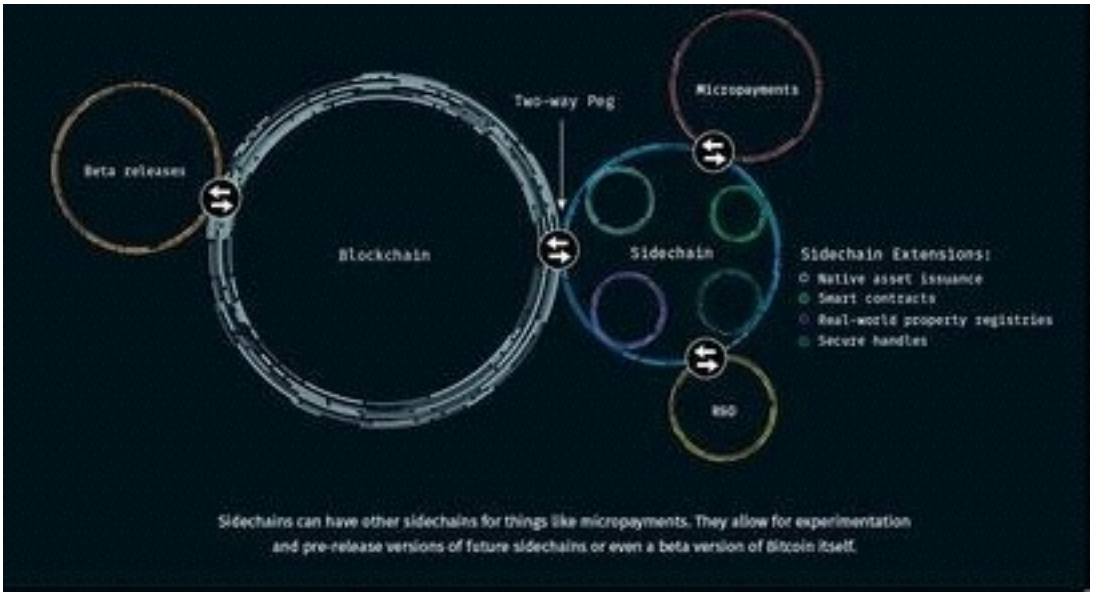
高戎汇资本
区块链技术与虚拟货币实验室出品
2015年12月



区块链技术与信用去中心化白皮书

编者按：高戎汇资本成立于2014年，是一家新型顾问式投资银行。 为中国高增长领域的创业者提供包括创业融资、私募融资、合并收购、战略重组、影视基金发行、定向增发等方面的服务。专注在TMT、物联网金融、创新医疗、新材料、环保科技、人工智能、智能产业、物联网等领域。

此白皮书由高戎汇资本区块链技术与虚拟货币实验室出品。由首席观察员、高戎汇资本创始人陈刚先生亲自领衔主笔。

第一篇：区块链技术正在发动新启蒙运动

建立商务关系的合作，我们选择签订一份合同，纸质合同或电子合同。这些合同基本都是建立在人与物的关系，有没有一种新的合约可以真正追溯信任？而信任的主体是基于物与物？

钱除了放在银行,还可以放在什么地方?

如果法币不存在了,世界就完蛋了吗?

笔者是方法论的拥护者,是伪文明进化学者，也是怀疑主义理论的捍卫者，更是权威主义的挑战者，总是充满激情地愿意参与教条主义的颠覆运动。始终相信，真理只会掌握在少数派手里。也坚决捍卫自由和个人意志。

现实世界并不美好，正如金融体系并不公平。不公平是因为人与人关系、人与物关系的存在，或者出生，或者教育，或者运气等等。金融的世界里到底有没有公平、民主与自由。笔者经常陷入深深的思考。

经济学的理论存续太多年，学科是世界的真理吗？

哲学世界是虚拟世界的真实想象，它是新文明的缔造理论。哲学与金融体系的关系在哪里？

互联网在重塑社会结构、知识结构，人与人之间的关系，互联网的使命应该是人、物、人与人、物与物治理结构规

则的制定者，和上帝一样是新信仰体系也是最基层层次信任关系的重建者。互联网真正的思维是如何将算法带入规则与文明的重塑。

从桌面互联网到移动互联网，再到物联网，万物网。算法是新世界的主宰者，连接是动机是过程也是结果。

算法与算力行者无疆！算法不应该仅仅是算法。程序不应该仅仅是程序。数字也不应该仅仅是数字。资产不应该仅仅是资产。

任何学科都是交叉的，社会学、政治学、法学、数学、哲学、密码学、易学、物理学等等，交叉会产生怎样的社会魔力呢？

世界本是0和1，信任就在0和1。

计算机的算法难道只是人类的科技发明吗？应该还有其他的渊源吧…

可否把信任放在计算机系统里？机构信任依旧不安全，这是金融总是把风控放在第一重要的根本原因。因为机构信任有瑕疵！

所以诞生了这样的思考:

社会共享的信任是算法式信任

而引领新的信任结构重塑的正是区块链技术。我个人称它为金融的终结模式！更是金融互联网化的快捷通道，当然绝对是互联网金融从青少年迈入成熟期的必经之道！

区块链对于互联网治理结构的重塑意义不言而喻。区块链技术的真正诱人的地方和潜力是彻底地重新思考现实——

什么是对我们所做的一切事情进行去中心化，并通过一个丰富的、有内蕴性的框架去重新思考生活，仔细地关注什么是可能的、被需要的，而不仅仅是对一个看上去被稀缺性所控制的现实的反应。

这一场新的思考会是精英群体由少数派引领的文明变革。新的启蒙运动不是从无知到有知，而是有知到有知。它的启发源是互联网的社交革命对于金融体系的思考，它是數學與哲学的原理驱动，它的启发源最直接的力量是比特币的区块链技术的文明进化。是人类的一次自我颠覆与升华！

区块链技术是思维模式的变革，是生产关系与生产力的倒转，是社会生态的平衡的最后的涅槃，是金融体系与社会体系的无缝衔接，是自由世界民主世界的召唤与运动。

社会信用体系的终结不是完善再完善，而是将信用体系放置在计算机的算法和程序里；中国如火如荼的征信业态的建设永远无法完美仅仅是改良和机构约束。依旧是机构信任的传统思路。

唯有算法的信任，终结模式的完美收官。

之后，人类将进入人机文明的共存。算法与程序主导的新文明让人类进入一段忧伤的时光，人类进入强人工智能的世界，万物相联，一切的价值资产皆为代码，以算法存在于万物之中。

不要阻止文明的进化。不要阻止趋势。

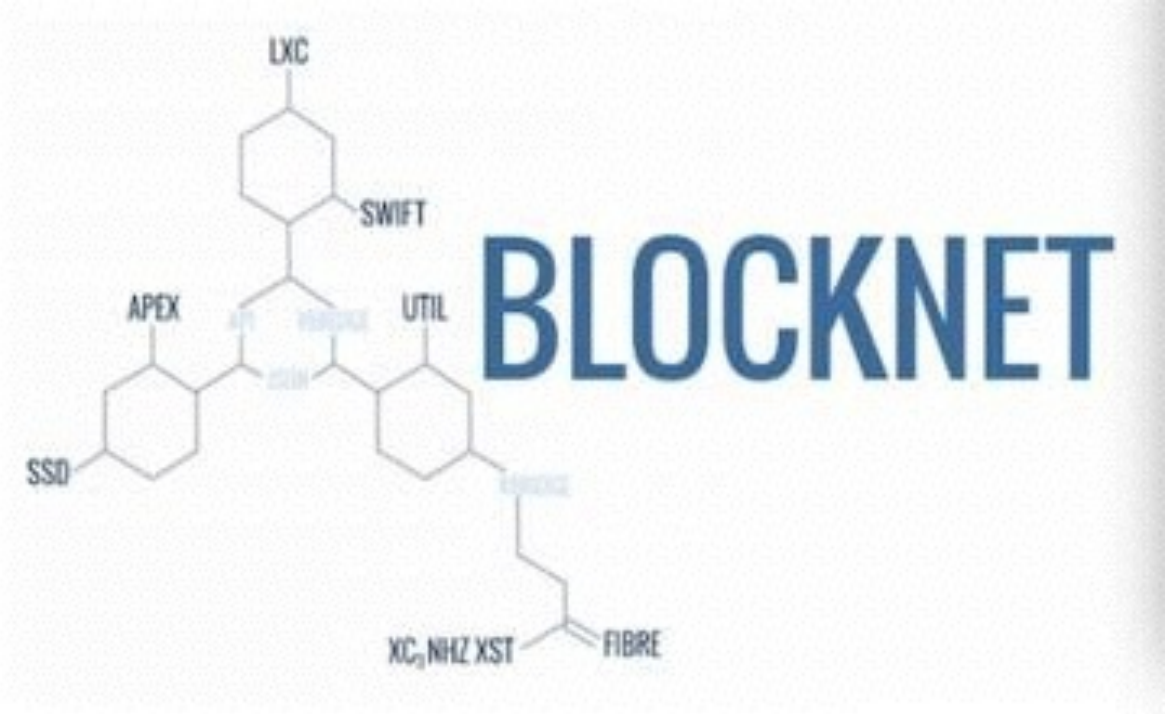
技术正在加速。传统终究成为历史。智能世界正在蔓延。我们也终将不再是我们。

人类爱上程序，人类与机器人恋爱，指日可待！社会伦理、道德、法律、世俗、二次元等等都面临重塑。

静心等待。拥抱变化。

参与与见证这一场新启蒙运动吧！

第二篇 区块链技术重新定义：信任



亚洲数字资产认证协会已经成立，致力于区块链技术与虚拟货币领域的ISO的认证。不同国家区块链技术的协会、学术机构正在设立过程中。全球著名大学计算机系的区块链技术讲座课堂济济一堂。北大，清华，南大等计算机博士生们，夜以继日的研究区块链技术。

区块链技术最成功的应用-比特币在世界范围内，掀起了一场数字资产的变革。200多种加密虚拟货币及组织积极地推广着区块链技术。笔者最近看到德勤会计师事务所已经成了区块链技术部门，来参与日常的审计工作，效率提升！笔者建议股权众筹平台可以应用区块链技术进行众筹股权登记，用智能合约替代电子合约。笔者建议各金融平台应用区块链认证与登记技术纳入风控技术体系。笔者建议征信公司在学习美国FICO模式同时，建立区块链技术实验室，开展分布式信用资产“链计划”。区块链技术商业前景无限光明，笔者会在后面的文章做更多案例研究分析。

万向金融率先在国内成立了区块链实验室，在肖风同志的感召下，高戎汇资本作为中国本土创新型顾问投资银行也于本周在中国上海成立了区块链技术与虚拟货币实验室，同时邀请了国内领先的几名高校计算机博士生以及几家加密货币的创始人参与到区块链技术的研究中。笔者将致力于区块链技术与物联网金融应用场景的设计与商业探索。笔者认为，桌面互联网和移动互联网20几年的黄金光辉好景已经迎来夕阳的最后日照。科技的进步将我们带入物物相联的新世界。 这个全新的智能世界，完全由数据和算法驱动。

之所以关注和研究区块链技术，因为，金融科技是商业社会变革的基础力量，区块链技术的去中心化思想从理论体系逐渐成熟，接下来就是商业场景的应用。笔者预测在5年内会诞生几家区块链技术的独教兽创业公司， 区块链技术引领的商业革命是颠覆式的。

作为中国金融业态的参与者，高戎汇资本秉持对于金融的敬畏，同时保持怀疑。 正如在之前的文章里，不止一次

的质问权贵金融对于自由的奴役的公平性。区块链技术已经告诉我们答案。

金融的交易缘于信任。

然而人与人之间的信任是建立在时间高昂的成本与心智的高频磨合，这样的信任，脆弱不堪。人与人之间的连接最大的特点就是不稳定性。

中国有句俗话，叫做事就等于做人，几乎没有一个中国人对这句话表示怀疑，似乎代言了真理，然而，如果人的短暂一生战战兢兢地为做人而奔波，不是一件很悲哀的事吗？

中国最害人的一句话叫“古人云”。古人已古，世界在变，云则往也。

生活发明了“对不起，谢谢你，请原谅，我的错，你很好”等等这些心灵慰藉的语言，有没有问过自己，你每一次道歉都是诚心诚意地吗？你的谢谢是走心的吗？心累是因为角色的扮演。心累缘于不稳定的信任危机。

科技的发展并不是人类的需求，而是早已存在于那里。人类并不存在发明与创造，只是在应该发现的时候发现，正如，任何事情的发生，你在某个时候遇到某一个人，绝没有偶然。 因为，它本来就存在于那里。时空只是纬度的约定，一切都是一种协议。

信任是一种协议。

信任的原理是点与点的链接，存在与物理和数字空间，存在于真实与虚拟世界，它或许在某一个区块，或者存在于两个不同的区块，衔接的就是“链”。这个区块的布局是分布式的，没有中央集权。有中央集权的叫背书，背书的东西叫第三方。区块的世界里没有背书，没有第三方。信任

关系链条里活动的是信用资产的数字，即为数字资产，在虚拟的世界通过算法转化为代码，代码形成程序，程序驱动着链接，而信任的链接是在一个系统里，经过注册、登记、交易，一切都在程序里进行，一切都在0和1之间转化。 这里没有权威，没有意见领袖。这是一个天然的社区，一个去中心化的社区，是协作式的，其基础架构就是区块链技术。

这就是算法式信任的原理。

算法式信任是机构式信任天然的敌人。正如，草根金融发动的互联网金融革命，是对权贵金融的挑战一样，会引起后者的不安。但深层次的意义是引发后者思考继而是自我变革。互联网金融扮演的是“药引”的角色。

旁观不是真正的参与，参与是必须加入“链”的活动。 链的协议就是信任。诉求就是把信任交给计算机的算法。

互联网基于协议而建立连接，是自由世界的1.0， 物联网的链接协议是自由世界的2.0。这里面有一个重要的“门”或者说是“开关”就是协议。

金融的融，正是“链”。作为金融科技的终极模式，区块链技术必然先从金融领域实现突破。首先就是技术驱动的代币和法币的博弈。我预测必然是法币的消失。因为，这是进化，这是趋势，这是文明再造。

趋势不以任何人的意志为转移。正如我预测人类“发现”的人工智能最终会打败人类的道理一样。请注意，我这里用的词是“发现”不是“发明”。发现是看到了原本就存在的事物，发明是发现文明。 这是文明的进化。 当我们把趋势放在嘴上的时候，趋势已经发生了。你所说的未来，其实

已经到来。 伟大的心灵学告诉你，要活在当下，其实是说要相信未来。因为当下即未来。所谓保持一颗平常心就是保持一颗未来心。这是宇宙的密码，而掌握密码的一定是少数派。 人人都挂在嘴里的是教义，不是真理。不要做教义的传播者，要做真理的发现者。发现真理先从怀疑开始。

区块链技术不是发现，是发明，是发现了新的文明。这个文明的本质是自由和意志。这个新的文明与强人工智能的发现是同步的。 区块链技术的成熟是与超级人工智能匹配的。

区块链技术将宣告平台意义的终结。我们不再需要平台的服务， 平台依然是机构式信任的产物。 互联网最后一次的浪潮可能是C2B模式，是云计算，终结成数据驱动物联网的基础，这是一场伟大的“交接”。 某平号号称要将双十一再进行93年，听上去悲壮而可笑。 电子商务平台的消亡不是趋势，是正在发生。 工业4.0 刚刚起步，它的变革是大规模定制，即无数个C直接与B建立沟通，接入区块链技术，这些B会以数字资产存在于区块里，和各个C进行点对点，端对端，p2p的连接。平台此刻消亡了。物流依然存在，只是规则变了，届时你一定会在媒体上看到这样的字眼“区块链技术智能物流解决方案”。 确实有点太考验大家的想象力了。

产销者将代替用户的概念。传感器将接替流量。所以，请不要在痴迷和困惑于流量的获得，也不要沾沾自喜在流量的暂时领先。最近一些互联网金融的平台的同学纠集于流量的获得，痛苦不堪，我说为什么不研究下“物联网金融”呢？ 浮躁的商业环境，创始人总是不原意深度思考，模仿和抄袭者不仅没有自尊，长远来看，不太可能获得商业

的丰厚回报。更谈不上价值的创造。 如今资本寒冬，是资本在思考，在检讨。资本追逐流行，流行玩烧钱游戏。资本只是个游戏。用户为王，流量为王，所谓的互联网思维，是一种毒药，这个毒药的创造者，不是创业者，正是资本者。不多说，否则会伤及无辜，遭人讨厌。

显而易见，草船借箭的事件不再发生，鸡毛信的浪漫传说不会再有。中世纪应该发现不了今天众里寻她千“百度”伟大平台的诞生吧。说明，规律不能跳跃，除非想象。0和1是密钥，算法是人类文明的开始也是终结。

人类的思维正在脑洞打开。这就是进化！爱因斯坦和霍金早已发现。证明靠我们这一代和下一代人。如果2045年奇点时刻可以来临，我们将是这个文明时代最幸运的。

依旧还是思考问题的基本逻辑：真理是掌握在少数人的手里。大多人达成共识的绝对不是真理。也许你会批评笔者的可笑，没关系，所有的真理诞生的前夜都不会被接受和相信。因为相信未来是一种能力，而这种能力是宇宙的主宰。

首先来看看区块链作为一项技术的理念。笔者思考的逻辑是技术本身是理念，然后形成理论的依据，按照理论的依据，形成框架，在框架里实施系统的建设。而建设的这个过程，我们将其称定义为“算法”，而每一个“算法"的步骤其实就是达成一个又一个的“协议”。互联网的诞生是基于协议，是人与物的协议，是人与算法的协议。互联网就是介质，是中性化的。

我们过去写一封信，通过邮递员或者飞鸽，我们看上了街上的一个姑娘，我们通过媒婆去上门提亲。 我们想把家

里的鸡卖了换点棉被，于是我们到集市上去。我们想学习知识，于是家长们把我们送到了学校。我们拿着央行发行的法币，可以自由地买卖。我们发现身上的现金不够了，于是我们到ATM机取款。社会文明的形态发展，不难看出，介质的重要性。我们将这个介质定义为“中心化”。似乎失去了“中心化”，我们很难与社会共融。

比特币的诞生，让全球的理想主义和自由主义者，睁大了眼睛，因为看到了不一样的世界。每一个热爱比特币的家伙都特别想到日本和中本聪聊一聊，可是至今，没有人知道中本聪是一个人还是一个符号，或者是外太空落地在地球的新的文明？比特币的诞生引发了全球性的大讨论，有的忧虑，有的恐慌，有的兴奋，有的漠然。 有大量的投资客在悄悄地囤货，也有一些极客分子在中本聪的感召下，秘密地开设了挖掘比特币的工厂，每天在用电力和算法兴奋地憧憬着未来的新世界。

中国央行冷漠地看着比特币，这应该是最正常的政治态度。 一个中央集权的国度，怎么会轻易地容忍一个充满了自由主义意志的家伙与法币共存。然而，我们也惊喜地听到央行周小川行长明确的表态：比特币是数字资产，具有商品属性，政府不存在取缔。中国属于大陆法系，法无明文规定即可为。中国金融监管的基本套路是，静悄悄的观察，看你能玩出什么要蛾子。顺应民意，又不违反原则，通过，反之，则严肃查办。这才是大智慧。

综上所述，笔者想表达一个基本观点，就是追求梦想的道路，坎坷但是光明，任何新技术新事物都是规律在驱动，并不取决于任何人的意志。所以，过度的关注政府的态度，

不如将重心放到技术本身，挖掘技术的价值，应用于时代的需要，契合于人类的积极的探索。

不要太沉溺于比特币和法币的竞争，不要用一个基于算法的应用而去和社会的秩序抗争。这对于比特币的存在主义不公平，也违背了它诞生的基本使命。

让我们回到最原始的基础架构的基础。即本源。

宗教，哲学，数学，物理，法学，计算机，易学，材料学等等几乎所有的学科都在研究同一个问题，这是回答的场景不同。 同一个问题就是关于世界的本源。关于宇宙的本源。

易经是古老而神秘的学科，和西方的玄学一脉相承，研究的是：宇宙间一切事物发展的规律。其方法论是：阴阳。逻辑是：平衡。

物理学研究的是正极与负极，一切物理世界全部围绕着正极与负极。

计算机学说，就是0和1。

哲学，永远都是辩证。 哲学的本源：我是谁，我从哪里来，我到哪里去。

法学的本源是公平与正义，罪与罚，权利与义务，自由与约束。

灵性学的本源：本我与小我

宗教的大多教义都在讲同一个问题：有和无。

这些就是宇宙的规律。宇宙本源属于二次元。

宇宙的本源在另外一个科学的世界里，又诞生了新的发现。通过比特币，人类发现了区块链的秘密。

“发现”是看到了原本就存在的事物，而“发明”是“发现文明”。任何文明的进化，就是真理的意识之光。它藏匿于趋势与规律。它只为少数派代言。

无论你喜欢或者不喜欢，它就在哪里。

如果爱因斯坦能多活几年，笔者相信，进化论和“复利”原理这个世界第八大奇迹的发现之后，他一定可以推算出区块链技术的秘密。然而，假设并不成立。所以，担负起这个使命成了我们。

区块链技术有无限空间，本白皮书只聚焦一个话题，就是关于“信任”。

信任是如何诞生的？

信，顾名思义就是相信，两个元素1是人2是沟通。

任，顾名思义就是连接或到达，两个元素1是人2是连接

沟通即连接。信任，就是关于人的连接。

信任是一种协议，存在于潜意识里。

商业社会，协议可能表现为合同。

协议是人和人，人和物的连接。

技术的进步，人与物的连接，有了算法的加入，于是诞生了软件，诞生了互联网。从桌面互联网，到移动互联网。人与人的连接，建立在人与物的协议上。

这里的协议其基础架构是算法，其逻辑思想是：中心化。

中央银行的存在，是中心化驱动法币的地位，让人和人，人和物之间建立协议，法币成为了信任。

民政部门执行法律的意志，让婚姻合法，夫妻关系建立了协议，成为信任。

人性的弱点和劣根性，统治阶级不能放任被统治阶级的自由主义，必须圈养，以维护规则，于是诞生了法律。

宗教的统治，通过教义。教义是什么？同样是协议，协议成了信任。基督教，佛教，异教等本源一样。教主和教徒之间通过教义达成协议。本质是觉醒者与准觉醒者之间的连接。也可以理解为神性与人性的协议。

是不是，突然感觉协议无处不在？！

之前笔者将历史长河以及当下的种种协议下而约定的信任，定义为“机构式信任”。

机构式信任，其中心思想是“中心化的人的规则”，规则的制定者，是人。

正是由于人和人的协议的不稳定性，自古至今，战争，杀戮，被判，痛苦，悲伤，爱恨情仇等每天都在发生。其根源都是由于人所主宰的协议的漏洞。

互联网遭遇黑客的攻击，就是自由主义协议也就是我在之前文章里所说的“算法式信任”对于“机构式信任”的挑战。

那么问题来了，你一定会问，世界上有没有无懈可击的信任机制？

有！ 这个信任也同样是一种协议，这个协议的连接主体不再是人和物，而是物与物。

协议的规则：将物与物替换成代码，将代码储存在算法里。 讲到这里，计算机专业的同学们是不是应该开始兴奋了？

第三篇： 区块链技术：金融风控的终结者

让我们回顾一下，为什么会有风控这件事。

中国有句古话：人无远虑，必有近忧。还有一句话，凡事要“防患于未然”。中国的文化，崇尚的是平衡之道，制衡之说。金融业，同理可证！

金融的本质是什么？是资金的融通。资金在融通的过程中，每一个环节都具有不确定性，不确定性就是风险的基本因子。根据文化的教义，平衡才具有可持续性，和谐才健康。 从文化出发，延伸到政治经济学，统治阶层的上层建筑和经济基础关系微妙，谁决定谁都是极左的思想，取决于“屁股决定脑袋”的中国式的思维。这是中国式权利文化在金融市场的蔓延。

父母与孩子的关系，爱人之间的关系，投资者与创业者的关系都是有人的关系，存在于人和物的融通。借与贷也是人的行为，同样基于人和物的融通。 金融的三个基本要素，安全，收益和流动性，有一个共通之处，即现在与未来的空间和时间的冲突。冲突就是融通的漏斗，是不安定的因素，必须通过权力的设计进行约束，这个权力设计的约束就是控制。这个控制的过程，是物的诞生，无形之物，看不见的权力的设计，对应的是等价的交换原则，或者说冲突性的防御性设计。融通“正向防御性”设计为0，融通为“逆向防御性”设计为1，0则不作为，1则作为。

让我们看看这个防御性设计原理，第一步是做评估。

风险评估的定义：在风险事件发生之前或之后（但还没有结束），该事件给人们的生活、生命、财产等各个方面造成的影响和损失的可能性进行量化评估的工作。即，风险

评估就是量化测评某一事件或事物带来的影响或损失的可能程度。

从信息安全的角度来讲，风险评估是对信息资产（即某事件或事物所具有的信息集）所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性的评估。作为风险管理的基础，风险评估是组织确定信息安全需求的一个重要途径，属于组织信息安全管理体系策划的过程。

评估是动机，记住，人有动机，机器和程序只有指令。这是重要的意识。

然后，我们来看风险控制之防御性设计的过程管理：

首先，要确定保护的对象（或者资产）是什么？它的直接和间接价值如何？

其次，资产面临哪些潜在威胁？导致威胁的问题所在？威胁发生的可能性有多大？

第三，资产中存在哪些弱点可能会被威胁所利用？利用的容易程度又如何？

第四，一旦威胁事件发生，组织会遭受怎样的损失或者面临怎样的负面影响？

最后，组织应该采取怎样的安全措施才能将风险带来的损失降低到最低程度？

解决以上问题的过程，就是风险评估的过程。

进行风险评估时，有几个对应关系必须考虑：

每项资产可能面临多种威胁

威胁源（威胁代理）可能不止一个

每种威胁可能利用一个或多个弱点。

上面的内容，就是现代金融风控体系的重要的思考原理。风控体系就是在关于动机及过程管理的体系。而动机和过程管理正是风控体系的基本逻辑。有没有发现，这些都是人的设计。人的设计，基于知识结构和经验判断。基于案例和统计学的原理，产生了尽职调查。调查的根源是空间和时间的不确定性。调查的动机是为了使得未来和现在达成共识。请注意，这还是人的设计。正如所有的调查报告都是人写的。人参考的资料和数据还是人写的。

那么，重点来了，人设定的程序，能不能被技术取代。答案在过去可能是无解的，如今它有了。

这个答案就是区块链。

区块链技术的发现是通过理想主义的超主权货币-比特币被发现的。有人说，没有货币，就没有人类现代文明。有一位学者说：货币将决定人类命运（money will decide the fate of mankind）。凯恩斯在《货币论》中说过：如果以货币为主线，重新撰写经济史，那将是相当激动人心的。显然，比特币的出现，对于人类文明的进化意义已经是无可厚非的。尽管，它在世界范围内还依然是具有争议性的物种。所以，我们今天在文章里不讨论这个争议性的创世纪的物种。我们将注意力聚焦在它的底层技术架构：区块链的技术。

看看它是如何通过技术的实施来终结风控的传说。

区块链重塑交易结构，重塑信任。

去中心化的通俗含义是说，不要中央集权就可以能够成功在多方之间处理交易。显而易见，金融业的风控体系正是中央集权的表现，一切的金融活动如果失去了风控，将是不合法的，不合规的，是不被支持的。 金融机构赋予了

风控部门独立巨大的权力。这个权力是中心化的集权，以控制作为信任机制的出发和归宿，管理着所有金融活动的运行。

风控的首要任务是防止交易的欺诈。

区块链技术的基本原理是：它能够通过一个分布式电脑网络来自动处理，通过加密手段来保障安全，让交易欺诈变得难以实现。

区块链（比特币的底层技术）是一个神奇的盒子—通过把现有解决方案重新加以利用并且赋予许多创新，使它变得极具革命性。在一个技术中，很难可以看到有这么多创新的理念放置一个框架内。

现在让我们看一下区块链技术对于风控体系颠覆性的特点。

自我监管

我们很少可以看到一个平台能够在几乎没有人干预的情况下进行自我监管。在所有类似于金融行业的领域中，中央银行和监管机构来制定统一的规则，并且进行管理。而区块链技术让系统不再需要这些来自平台自身的监管。这个革命，让许多人失业，也让监管部门的权力被转移。一项技术真的会有如此大的魔力吗？我知道你一定会质疑。

工作原理

区块链提供一个称为“工作量证明”的机制，让系统中的每一台计算机节点参与审批每一笔交易。该系统内置检查和平衡机制，以确保系统中的任何计算机都无法欺瞒系统。所有的这些审查和监督完全由计算机自动完成。目前已经有不少可以替代“工作量证明”机制的其他共识模型，但是

依旧保留了每个客户端或者节点能够点对点管理系统的这个核心理念。更加重要的是，区块链让系统中的每个元素都是完全透明，因此对于一个遍及全球这么大规模的社区，区块链技术能够很容易的对它进行审查和管理，从而有效地降低了欺诈行为。想象一下它能够多大程度的节省成本和提高效率。然而这些工作目前是由金融机构的风控部分在操作。只要有人的地方就有误差，风控太严则过，太松则不及。过与不及都不恰当。把风控交给计算机的算法吧。把客户的资料、动机、行为、数据记录在区块里，用公钥和私钥进行管理，区块和区块之间通过“链”的活动进行自主的管理。

这样的过程，就是笔者在之前文章里所定义的将“机构式信任”转移到“算法式信任”。去人格化，账户不再是个人或机构客户的交易账户，而是一切数字化交易的主体和客体。 这个过程的管理交给算力，我们称之为“哈希”。区块链技术的算力非常强大。

交易动机和交易过程，人被替代了。客户和金融机构之间的关系，变成了交易账户的关系，点对点，交易结构成完全P2P化。 一切的操作都是计算机的算法和算力（哈希）在驱动。

流程依然存在，只是账户在融通中变成了代码，代码在区块内以及区块与区块间进行。

交易的安全性，依旧存在。密码依旧存在，公钥和私钥是区块“链”的通行证，这个通行证发放和审核，也在算法中进行。

描述到这里，你应该看到，无论是自然人还是机构的法人（或者非法人团队）作为人格被转化成了代码，代码在区块链的技术中，被程序化了。人与物的关系，被格式化为物与物，一切都是数字化的资产融通。金融的本质没有改变，依然是资金的融通。 金融的风控流程，人的操作以及机器辅助人的操作被格式化为代码化，一切的过程被记录，而且永远不得篡改。

行为背后的是协议，协议和协议组成了程序。

安全、收益、流动性管理这三个要素全部通过区块链技术进行管理，全部弱化人为的操作。这就是物联网金融的基本理念。

法律意义和便于追踪

行动主体和他们的行为都是被记录在区块链上的。任何交易双方之间的交易都是可以被追踪和查询的，并且能够在法庭上进行证明。这是因为所有的交易都是需要一组公钥/私钥来加解密处理和交易的，一旦加入到区块链上，就永久性的不可改变。任何记录，一旦写入到区块链，都是无法篡改的。任何在区块链上持有资产或者数字货币的人都会有在区块链上有他们自己的公钥。当发生交易时，需要由控制这些资产的前一个持有者使用私钥进行签名。区块链还允许多种机制来发生交易，比如可以设定为需要两个人联合签名才能进行一笔交易。在一个没有企业或政府来背书的系统，具有法律约束力的机制能够极大的提升对于该系统的信任因素。

系统性技术风险的规避

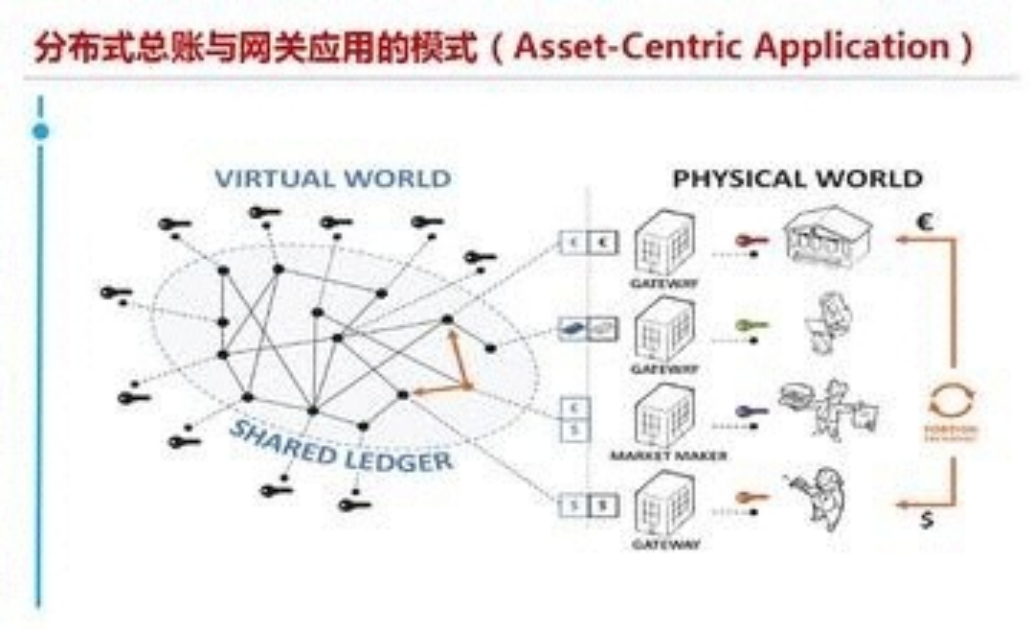
全球化的平台系统或者全国性的平台系统，在进行重大交易时是不能承受宕机风险的。区块链，一个完全的点对点网络，有许多分布式节点和计算机服务器来支撑，有着极高的可靠性，每一个系统中参与的节点上都保存了一份完整区块链数据的副本。这使得整个网络具有极高的容错性，如果任何一部分的几个节点出现问题，都不会影响网络其他部分继续运作。这使得在没有使用复杂技术的情况下就能够像灾难恢复中心或数据库冗余中心一样，获得24/7的全天候运营特性。所以说，区块链技术提供了金融大数据和云端储存的基础架构。这个技术使得交易的过程，本身就规避了网络的不可预见性带来的灾难。

当然，理论规理论，实践归实践。当前，金融的世界依然还是人的世界，人是金融世界最宝贵的资产。风控是金融最为重要的元素。人依然是风控的主力军。改变不是一朝一夕的。

区块链技术的诞生不是偶然的，它是文明进化的使者。技术可以被大量应用取决于真理的探索者对于真理的普及。互联网诞生前夜走的路，区块链技术同样要走上一遍。

“算法式信任”是基于信任体系的深度研究。 人与人的信任，没有完美方案，人与物的信任也只不过信任在技术加入之后的创新与进步， 然而，不是终结，那么，终结者可能就是在物与物的之间，它存在于“算法”中。

第四篇 区块链技术之应用场景：信用去中心化



一项技术如果只是在实验室,不能出街，绝对是技术的悲哀。

谈到商业应用，必须谈场景。 物联网几乎是为场景而生。区块链技术我暂且将其约束在物联网金融的范畴里，研究下它到底是如何为场景服务的。

互联网金融平台大多在思考如何接入权威的征信公司的数据来给自己增信。大多数平台还在思考流量如何获取，用户如何获取，怎样从竞争对手那里抢客户。甚至，还在用小恩小惠传统方式取悦客户，在大街小巷拿着二维码让客户扫。兑付的危机，平台系统遭受黑客攻击时刻担心受怕。

你有没有想过，你本可以跨平台抢客户，甚至，不用花大价钱宣传品牌，也不用处心积虑找大的机构给自己做背书。有没有想过或许你根本不需要什么资金托管，什么第三方支付平台，什么第三方征信平台接入，什么风险备用金等等。

区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了过去十分钟内所有比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。

中本聪持有第一个区块，即“创世区块”。

中本聪是区块链的创始人，但不是CEO。区块链没有董事会，只是一个宗教。这个“教派”迄今为止，包含了意识形态、数学、密码学、电力学、金融学、计算机等众多学科。

探讨信用去中心化，首先要来理解什么叫：去中心化的去中心化。

简单讲就是基础架构的基础架构。

这个架构是由两个数字组成，0和1，按照二进制的换算，成为可以可以驱动点对点交易结构的底层交易结构。

这个最底层的架构就是区块链的技术。

区块如何形成？从第一块开始，就有第二块。按照中本聪的算法，合计固定比特币的总数量为2100万个，并且越开采越困难，每四年一次对于开采矿工的奖励减半。2009-2012年为50个比特币奖励，2013-2016年为25个比

特币奖励。2100万个被开发后，可以全部投入到流通领域，足够替代地球上所有的法币流通。

根据哈希算法，我们设定每个区块可以有2016个客户端，即2016个交易账户，每个交易行为的形成需要10分钟时间，即一个区块的形成需要2个礼拜的时间，即2*7*24*60分钟。

假设一个互联网金融平台有10万的投资用户帐号，可以将10万个投资用户帐号按账户形成的时间和交易登记记录进行登记在不同的区块上。

登记规则如下，首先对10万用户进行定位，假设有一个账户属于投资人，则将其账户开在以D开头的账户目录下。平台公司以根目录替代，用英文字母加注册登记时间为根目录代码。 同理，把借的账户登记在J开头的账户目录下。

笔者发明一个“三维”记账法。三维分别是：身份代码、身份定性、委托需求。比如在钱趣多平台上一个叫张兵的用户， 需要借10万块钱，时间6个月，每月付息，到期还本。钱趣多CRM记录其账户为：ZB****-J-10-06（****是张兵身份证后四位）； 当钱趣多登陆区块链，张兵的帐号则自动识别为：QQD-ZB****-J-QQB10，000，0-6*30*24*60

解释下：第一个QQD是区块链识别，QQD是钱趣多的代码为根目录单位；J是账户定性（借）；QQB是钱趣多自动系统分配的数字钱包“钱趣币”，6个月要合算为分钟单位。

帐号是张兵获取的私钥。储存在区块的Header部分。 因为系统识别这是来自钱趣多的账户信息，所以钱趣多可以以私钥察看张兵账户情况。

张兵的帐号的交易记录储存在区块的Body部分，不可篡改，钱趣多的私钥权限可以访问。

这里要说明的，在没有区块登记之前，平台是平台，个人是个人，也就是说钱趣多是平台，张兵是个人。这是一个中心化的连接机制。

然而一旦钱趣多登记在区块上，钱趣多和张兵都全部变成账户，变成代码，通行证就是各自的私钥，因为张兵是钱趣多的用户，所以钱趣多的私钥是可以打开张兵账户信息的。这是钱趣多在私有链上的Power。 张兵不可逆。

账户不属于人，属于物。无论个人还是平台，一旦在区块上进行注册，进入区块链技术的算法，就只有物。物以数字代码的形式呈现。

再说张兵的委托事宜。张兵的账户动机是在区块的各交易点匹配其需求的动机账户。形成在区块里或跨区块的点对点的“链”接。如果在一个区块里匹配，则不惊动“链”，如果不能在一个区块里匹配，就要通过“链”的Power进行匹配，每次匹配活动以10分钟为一个单位。也就是说10分钟进行一次匹配。不足10分钟计为10分钟，超过10分钟，不超过20分钟，以20分钟计算。以此类推。直到匹配完成。

这里会出现这样的现象：属于在钱趣多注册的张兵，他在另外一个叫添米的平台上，匹配了一个叫刘军的账户，

比如刘军的账户默认为：TM-LJ****-D-TMB15，000，0-6*30*24*60 。

解释下：刘军的帐号是张兵的目标值。目标值（数字资产以及时间值）必须大于或者等于账户值。刘军账户的描述：注册在添米平台上，可以借出金额不超过15万，借出时间最长为6个月。

区块根据算力，在最短的时间内匹配到两个账户。交易记录成立，并且被永久的记录下来。交易信息会在区块里以智能合约的形式，瞬间成立，并按照账户私钥授权签订数字签名，系统发送交易信息到账户默认的优先智能设备上。 不是确认，而是告知送达。当然交易账户双方可以以私钥察看交易记录。

这就是区块链P2P的过程原理。

这样的匹配，7*24小时，永远不停地进行着。

这里没有平台，没有人，只有账户和账户在交易。

交易信息可以修改吗？显然，不可以。

交易记录可以被删除吗？显然，不可以。

交易的过程中资产在数字货币钱包里流通。 交易过程，不可逆转。

平台可以察看账户的资产情况吗？显然，不可以。

账户的隐私，是绝对化的。

区块链的最新技术应用：脱胎于2008年出现的比特币技术，它提供了一种去中心化的、无需信任积累的信用建立范式。区块链技术本质是去中心化且寓于分布式结构的数据存储、传输和证明的方法，用数据区块（Block）取代了目前互联网对中心服务器的依赖，使得所有数据变更或者交易项目都记录在一个云系统之上，理论上实现了数据传输中对数据的自我证明，深远来说，这超越了传统和常规意义上需要依赖中心的信息验证范式，降低了全球"信用"的建立成本，这种点对点验证将会产生一种"基础协议"，是分布式人工智能的一种新形式，将建立人脑智能和机器智能的全新接口和共享界面。

信用去中心化帝国

区块链技术思考的结果是通过全网节点记账的方式建立信用。协议的信用基础就是盖"时间戳"。谁来盖呢？叫做"矿工"的角色来盖，（笔者认为每个互联网金融平台就是一个矿工），矿工的报酬是获得挖矿的报酬。

在区块链上每十分钟全网进行的每一笔交易盖上时间戳，并记录在区块（Block）里面，然后用解SHA256密码学难题来证明各节点的算力，大家一起在全网竞争记账，最后比赛谁的算力最大。上面的模拟案例：张兵遇到刘军就是算力的结果。

算力最大的就能竞争到每十分钟一个的合法区块记账权并向全网广播，得到二十五个比特币的奖励，比特币产生的前四年是50个（这个过程俗称"挖矿"，其本质是全网竞争记账，建立P2P信用）。这样每十分钟出一个全网记账的合法区块，并链接在一起，形成一本总账，就是所谓"区块链"（blockchain）。

所以，区块链的创新，开启了人类物联网时代，信用去中心化的建立。信用成本最低，而且永恒。

*以上临床案例模拟：钱趣多和添米财富

第五篇 区块链技术重塑信用未来

法币的产生，虽然把金银作为信用载体的成本在物理上降了下来，但是一定需要央行的中心化信用背书。各国央行的信用是不一样的，有的国家的信用很差，有的国家信用超好，如中国央行。这样事实上又增加了国际贸易的信用流动成本。

毫无疑问，区块链技术的去中心化是建立P2P信用可能是最完美的Solution。

互联网完成了协议的建立，但是不能执行去中性化的问题。所以TCP/IP协议是平等的、协议的、程序的、可执行的，完成了信息传递的高效率低成本。

但是信息传递的协议，尽管高效，却不能上升到价值层面。比如facebook和中国的微博，无法价值对话。因为，一个重要的发现就是信息传递的成本是接近零了，但大家凭什么相信你传递的信息是真的呢？所以，还是信用问题。信用问题是互联网永远的痛点！

协议的最高境界就是价值协议。价值协议，即信用协议，在互联网的世界里没有办法完成，任何可以用于背书的中性化的介质都不是价值的最终。

2015年，是区块链技术的创新冲出比特币的领域，向其他领域传播的标志年份。2016年，将会有商业场景与技术进行匹配。越来越多的区块链技术实验室的成立，大家的共同目标就是商业应用。用不了几年，区块链技术会诞生独角兽的创业公司。

未来，所有的智能设备连接在一起，以区块链技术为基础，建立智能合约，形成智能金融网络，人人都是金融家，物物都是金融标的，自金融形成终极体系。

出品人：高戎汇资本 区块链技术与虚拟货币实验室

*我们正在寻找区块链技术领域未来的独角兽公司，商业计划书请发送bp@grhgroup.cn 或者如果您对区块链技术感兴趣可以直接发电子邮件jc@grhgroup.cn