要配件有没有被动过？衣服、包包是不是真的名牌？这些都是人们在交易二手物品时所顾虑的问题。一旦区块链技术让这些难题得到解决，可想而知将带来二手交易市场的空前繁荣，同时也将促成“良币驱逐劣币”的健康发展局面。

区块链在人力资源领域的应用

近几年来，“组织扁平化”和“合伙人制度”是人力资源发展的一大趋势。“组织扁平化”和“小组工作制”实际上就是通过“多中心化”来替代过去的“层级制”，从而提升人力资源管理的效率，这和区块链的“去中心化”不谋而合。不仅如此，区块链与人力资源结合，还能起到节省人力、打击履历造假、提升招聘效率等多方面的作用。

因此，虽然区块链在人力资源领域的应用是近一两年才走进大众视野的，成熟的案例不多，但却被业界非常看好，未来这一领域的应用拥有十分广阔的发展空间。

区块链+人力资源拥有无限发展空间

区块链+人力资源的应用是近一两年才走进大众视野的，虽然对于这一领域的应用还没有达到白热化的程度，但是，区块链可以与人力资源结合的点非常多。未来这一领域的应用将拥有无限潜力。

区块链的去中心化与人力资源发展趋势不谋而合

区块链的一个核心特点就是它的去中心化。恰好，这也是未来人力资源发展的一大趋势。

过去，企业组织结构一直都是层级式的，呈现集权式的特点。往往是最顶端有一个总经理，下面有区域总经理、总监、各部门经理、主管、基层员工等。这样的组织结构不仅决策效率很低（需要一层一层审批），还容易形成官僚化作风乃至腐败，打压基层员工的积极性。

所以，近几年来，“组织扁平化”和“合伙人制度”是人力资源发展的一大趋势，当前比较热门的公司，例如小米、华为、万科等都在提倡这种模式。这种模式本质上就是部分去中心化——中心的作用在减弱，围绕在中心周围的小团队的话语权在加强。

但是这种模式实施起来并不是那么容易的，去中心化一旦操作不好，就容易乱。没有了中心的协调，团队之间如何达成信息透明化，如何达成高效沟通和友好协作？

我们会发现，由于区块链是点对点之间的通信，且具有数据透明化，所有节点都可以共享，因此在人力资源组织变革这一领域大有可为。

具体说来，区块链+人力资源还可以运用于以下这些领域。

节省一些人力

随着科技进步，未来智能设备通过物联网能帮助用户自动化处理一些日常工作，缺少某些日常用品时能自动收集信息并购买。通过区块链技术，可以在分布式物联网上建立信用监督机制。利用区块链的交易信息记录来查看智能设备是否工作，也可利用智能合约来约束智能设备的行为，这样就可以节省很多人力。

彻底打击学历履历造假

无论哪个行业、哪个领域的招聘，不确定性最大的就是候选人的资历真实性，这项流程耗费的时间和成本也很大。因此现实中，大多用人单位选择不去审核证书及履历。如果将所有信息保存在区块链里，候选人可以授权信息访问，就可以避免繁杂的流程，达到更精确的核对效果。

学习机器技术（Learning Machine Technologies）和麻省理工学院媒体实验室联合开发了Blockcerts钱包App，Blockcerts钱包App让毕业生轻松访问可验证的防篡改的毕业证，并与潜在的雇主共享。

麻省理工学院已经进行了首次测试，2017年夏天试点项目中的111个毕业生已经通过区块链系统获得证书。未来，即使服务

供应商不存在了，麻省理工颁发的正式学业成绩格式也可以永久保存。

澳大利亚墨尔本大学也正在测试一种基于移动设备的系统，用于在区块链上发布和维护所有者的学历证书。而这些工具基于 Learning Machine Technologies 和麻省理工学院媒体实验室共同开发的 Blockcerts 区块链证书开放标准。通过将凭据数据存储在区块链上，在特定的时间点上，该信息将被关联到某个事务节点上，来降低证书造假风险。

企业流程再造

企业在交易过程中，交易方都希望透明简化交易过程，尤其是采购方希望节约交易成本，想要设立一个自动化交易过程，比如全款支付、支付部分金额、补贴、罚款等，但是在交易过程中多方会参与进来，例如银行等金融机构、采购方、物流公司、供应方等，这就需要对整个交易供货流程有完整记录。

而区块链技术能实现透明公开的交易，会把整个交易信息都记录在总账本上，交易涉及者都能够监管记账，提高交易效率，降低交易风险。

改造招聘

除了证书造假，背景调查也是一项让招聘者头疼的事情。

很多小型公司依赖于和候选人指定介绍人的几通电话或者电邮，其限制性很明显。大型公司有时会直接或通过第三方进行更多背景调查。

确认候选人背景的可信度需要接触多个不同的信息源，特别是候选人曾经的雇用时间及地点。现在任何人都可以随便说在哪里工作过。

而一旦有了区块链，了解候选人背景就很容易了，因为区块链可以溯源。

当然也有合理的担忧，尤其是隐私性。相关信息本质上是私人的，在很多国家受到严格监管，然而只要个人许可，还是可以安全地在区块链上发布信息，让个人只与自己授权的对象分享信息。

区块链在广告及传播领域的应用

移动互联网时代，社交化媒体出现，人人都可以制造信息，也可以传播信息，人类社会进入自媒体时代。这在给社会化传播和人类生活带来诸多便利的同时，也带来了监管上的难题，造假侵权现象屡屡发生。区块链与传媒的结合可以很好地解决这些问题。

在数字广告领域，透明度的缺乏正在危害该行业。而区块链的公开性和可追溯性让“水军”无所遁形，造假变得困难，让数字广告业更加良性地发展。

区块链公司正在试图颠覆全球内容传播乱象

事实上，互联网的出现，已经对传播领域进行了一次颠覆。在互联网出现之前，即大众传媒时代，信息传播是中心化的，信息源往往掌握在少量媒体手中，大众无法制造信息，也无法传播信息，只能被动地接收信息。

互联网的出现彻底颠覆了这一格局，移动互联网时代，社交化媒体的出现，导致人人都可以制造信息，也可以传播信息，人类社会进入自媒体时代。

那么，如果在传播领域再加上区块链呢？将会给传播领域带来怎样的改变？

“版权为王”，内容制造者将得到尊重

在互联网时代，由于信息复制粘贴的成本实在是太低了，因此侵权现象十分严重。在这种情况下，内容制作者往往处于产业链的最底端，其权益得不到保障。大部分利益被那些大型平台、网络推手等获取。

而一旦引入了区块链技术，则可以通过不可篡改的数字签名、可信时间戳，很便捷地为原创新闻作品提供者确权，并提供跨平台的版权交易和数据增值服务。

由于区块链上的信息可以追溯，可以利用区块链构建一个更完备的侵权监测系统、证据保全系统，最大限度地识别侵权行为。由于区块链的高效，可以让新闻同时在多个平台发布，并大大降低版权使用的费用；在区块链上，还可以建立版权自助交易平台，让作者们最大限度地享受到作品的版权收益；可以实现打赏去中心化，还可以跨境支付。

去中心化，减少平台操控

虽然新闻领域的去中心化目前受到政策法律的影响，实现起来比较困难，但却有着诱人的前景，例如：

在区块链网络里，可以在全球范围内建立虚拟编辑部，实现跨区域的信息传递，信息传播更全面、更及时。

区块链的身份验证功能，让每个人都可以在链上制造并传播信息，一旦被采纳可获得报酬，从而大大降低新闻线索搜寻成本和新闻采编成本。这比任何爆料都更及时、更可靠，因为必须是被链所验证了的信息才可以获得报酬，为了利益人们不会轻易造假，因此可靠性大大提升。同时，区块链的匿名性还保护了用户隐私，人们的参与度更高。

媒体传播的各个环节都可以搬上区块链网络，打通媒体全环节，提升各区域、各部门的合作，大大提升效率。

给媒体提供信用保障

网络自媒体虽然给人们提供了大量的信息，但其中虚假的信息也特别多，耗费了人们大量的甄别时间，也降低了媒体信息的信用度。

将区块链技术运用于传播领域，可以给媒体提供信用保障。

例如，网站、论坛、博客、微博、微信公众号、即时通信工具、网络直播、各类应用App的出现，让所有普通大众都具备了制造信息和传播信息的能力，也带来了一系列管控难题。

运用区块链技术，可以给每一个合法的自媒体注册唯一的数字身份，通过区块链网络记录该数字身份的所有信息。这样的方式，既保障了安全，也保护了隐私，因为在区块链上信息虽然是公开的，但身份却是匿名的。

还可以邀请区块链网络上所有用户参与评分，通过一定的算法对各种媒体的信用度进行管理，并向全网公布，提高其违规成本，让大家自我约束。

甚至还可以通过智能化合约或者区块链网络内的民主投票，使信任度低的自媒体账号直接关停。

促进传播生态系统的形成

借助区块链技术，区块链网络内的所有信息和交易都可以做到不可篡改，可追溯，且信息都是公开的，任何一方想要了解另

一方的信用信息都很容易，想要评估其产品和服务的质量也很容易。这使得花钱删除负面评价、请“水军”刷好评、抹黑竞争对手等操作难以实施，因此可以帮助打造一个更良性的传播生态系统。

信用的建立，也可以大大提升媒体和传播平台的价值，平台可以借助区块链技术打造一批区块链应用场景，培育一批区块链创新企业，形成一批可推广的商业模式，使媒体自身成为资源聚集的平台、服务增值的平台，玩转生态。

应用实例：第一个基于区块链技术的“广告链”

区块链在广告业的应用目前还处于初步尝试阶段，相关落地案例还很少，不过2017年已经有公司在尝试了。

位于洛杉矶的广告科技初创公司MetaX已经推出了声称是第一个旨在协调数字广告供应链的区块链协议，被称为AdChain（广告链），其目的是消除欺诈，提升透明度，提高效率，从而为广告生态系统带来重大收益。

该协议是第一个能允许广告供应链中的参与者在无欺诈和无恶意软件的生态系统中进行合作的区块链解决方案。该平台还提供完整的透明度，允许品牌和广告的购买商访问与广告影响相关的所有数据。同时，广告商还会得到包括媒体和参与者详细广告审核跟踪的数据。

AdChain（广告链）还存储了如印象、点击率和受众细分等信息，广告分销商可以在广告交易平台中找到目标受众群体，并访问来自数千家发布商的广告资源。

目前，AdChain（广告链）正在与一些合作伙伴进行私密的试水测试，MetaX公司希望该项目是具有公益性的，通过基金会运营并鼓励更多的公司使用它。

区块链将构建全新的社会信用体系，打造契约社会

前面我们讲述了区块链在商业社会中的种种应用。但是，未来区块链的影响可能不仅仅局限于商业领域，而会拓展到整个社会。可以说，哪里有信任问题，哪里就有区块链的用武之地。

可以毫不夸张地说，数学（算法）是全球文明的最大公约数，也是全球人类获得最多共识的基础。如果我们以数学算法（程序）作为背书，所有的规则都建立在一个公开透明的数学算法（程序）之上，就能够让所有不同政治文化背景的人群获得共识。^[1]

关于区块链，最激动人心的构想，是利用这一技术来打造社会信用体系。按照理想化的预测，人类有机会利用区块链打造契约社会。

构建社会信用体系

区块链可尝试以城市为试点建立信用信息共享平台，逐步提高信用信息的公开和应用水平，从而构建守信者受益、失信者受限的全新社会信用体系。

通过失信“黑名单”归集、信用监测数据定期公布等，构建一个公开透明、不可篡改的社会信用统一数据库。

推出信用云、媒体公信指数、智能合约平台等，大大降低企业、个人、非企业法人（政府机关、事业单位、社会团体等）等之间的交易信任成本。

推进媒体信用监督体系建设，推出信用数据流转监控、信用评估、信用保险、信用管理咨询等服务。

区块链将影响法律体系

未来，区块链可能会像现在的互联网一样，在社会的方方面面得以大规模应用，关于区块链的基本知识会成为我们这个社会的生活常识。

法院可能要处理大量的“区块链世界”里面的纠纷，同时区块链作为工具和应用从很多环节改变了现有的法律体系和流程，区块链的不可逆、无法篡改、可追溯性，都有可能被应用在法律领域，先进的时间戳可以实现新的公证方式。

智能合约可以用于仲裁，甚至大量简单的合同和协议不需要仲裁，可以完全基于机器的自动化履约和兑现，由机器强制执行、透明公开，这将减少很多纠纷。利用区块链技术，在部分层面可以实现智能“法制”，不需要人为干预，或者干脆无法干预（例如，智能合约到了约定的时间就自动执行）。

[1] 梅兰妮·斯万. 区块链：新经济蓝图及导读[M]. 北京：新星出版社，2015.

区块链在政府层面的应用实例

微软为政府提供区块链应用，保障机密数据的安全

科技巨头微软2017年10月17日于华盛顿特区召开了“政府云论坛2017大会”，宣布将推出“Azure政府机密”（Azure Government Secret）服务，旨在使政府机构能够更好地访问云计算。除了提供这种新服务，微软还将打开区块链供应的大门，使其当前的“政府云”客户能够访问微软Azure区块链即服务（BaaS）产品。

BaaS于2015年推出，用来帮助私人公司试验区块链工具，目前处在一个沙盒环境中，拥有Chain, ConsenSys和Emercoin等合作伙伴提供的技术服务。虽然微软云服务的私人部门用户近年来都可以使用这些工具，但美国政府严格的安全要求阻碍了这些机构对此类产品的利用。

具体来说，微软有6个数据中心目前已被“隔离”，并获得美国国防部5级临时授权。此外，还有联邦风险和授权管理计划（FedRAMP）和国防信息系统局（DISA）等组织的一系列认证。

据微软Azure首席技术官Mark Russinovich介绍：“美国政府要求这些数据设施经过认证后由美国公民进行操作，所以我们的承包商要符合这种要求。”

鉴于这些因素，“Azure政府机密”服务将为使用“机密数据”的客户提供高级分析和更高级的“检测”功能。

Russinovich认为这个项目是政府利用区块链优势的新途径，也能使政府对纳税人负责。

美国犹他州运用区块链进行总统候选人投票

犹他州领先使用区块链技术，选出参加美国总统选举的共和党候选人。犹他州投票人不需要到投票站去投票，而是可以直接坐在家或任何地方的电脑前参与网络投票。

这个投票系统由Smartmatic设计，简单方便。参与投票者，只需要访问犹他州共和党网站并注册。一旦确认身份，就会获得一个密钥。这个密钥就是投票者所持选票。网上投票需要投票者输入这个独特的密钥。

在确认提交之前，可以无数次更改投票。但是一旦提交，选票就不可撤回了。

贵阳市运用区块链推动社会诚信体系建设

2017年，“数聚诚信·上链贵阳”暨区块链底层技术系列发布会在贵阳综合保税区举行，贵阳市政府希望进一步推动以智能合约、跨链技术等为代表的区块链核心技术发展，推动社会诚信体系建设，加快区块链技术应用落地。

据了解，区块链技术支撑下的政府治理，将使老百姓实实在在地感受到政府福利发送、救助行为的透明和精准，政府各项政务处理的便捷和高效，自身权益维护的公平和公开。同时，政府通过线上线下的身份统一管理，能实现对辖区“人财物事”状态及流动的及时跟踪、分析、预警、引导。

贵阳市委书记表示，贵阳市当前正在尝试利用区块链等新技术，在可信数据生态环境下，把诚信体系建设这一道德问题逐步变成数学问题。

美国政府运用区块链打造透明数据平台

美国监管机构和政府机构从2015年开始就关注区块链技术，来创建一个用于各行业的可靠和透明的数据处理平台。美国卫生与公共事业部（HHS）是第一个计划部署区块链来确保医疗健康记录安全的政府机构。

洪都拉斯运用区块链技术进行房产登记

成立于2014年的Factom公司一直将“构建诚实的世界系统”作为发展使命，该公司2015年与洪都拉斯政府合作，试图在该国缺乏互信的市场环境下建立以区块链为基础的房地产信息系统。

爱沙尼亚政府在区块链的应用上已经处于世界领先水平

这个位于波罗的海边的数字化小国拥有接近100%的电子银行交易率和30%的互联网选举投票率。该国早在2007年受到网络攻击后，就开始发

展基于区块链的“无密码签名设施”（keyless signature infrastructure, KSI）管理政府和公民信息。得益于该系统，爱沙尼亚的每个公民都可以独立检查政府记录的完整性，有效监督政府行为。而政府内部的特权人员却无法清除系统上的电子日志，从而避免了公职人员的犯罪行为。同时，事实证明该技术极大地增强了该国信息系统的安全性，这点非常值得他国借鉴。

瑞典当局运用区块链技术进行土地登记

作为最早流行比特币的国家之一，瑞典当局已决定于2017年3月开始试使用区块链技术登记国家土地信息。依靠强大的技术团队和成熟的信息管理体制，该国很可能是第一个完善区块链土地登记系统的国家。

澳大利亚政府出资支持区块链研究

澳大利亚政府已经宣布将提供超过800万澳元（约600万美元）作为对一个基于区块链的智能公共事业项目的补助。

这个项目旨在探索城市如何能够使用区块链技术和数据分析来推动分布式能源和水力系统。澳大利亚科廷大学将负责监督项目管理并执行支持这个试验的研究。我们将开发一种智能测量、电池存储和区块链交易系统，为那些重要但地理位置分散的基础设施带来能源和水力高效性。

除此之外，区块链还有很多政府应用的案例，例如：

- 位于马里兰州的BitHealth公司尝试用区块链技术构建全球统一的健康信息系统。
- 英国政府在国民健康保险制度（NHS）中应用区块链技术，用虚拟的算法去解决现实的问题。
- 迪拜把土地登记100%转移到区块链上。

传统货币与数字货币

货币发展到今天，其使用价值早已不再重要，它更多的是一种信用的凭证和记账的符号。从这个意义上讲，数字货币是完全可以成为货币的。

与传统货币相比，数字货币在降低成本、支付便捷、反洗钱等领域都有着无可比拟的优势，我国央行已经将发行数字货币提上了议程。不过，当前数字货币的发展还很不成熟，数字货币想要成为主流货币还有一个漫长的过程。

数字货币的发展回顾及现状

对数字货币的构想，其实在20世纪已经出现。

1982年，David Chaum最早提出了不可追踪的密码学网络支付系统。1990年，Chaum将他的想法扩展为最初的密码学匿名现金系统。这个系统就是后来所谓的ecash。

1998年，Wei Dai发表文章阐述了一种匿名的、分布式的电子现金系统，他将其命名为“b-money”。同一时期，Nick Szabo发明了“Bit gold”。和比特币一样，“Bit gold”也设置了类似的机制，用户通过竞争性地解决“工作量证明问题”，然后将解答的结果用加密算法串联在一起公开发布，构建出一个产权认证系统。“Bit gold”的一个变种是“可重复利用的工作量证明”，开发者是Hal Finney。

然而，直到2009年比特币出现，数字货币才真正进入蓬勃发展的时期，当前，数字货币市场呈现一派繁华景象。我们可以看一些具体的数据：

2017年4月，剑桥替代金融中心（CCAF）发布了全球首份数字加密货币报告，其中涉及数字加密货币的使用以及支撑这种新货币发展的新兴货币系统等多方面内容。正如报告所说：“货币和金融世界正在我们眼前发生着改变。”

这份名为《全球数字加密货币基准研究》的报告是CCAF首个关于替代支付系统及数字资产的研究。该研究通过安全的网页问卷调查，收集了全球38个国家100多家数字加密货币公司的数据。CCAF称调查覆盖了加密货币业约75%的数据。30多名数字加密货币挖掘工也接受了调查。调查主要针对四大关键领域：交易、钱包、挖掘、支付。这份调查显示：

- (1) 交易领域拥有运营实体最多，员工也最多，有很强的地理分散特性。如今大约有52%的小型交易企业有正式政府执

照，而大型交易企业仅有35%拥有执照。CCAF在报告中称，中国人民银行近期的举措可能很快改变这一现状。

(2) 现在有580万到1150万的数字加密货币钱包可视为“活跃”钱包。如果平均每个人有两个钱包，就意味着数字加密货币有290万到580万个人活跃用户。近52%的钱包提供综合货币交易功能。

(3) 79%的数字加密货币支付公司都与银行及支付网络有合作关系，支付公司交易总量中法定货币到加密货币的支付占三分之二，法定货币到法定货币占27%，加密货币到加密货币占6%。

(4) 有名的加密货币挖掘机构具有地理集中性，中国某些省份这种集中性更加显著。大型加密货币矿池中约75%分布在中国和美国。^[1]

事实上，截至2017年年底，数字货币统计网站coinmark-etcap.com公布的数字货币多达1372种，市场价值超过6000亿美元，其中，比特币价值最大，为2700亿美元左右。数字货币种类间的市值差异非常大，比特币的市场价值占数字货币总额的81%左右，97%的非主流数字货币只占总市值的1.3%左右。^[2]数字货币间的排名变化也很大，新的数字货币不断出现。

几乎所有的数字货币，其市值波动都非常大。

[1] www.zhongbangshujuwang.com.

[2] <https://coinmarketcap.com/>.

比特币

比特币是区块链的第一个应用，它是最早的数字货币，到今天为止，它仍然是单价最高、市值最高的数字货币。从2009年比特币网络正式上线，到现在发展已经将近10个年头，在不到短短10年的时间里，它的价值翻了1万倍都不止。不过，到目前为止，比特币的市值依然不稳定，仍然处于大起大落的状态。

由于比特币系统是一个完全自治的系统，在比特币的扩容问题上，技术团队和矿工之间的意见有些分歧，由此造成了比特币的硬分叉现象。这是众多比特币的参与者比较忧虑的一个问题。从长远来看，硬分叉会造成怎样的结果还不明朗，业界预测了多种可能性。

比特币的发展历程

2009年：比特币网络正式上线

2009年1月，首个比特币开源客户端和首批比特币发布，比特币网络正式上线。中本聪通过挖矿的方式，获得50个比特币。

2009年10月，首个比特币汇率公布，1美元兑换1309.03个比特币。

2010年：首次公开交易

2010年5月，佛罗里达州程序员完成首个比特币真实交易，花费10000个比特币买了两张比萨。后来面对高昂价格的比特币，Laszlo Hanyecz说：“我没感到特别沮丧，比萨真的很好吃。”

2010年7月11日，比特币新版客户端消息被著名新闻网站Slashdot提及，为比特币带来大量新用户。

2010年7月16日，经过为期5天的10倍暴涨，比特币价格从0.008美元升值0.08美元，这是比特币的第一次价格剧烈波动。

2010年7月，成立MT.GOX。这是世界上最知名的比特币交易平台。

2010年8月，比特币协议暴露缺陷，这是比特币历史上唯一被发现的重大缺陷。用户可以绕过比特币的经济限制，创造无限量的比特币。

2010年11月6日，MT.GOX上的价格达到0.5美元，此时比特币经济达100万美元。

2011年：上半年大涨，下半年大跌

2011年1月27日，最大数字的比特币交易产生：三个来自津巴布韦的账单在Bitcion-otc上以每4个比特币换100万亿津元。

2011年2月9日，价格首次达1美元，与美元等价。BTC与美元等价的消息被媒体大肆报道后引起人们的高度关注，新用户大增。此后2个月内，比特币与英镑、巴西币、波兰币的互兑交易平台先后开始营业。

2011年3月6日，全网计算速度达900ghash/sec，但很快又下跌了40%，显卡挖矿开始流行。

2011年6月，比特币市场价值达到2.06亿美元。

2011年6月8日，继6月2日汇价迈过10美元后，MT.Gox上的成交价格高达31.91美元。

2011年6月19日，MT.Gox上6000份用户信息遭到泄露，导致比特币价格从17.51美元跌至0.01美元，此后半年一蹶不振。

2012年：经历一年平缓发展期

2012年3月1日，服务器超级管理密码泄漏，价值228845美元的46703比特币失窃，黑客是比特币世界挥之不去的噩梦。

2012年9月15日，伦敦比特币会议召开，此时比特币价格为11.8美元。

2012年11月25日，欧洲第一次比特币会议在捷克布拉格召开，此时比特币价格为12.6美元。

2012年11月28日，区块供应量首次减半调整，从之前每10分钟50个递减至25个，同时比特币发行量占发行总量2100万的一半，此时比特币价格为12.4美元。

2012年12月6日，首家在欧盟法律框架下进行运作的比特币交易所——法国比特币中央交易所诞生，这是世界首家官方认可的比特币交易所，此时比特币价格为13.69美元。

2013年：发展前景良好

2013年2月28日，比特币价格在601天之后，超越2011年6月8日的历史最高点31.91美元。

2013年4月10日，比特币创下历史最高价，266美元。

2013年5月3日，中国央视《经济半小时》比较客观地向中国观众第一次介绍比特币这个新生事物，此时比特币价格为92美元。

2013年5月9日，比特币公司Coinbase获得了投资基金Union Square的500万美元A轮融资，此时比特币价格为112.09美元。

2013年7月7日，以中国为代表的矿机产业链日益成熟，比特币股票分红令人垂涎。随着越来越多的人士介入挖矿行业，挖

矿难度与日俱增。

2013年10月，世界首个比特币ATM机在加拿大温哥华问世。

2013年11月，美联储主席伯南克表示他们没有权利监督虚拟货币，并认为，如果这项创新能够给人类带来安全、快速和高效的支付系统，那么它具备一个长期的发展前景。

2013年，中国人民银行宣布所辖银行不接受比特币交易。

2014年：快速发展的一年

2014年1月1日，以狗狗币为代表的山寨币纷纷出现。

2014年1月，Blockchain.info钱包的用户数量已经突破100万。中国最大网购零售平台淘宝网宣布比特币禁售令。

2014年2月，俄罗斯检察长办公厅颁布法令称：俄罗斯官方货币是卢布，引入其他货币或替代品都被禁止，如公民匿名使用比特币，都涉嫌参与非法洗钱或恐怖主义融资。

2014年2月，全球最大交易平台Mt.Gox确认倒闭，85万比特币被盗一空。

2014年4月，“4.15事件”^[1]事件导致比特币大跌。

2014年7月，戴尔接受比特币支付。

2014年12月，微软接受比特币支付。

2015年

2015年3月，纳斯达克首次涉足比特币领域，这家世界第一大的证券交易所宣布与比特币初创公司Noble Markets达成合作关系。

2015年3月31日，全球首名因涉嫌比特币洗钱问题的罪犯Charlie Shrem于3月30日起开始服刑，其刑期为2年。

2015年4月8日，美国肯塔基州参议员兰德·保罗，正式宣布已接受比特币的捐款方式来角逐2016年总统大选。

2015年5月19日，纽约证券交易所（NYSE）宣布正式推出纽交所比特币指数（NYXBT），这是全球首个由证券交易所计算和发布的比特币指数。

2015年10月，欧盟法院裁定，比特币及其他虚拟货币的交易将免征增值税（VAT）。这一决定对于比特币交易群体而言，将是一次重大的胜利。

2016年：政府和大企业参与

2016年1月20日，中国人民银行数字货币研讨会在京召开，会议要求早日推出央行发行的数字货币。

2016年4月28日，骨灰级游戏迷都在著名游戏平台Steam宣布接受比特币支付。Steam上有9000多款游戏，覆盖全球237个国家和地区，用户人数超过8900万。

2016年5月，微软加入专注区块链的数字贸易商会。

2016年6月，由于投资者们广泛存在对比特币减半的利好预期，比特币迎来一波大行情。从3000元到5179元，比特币1个月涨了72%。这也使得比特币时隔3年后再上央视。

2016年6月，腾讯、华为加入金融区块链合作联盟。

2016年6月，澳大利亚政府拍卖2.5万个比特币。

2016年7月，比特币迎来新的一波减半。

2016年11月，比特币迎来历史新高。

2017年：飞速发展和经受考验的一年

2017年，国家监管入驻国内几家知名的数字货币交易所进行检查，意味着比特币及其他数字货币正式进入监管层面，不少业内人士将2017年称为“数字货币的监管元年”。

2017年9月，国内全面叫停ICO，随后又全面禁止了数字货币的交易。

但与此同时，数字货币的发展有增无减，价格继续高涨，可以说，2017年是数字货币经受考验继续前进的一年。

[1] 央行在3月中旬下发内部通知，要求银行和第三方支付机构不得服务比特币交易，现有开户限期在4月15日前清理完毕。

比特币的硬分叉现象

比特币的硬分叉现象是行内人士非常关注的一个问题，那么什么是“硬分叉”呢？

比特币分叉和硬分叉

首先我们来看看什么是比特币分叉。

比特币是一个大量网络节点共同维护的分布式账本，这些节点维护账本使用的是统一的比特币软件。如果是一个中心化的系统，例如银行的数据库，在进行软件升级时只需要在中心服务器上安装升级后的新软件即可。但是在分布式系统中进行软件升级就比较麻烦，需要在约定的时间将所有网络节点同时升级软件，如果中间有的节点没有及时升级，就有可能出现分叉。

举个例子，一个节点运行着老版本的软件，当其他节点升级后，大家继续抢夺记账权，这时候有两种情况：一是新版本的软件抢到记账权，打包成区块后广播出去，老版本的软件验证通过；二是老版本软件抢到记账权后打包成区块广播，被所有新版本软件认为区块不合法，这种情况叫软分叉。只要有超过50%的节点升级到新版本，就不会出现软分叉，只会造成运行老版本的节点拿不到奖励，逼着老版本尽快升级。

另一种情况比较严重，就是如果新版本的软件抢到记账权，打包成区块后广播出去，被老版本认为不合法，这就变成硬分叉了，会产生两条区块链。

硬分叉的原因

通常来说，不到万不得已，比特币软件升级会尽量使用软分叉升级的方式，避免分裂成两条链的风险。但是在2017年，比特币就已经发生了两次硬分叉，这其中的原因是什么呢？其实一句话概括，就是在扩容方案上，比特币技术团队和矿工之间发生

了意见分歧。

目前比特币每个区块容量上限为1MB，由于每笔交易都会占用区块容量，理想情况下处理速度是约7笔交易/秒，实际情况中处理速度更低。现在每个区块基本都接近1MB，达到了区容量上限。比特币网络中有大量交易不能马上被记账，产生了交易延迟。由于提高交易费用能让自己的交易被尽快打包，用户转账的手续费越来越高。

这种情况制约了比特币的推广和发展，于是比特币社区内部提出了很多备选解决方案进行投票。

那么，中本聪在最初设计比特币时是怎么想的呢？在初始设计框架里区块大小最大可以达到32MB，但是考虑到在比特币诞生早期币价很低，有人恶意制造的大量小额转账导致正常的转账不能被确认，影响网络正常运转，于是中本聪将比特币的区块大小暂定为1MB。在比特币白皮书第7章，中本聪就明确提出了未来容量不够用的时候应该怎样进行扩容，他当初的思路是直接增加区块大小。

2011年Gavin Andresen被中本聪指定为比特币的首席开发者，他吸纳了多名技术人员加入开发者团队，逐渐形成了比特币核心技术团队，我们现在称这个团队为Bitcoin Core。2015年年初，Gavin Andresen提出将比特币区块一次性扩容至20MB，但这个提案被Bitcoin Core的其他成员拒绝了。2015年年底，Gavin Andresen联合开发者Mike Hearn提出了将区块增大至8MB的方案，又被Bitcoin Core的其他成员拒绝了。2016年年初，Gavin Andresen被取消了比特币维护权，Mike Hearn也退出了比特币社区。

Bitcoin Core团队反对直接增大区块容量，他们的想法是比特币主链容量不变，还是1MB，但是开启“隔离见证+闪电网络”。这种技术用一个形象的比喻就是：公路太窄造成交通拥堵了，但是不对公路进行翻修扩建，而是在公路边上新建一条公路，专门供小车使用，主路只让大货车通行。这条新公路就是闪电网络，新公路上跑的小车就是小额高频交易，主路上跑的大货车是大额交易。关于闪电网络，后面我们还会详细讲到。

隔离见证是什么呢？

区块链上有两种信息，一种是交易信息，另一种是见证信息，原来的区块链网络必须把交易信息跟见证信息绑定在一个区块里，占用区块容量大。现在把见证信息单独拿出来打包，不但能实现更多复杂的金融功能，而且可以在不增大区块容量的基础上提升约70%的扩容效果。

Bitcoin Core虽然想在不增大区块容量的前提下开始“隔离见证+闪电网络”，但是却受到很多矿工的反对，大部分矿工主张直接扩大区块，或者在部署闪电网络的同时扩大区块。

比特币社区是民主和去中心化的，为了不同的升级方案吵了好几年也没能统一意见。到了2016年2月，Bitcoin Core团队的几位开发者、主要的几大矿场主、比特币周边产业公司等在我国香港召开会议。在会议上双方各退了一步，把两个方案结合起来达成共识，在部署隔离见证和闪电网络的同时把比特币主链区块大小从1MB增大到2MB，由Bitcoin Core主导开发，称为香港共识。

可是Bitcoin Core的几位开发者在共识上签完字回去之后，团队里的其他成员不认同这个方案，拒绝开发。经过这次事件，大矿场主们与Bitcoin Core的关系陷入冰点。

由于比特币社区多年来对于扩容升级没能达成一致意见，社区中出现了一个新的开发团队Bitcoin Unlimited，其研发的方向是无区块容量上限的升级方案，并获得了矿工的支持。

也就是说，比特币网络里分成了两派——支持大区块的，支持闪电网络+隔离见证的。支持大区块的大多是矿工，支持闪电网络+隔离见证的是Bitcoin Core（比特币核心技术团队）。

硬分叉的发生

这种分歧最终导致了硬分叉的发生。2017年8月1日，在比特大陆的推动下，比特币发生了一次硬分叉，产生了名为Bitcoin Cash的新数字货币，这一举动打开了潘多拉的魔盒。比特币是一个分布式公开账本，所有的源代码和账本明细都是公开的。理论上，只要有一定技术实力和充足的算力支持，任何人都可以基于这个账本创造一种新的分叉币。

2017年11月初，诞生了一种分叉币Bitcoin Diamond，2017年12月又出现了超级比特币、闪电比特币等多种分叉币，行业内人士甚至将12月称为“比特币分叉月”。

硬分叉究竟会给比特币带来什么，硬分叉后的链到底以谁为主，到目前还没有一个明显的定论，我们只能拭目以待。

新兴竞争币代表：超级现金

比特币和以太坊为我们打开了新世界的大门，向我们证明了区块链技术的价值和内在的潜力。随着比特币价值的水涨船高，各种数字货币层出不穷。

从2015年开始，一些非常有潜力的但并不基于区块的分布式账本系统底层技术也逐渐进入我们的视野，如DAG——有向无环图。

然而，一个最大的问题是：这几种基于完全不同系统的货币目前除了在中心化的交易所进行兑换外，并不能在这两种完全不同体系的分布式系统中自由流通。

超级现金（Hcash）就是这样一种可以实现各区块价值互联的载体。它可以连通基于区块的分布式账本和不基于区块的分布式去中心化账本系统，让所有这些去中心化的分布式账本之间的信息与价值自由流通。

超级现金的七大目标

传统的区块链，比如比特币、以太坊，还是采用基于诸如默克尔树这样的二叉树数据结构，如图3所示。

Hcash试图建立两个完全不同底层数据结构系统之间的通道，从而在底层技术层面兼容主流的区块链技术标准。这种挑战无疑是非常大的。Hcash的技术团队由深耕大数据、云计算以及密码学和区块链领域多年的技术专家组成，有信心能够克服各种障碍，实现系统的设计目标。

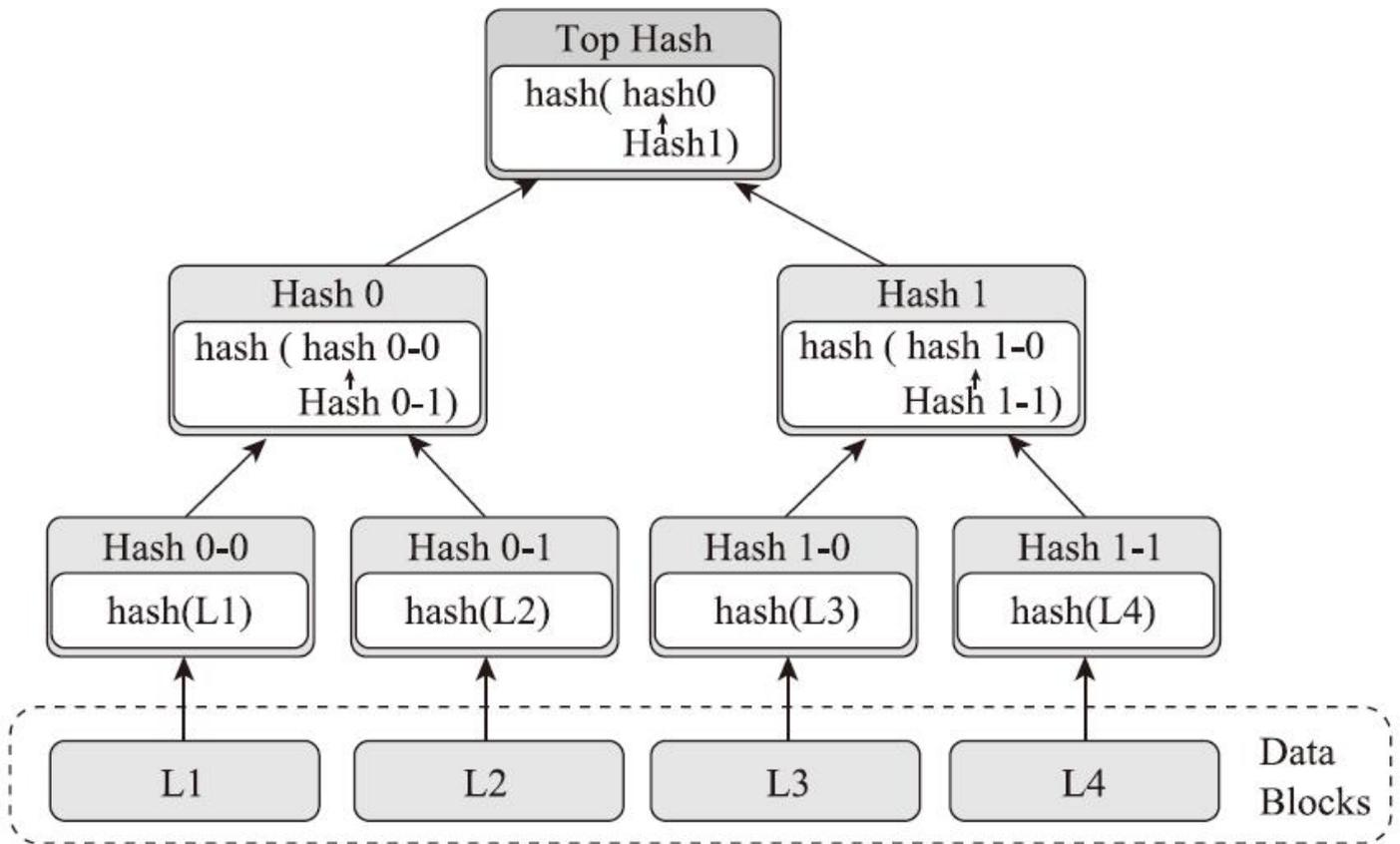


图 3

按照超级现金团队的目标和设计，研发完成后的系统将具有以下七大优势。

代表匿名，保护用户的隐私

Hcash借鉴Zcash的零知识证明技术，不单单在资产转移的过程中可以实现双向加密，还可以应用到很多其他对交易隐私要求极高的领域。

如何理解？我们先来科普下什么是“零知识证明”。

零知识证明（被称为“zk-SNARK”）是实现Zcash的匿名特性的核心技术。零知识证明的定义是：证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

举例：

A要向B证明自己拥有某个房间的钥匙，假设该房间只能用钥匙打开锁，而其他任何方法都打不开。这时有两个方法：

- ①A把钥匙出示给B，B用这把钥匙打开该房间的锁，从而证明A拥有该房间的正确钥匙。
- ②B确定该房间内有某一物体，A用自己拥有的钥匙打开该房间的门，然后把物体拿出来出示给B，从而证明自己确实拥有该房间的钥匙。

方法②属于零知识证明。好处在于在整个证明的过程中，B始终不能看到钥匙的样子，从而避免了钥匙的泄露。

A拥有B的公钥，A没有见过B，而B见过A的照片，偶然一天两人见面了，B认出了A，但A不能确定面前的人是否是B，这时B要向A证明自己是B，也有两个方法。

- ①B把自己的私钥给A，A用这个私钥对某个数据加密，然后用B的公钥解密，如果正确，则证明对方确实是B。
- ②A给出一个随机值，B用自己的私钥对其加密，然后把加密后的数据交给A，A用B的公钥解密，如果能够得到原来的随机值，则证明对方是B。

后面的方法属于零知识证明。

有一个缺口环形的长廊，出口和入口距离非常近（在目距之内），但走廊中间某处有一道只能用钥匙打开的门，A要向B证明自己拥有该门的钥匙。采用零知识证明，则B看着A从入口进入走廊，然后又从出口走出走廊，这时B没有得到任何关于这个钥匙的信息，但是完全可以证明A拥有钥匙。^[1]

简单来说：

能够在不告诉别人账户余额和交易支出的情况下，证明自己的花费少于账户的余额。

能够不记录收款方的公开账户地址，使收款方收到转账。

Hcash在客户端集成了即时通信功能，它不但能够利用暗地址实现代币的跨平台转移，也可以在日常的点对点（P2P）通信中利用零知识证明的机制实现高度的隐私通信，更能够跨越平台实现诸如从Hcash客户端到Byteball客户端的加密通信。因此，Hcash实现了从交易账户地址、交易金额到账户余额的完全隐私保护。^[2]

代表蜂巢，全面兼容

Hcash具有双重侧链，同时兼容区块链和DAG两种分布式系统，实现基于区块链和非区块链的信息与价值的互联互通。其中Hcash是跨平台价值互通的媒介，而Hcash平台本身是跨平台信息交换的载体。Hcash将会在这两个完全不同的底层数据结构系统之间搭建一个通道，从而在底层技术层面兼容主流的区块链技术标准。

基于Hcash系统的设计特点，Hcash在系统初始设计阶段已经考虑到了对基于区块链的系统（包含基于UTXO和Account Based）和DAG为基础的分布式账簿信息的读取。

与此同时，Hcash的货币体系设计也兼容Zcash的透明地址与暗地址以及Byteball的Whiteball与Blackball的地址体系。因此，在不久的将来，可以基于Hcash实现区块链与DAG系统之间直接发送或接受明（White）暗（Black）代币。同时，也能够Hcash客户端之间实现基于零知识证明的完全加密通信，以及其他一系列激动人心的特性。

代表DAO去中心化自治组织治理结构

在Hcash的系统内，有5%的代币会发送到一个DAO，由Hcash的全体持有者通过即时动态投票来决定资金的用途。DAO的生态体系为Hcash社区提供了源源不断的活力与积极向上发展的动力，同时，Hcash DAO的代码会经过严格的审核并在初期加入必要的人工干预（由基金会邀请第三方进行代码安全审核），以保障DAO在早期的资金运用过程中不出现重大失误。

为了帮助大家理解这句话，简单介绍下几个概念。

DAC

为了对DAC有一个明晰的定义，我们总结了DAC所必需的七点特征。

(1) 公开性：DAC系统的设计公开透明，公开透明性是整个DAC系统的基石。一个暗箱操作的组织不能作为DAC，现在的软件开源精神成为公开性的一个典型范例。

(2) 去中心化特性：没有中心化个人和组织能控制整个DAC，这条特性决定了自相似性，去中心化特性保证了DAC系统的生命力。

(3) 自治性：DAC系统人人可以参与，参与者都是DAC系统的子公司或者子单元，并从自身角度促进DAC的发展。参与者的自发行为保障了DAC的运行。

(4) 价值性：DAC系统必须是具有使用价值的，例如比特币系统的国际支付网络、匿名交易、避税、价值储存、不可冻结、不可监管的特性，这条特性决定了比特币DAC系统的盈利性。

(5) 盈利性：DAC的参与者会获得DAC系统发展的奖励，盈利性由DAC本身的价值性决定。

(6) 自相似性：即使在只有部分DAC节点的情况下，DAC系统仍能正常运作并发展，部分单元节点的摧毁不会影响DAC的发展，由去中心化特性保证。

(7) 民主性，DAC系统核心协议的改变需要绝大多数单元的投票才能完成，去中心化特性和自治性决定了DAC必须是一个能够民主投票的系统。

DAO

去中心化自治组织（DAO）是密码学技术革命的最理想的产物。DAO的源头可以追溯到Ori Brafman在《海星和蜘蛛》（2007年）中描述的组织去中心化，和Yochai Benkler在《网络财富》（2006年）中描述的“对等生产”（peer production）。但是这两个概念被与密码学货币相关的技术所连接起来，Dan Larimer提出了DAC的概念，他将比特币看作一个DAC。

Vitalik（以太坊创始人）将DAC概念进行扩展，提出了更为普遍的DAO概念（分布式自治组织）。不受监管的众筹和服务拆分是DAO的构成要素，还有密码学技术管理层和基于信任的自动化，这使得DAO能够运行起来。正如Stan Larimer（著名区块链公司Cryptonomex的创始人）所说，“在一组商业规则的控制下，不需要人类的参与。”

然而这种理想状态下的自治组织，如果在系统设计阶段不进行严格的把控，也会造成非常严重的后果。2016年6月，史上最大的以太坊众筹项目The DAO，这个众筹超过1.5亿美元的分布式自治组织，因为代码漏洞，遭受黑客攻击，在当时损失超过360万以太币，当时的价值超过6000万美元。其引发了ETH社区分裂，并造成现有的ETC与ETH双链共存局面。

Hcash是如何解决这个问题的呢

在Hcash的系统内，有5%的代币会发送到一个DAO，由Hcash的全体持有者通过即时动态投票来决定资金的用途。例如，开发钱包等基础设施建设，或者进行公开推广等商务公关活动。DAO的形态为Hcash社区提供了源源不断的活力与积极向前发展的动力，同时，Hcash DAO的代码会经过严格的审核并在初期加入必要的人工干预（由基金会邀请第三方进行代码安全审核），以保障DAO在早期的资金运用过程中不出现重大失误。

代表混合，双重共识机制更安全

数字货币社区的协同一直是个难以解决的问题，众所周知的比特币协议升级斗争在过去两三年的时间内一直影响着社区的发展。而类似于Zcash的过分中心化的数字货币则排除了社区其他成员的参与权。

Hcash参考了Decred和Dash的部分理念，提出了Instant-Open-Governance（即时开放治理系统），所有持币者可以通过PoS挖矿机制参与社区的重大决定，包括协议的更新和升级。更为先进的是，Hcash提供了一个平滑的执行方式，一旦投票通过，所有的决定将会被记录在区块链上且强制执行。这样就避免了矿工、矿池、交易所、钱包服务商的协同难题。并且，PoW和PoS的挖矿过程是有机结合起来的，二者共同保证了系统的安全性。

PoW和PoS有机结合具体是怎么操作的呢？

首先，PoW机制的存在是为了防止早期投资者在PoS分发机制中所占的收益比重过大，同时PoW是目前已经被证明的最能够有效保障区块链系统安全的机制。虽然它不可避免地要消耗部分能源，但是，从有效地保障系统安全的角度考虑，我们认为它是值得的。

我们所讲的PoW和PoS挖矿相结合，具体是这样操作的：

首先以一种传统的PoW方式开始挖矿，矿工相互竞争来解决密码谜团。根据这种实施，挖出的区块不包含任何的交易（它们更像模板），所以赢得的区块将会仅仅包括一个header和该矿工的奖励地址。

这时候，系统将会切换到PoS。基于这个header的信息，一组随机的validator（验证器）被挑选出来对这个新的区块进行签名。持币越多的validator，被选中的概率越大。一旦这些被选中的validator全部完成对该区块的签名，该模板就成了一个完整的区块。如果这些被选中的validator不可用于对该区块进行签名，那么将会被选中对下一个区块进行签名，然后选出新一组的validator，直到该区块获得正确数量的签名。手续费将会被分配给矿工和参与该区块签名的validator。

PoW和PoS结合的优势何在？

对于PoW，合格的区块可以表述为：

$$F(\text{Nonce}) < \text{Target}$$

其中Nonce是随机元素，Target是合格区块的量化，每个记账节点的Target一致。此外PoW的成功运行还需要配合如下两条约定。

(1) Best chain原则：将最长的链条视为正确的链条。

(2) 激励原则：找到合格的区块有奖励收益。

关于PoW，前面已经讲过，这里不再赘述。

对于PoS，合格区块可以表述为：

$$F(\text{Timestamp}) < \text{Target} * \text{Balance}$$

上面的PoS方式是目前nxt与Blackcoin所采取的PoS机制。最简化版本的PoS机制很容易引起财富中心化问题，同时对整个系统安全构成重大影响。

因此，我们必须在考虑Stake (Balance) 的同时，加上另一个变量来尽量避免由于单纯地参考Balance所造成的中心化以及安全问题。与PoW相比，公式左边的搜索空间由Nonce变为Timestamp（时间戳），Nonce值域是无限的，Timestamp极其有限，一个合格区块的区块时间必须在前一个区块时间的规定范围之内，时间太早或者太超前的区块都不会被其他节点接纳。公式右边的目标值 (Target*Balance) 越大，越容易找到一个区块。因为Timestamp有限，PoS铸造区块成功率主要与Balance (Stake) 有关。

Hcash的PoS机制将借鉴现有的PoS机制，在保障系统安全性的前提下，提高PoS的效率，着重提升用户在使用PoS机制时数字货币的安全性。

代表坚如磐石，抗量子攻击算法

Hcash从最初的系统设计开始就考虑了量子抗性，即使在未来量子计算机商用之后，Hcash仍然可以给用户提供安全的信息及价值加密服务。Hcash将会开发可与OpenSSL一同工作的Ring-LWE密钥交换协议，实现后量子时代区块链的安全问题。

在当前以比特币为代表的区块链系统中，SHA-256哈希计算和ECDSA椭圆曲线密码构成了比特币系统最基础的安全保障。但随着量子计算机技术不断取得突破，特别是以肖氏算法为典型代表的量子算法的提出，相关运算操作在理论上可以实现从指数级别向多项式级别的转变。因此随着技术的进步，比特币在未来遭受量子攻击是完全可能的。

什么是量子攻击

量子计算是建造计算机的新方式，在某些情况下，它的算法加速量非同寻常。正是这种特性使得原来在电子计算机^[3]环境下的一些困难问题，在量子计算机^[4]环境下却成为容易计算的。量子计算机的这种超强计算能力，使得基于计算复杂性的现有公钥密码的安全受到挑战。这就是量子攻击。

抗量子攻击意味着什么呢？

目前的绝大部分算法，都无法抵挡量子攻击。这意味着用户的所有信息，都将会暴露在量子计算机面前。如果有了抗量子攻击算法，意味着个人的信息得到最安全的保障，至少以目前的技术手段是无法破解的。抗量子攻击算法（也称为后量子密码）意味着安全。

抗量子攻击算法如果研发成功并成功应用于Hcash，Hcash将成为数字货币行业第一个采用抗量子攻击算法的数字货币，对数字货币行业和其他数字货币的影响都是深远而具有划时代意义的。

代表避风港

Hcash的地址分为明地址和暗地址，分别对应Zcash的透明地址和Byteball的Whitebyte以及Zcash的Z-Add和Byteball的Blackbyte。Hcash的用户可以在自己的钱包或者客户端进行明暗地址的转换，但是Hcash的代币总数量保持不变。在不同系统之间转换或发送的时候可以按要求发送明地址币或暗地址币。

代表便捷

Hcash在系统设计阶段就考虑与基于DAG技术的后区块链系统的交互，因此会借鉴DAG的特性与优势。在Hcash系统中交易的确认时间几乎是瞬时的。同时因为DAG并不基于区块，所以并不存在所谓区块大小的限制，理论上，单位时间能够容纳的交易量是非常庞大的（Hyper Transaction Per Second，HTPS）。而同时Hcash又需要考虑与基于区块的区块链系统的交互。所以，Hcash能够在有限的区块体积下实现单位时间的海量交易，从而真正地实现“超级现金”的功能。

[1] 案例来自于超级现金官方公众号，公众号名称为“Hcash 平台”。

[2] 内容来源于《超级现金白皮书》。

[3] 电子计算机就是我们通常所说的电脑。

[4] 量子计算机是一种遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。

超级现金的开发路线图

Hcash的数量规划

Hcash的代币总量是固定的，总量上限接近8400万，总体分为六个部分。

(1) PoW产出2100万（25%）。

(2) PoS产出2100万（25%）。

(3) 众筹（ICO）以及免费分发2100万（25%）。

(4) 早期投资者 (Pre-ICO) 1260万 (15%) 。

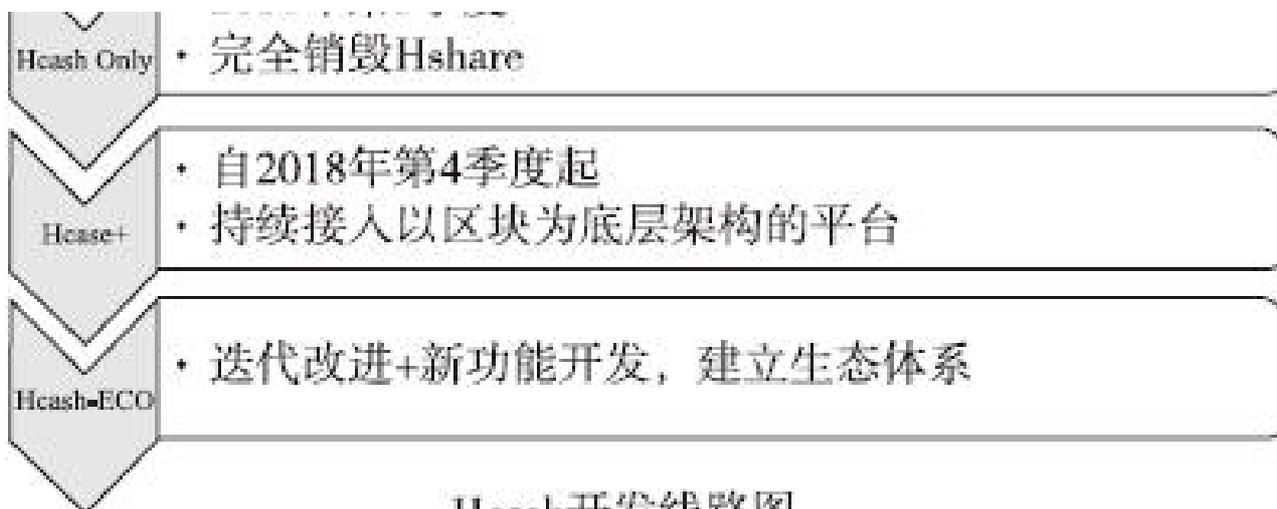
(5) 开发团队+Hcash基金会420万 (5%) 。

(6) Hcash-DAO 420万 (5%) 。

Hcash开发线路图

Hcash开发线路图如下图所示。





Hcash开发线路图

Hcash 与 Hshare

因为技术团队需要较长的时间来实现Hcash的代码和功能开发，所以在ICO结束之后，所有投资人会先获得Hshare作为代币，该代币基于UTXO模型的稳定区块链系统进行开发。而在Hcash主链上线之后，可以在任何上线Hshare的交易所或者Hcash官方团队与Hcash进行1:1兑换，并于大约10个月后完成所有的承兑与替换。Hcash团队将使用技术手段销毁所有的Hshare。在最后截止日期后，所有的Hshare将被永久销毁。Hshare的开源代码在Hcash的GitHub页面下，每个人都可以阅读审核Hshare的源代码并确认Hshare的发放总数量与Hcash白皮书所规定的Hcash数量一致。

政府对加密数字货币的态度

各国对比特币及其他加密数字货币的态度一直处于变化之中，以中国、法国、韩国等为代表的国家对比特币持较为谨慎的态度，对比特币的管理相对比较严苛，以日本、德国、澳大利亚为代表的国家对比特币及其他加密数字货币的态度比较友好，承认比特币的合法地位。

从最新的动向来看，越来越多的国家将比特币纳入了监管的范畴。

4 区块链的技术发展与未来展望

区块链从诞生到现在不足10年，虽然已经引起全世界的关注，但是很多相关技术还不够成熟，各方面对于区块链的技术探索从来都没有停止过。关于区块链所存在的一些问题，例如资源消耗的问题、扩容问题、51%攻击的问题、区块间的博弈和冲突的问题等，业界内外都保持着广泛的关注。为了解决这些问题，也出现了很多新的技术突破。

虽然技术尚不成熟，但人们依然对各种比特币项目保持着浓厚的兴趣，区块链项目大有成为下一个“风口”的趋势。当前，区块链的活跃应用主要集中于数字资产、智能合约、跨境支付等领域。同时，区块链与大数据的结合、区块链在共享经济领域的应用、区块链生态等也是未来前景看好的领域。

区块链技术存在的难题

区块链的“算力竞争”在保障“去中心化”的系统安全的同时，也带来了资源（特别是电力）的消耗，如何解决区块链运作而带来的资源占用和

浪费也将成为区块链大范围应用之前需要解决的问题。区块链的处理速度和规模也是一个问题，可以说，对区块链的扩容问题的探索一直都在进行中。此外，由于矿池的出现，51%攻击的问题也值得关注。最后，设计激励相容的共识机制，提高系统内非法行为的成本，避免区块链的各节点在交互过程中发生博弈与冲突，也是区块链有待解决的问题。

资源消耗的问题

区块链的共识机制是算力竞争，它非常依赖网络节点贡献的算力。

这些算力主要是用来做什么的呢？主要用于解决SHA256哈希和随机数的搜索，也就是用CPU进行纯粹的计算，并不会产生任何实际社会价值，因而一般意义上认为这些算力资源是一种“浪费”，浪费人力、浪费CPU等物力，同时被浪费掉的还有大量的电力资源。

正因为如此，人们对区块链共识机制的探索从来没有停止过。人们尝试过用其他的共识机制来代替算力竞争，不同的共识机制也造就了大量的“山寨币”。但是到现在为止，算力竞争依然被认为是最安全、最牢靠的一种共识机制。比特币用户及拥护这种共识机制的人认为这些资源消耗是值得的。

当前，挖矿所使用的算力大约为全网用户的万分之一，所以这些消耗尚在社会能源能够承受的范围内。与此同时，当前比特币的用户只有几百万。如果未来这个数字成数十倍甚至数百倍的增长呢？届时其消耗会给社会能源带来沉重的负担。

而在挖矿这一块，随着参与的矿工越来越多，挖矿的难度越来越大，对CPU、显卡等性能的要求也越来越高，当达到一定程度时，可能挖矿的收益会越来越低，矿工将不再乐意去挖矿。这也是一个问题。

因此，一旦区块链投入大规模的应用，如何解决区块链运作而带来的资源占用和浪费问题，仍然是一个需要解决的问题。

区块链最新技术成果

中国银行前行长、中国互联网金融协会区块链工作组组长李礼辉在2017杭州湾论坛的发言中指出：“阻碍区块链大规模应用的主要因素是技术障碍，技术限制比监管限制更加严重。当务之急是改善区块链的可扩展性，未来将有越来越多的系统称为区块链。”本节介绍几个区块链在扩容方面的最新成果。

超级账本

超级账本（hyperledger）是Linux基金会于2015年发起的推进区块链数字技术和交易验证的开源项目，加入成员包括荷兰银行（ABN AMRO）、埃森哲（Accenture）等十几个不同利益体，目标是让成员共同合作，共建开放平台，满足来自多个不同行业各种用户案例，并简化业务流程。最近，百度也加入了超级账本区块链联盟。

超级账本团队认为，支付系统在高度集权和完全去中心化之间应该有个平衡：权力既不是集中在某一个机构，也不是完全地分布式，而是合理地分割成若干个部分，用业内的说法就是“多中心化”。

比特币区块链的工作量证明机制让账本成效需要6次确认，每次10分钟，确认时间总共需要将近1个小时，而超级账本则是采用类似RIPPLE的“共识”机制，交易确认过程可在几秒钟之内完成，达成共识的技术手段主要是拜占庭容错算法机制。

分片技术

在比特币的扩容问题上，还有一个技术就是“分片技术”。分片也就是多链条。

什么是分片技术呢？

在区块链上执行交易时，网络中的所有节点都必须验证交易或执行智能合约。智能合约实际上就是网络中存储的一段等待执行的代码，该代码描述了交易需要符合的条件。当验证结果达成一致时，交易就得到确认，这个过程毫无疑问是需要时间的。

分片就是通过多个联网机器的并行处理能力，让这些机器分担验证交易的工作。它会自动将网络划分成较小的部分，也就是“分片”，每个分片都运行一个小规模的共识协议。

随着更多节点的加入，分片越来越多，验证交易时会越来越快。

案例：

Linux基金会联合IBM开发的Hyperledger Fabric这个分布式账本平台方案，2017年升级为1.0版本，采用背书共识分离的多链条多通道新架构，将交易的合约执行、区块验证与写入账本操作分离。

其交易速度在很大程度上取决于系统协同程度，常态可达每秒300笔以上，最佳可超过每秒钟1000笔，已经成功应用于资产托管等中低频次金融场景。