本篇文章给大家谈谈专家解读比特币，以及一文读懂比特币对应的知识点，致力于为用户带来全面可靠的币圈信息，希望对各位有所帮助！

·《文理两开花》主播·

肖小跑：《羊群的共识》作者，金融行业从业者及连续创业者，播客《墙裂坛》主播，公众号“肖小跑”主理人。

王玮： 数学和计算机学霸，兼通技术与金融。若干年前“all-in”区块链领域，成为区块链行业知名意见领袖之一。

“智能合约”这四个字似乎也是个“模因”了：这是一个在金融 科技 业界、甚至所有和 科技 、数字化相关行业中都会听到的概念——一个“听起来很厉害但并不知道到底是什么”或者“不知道厉害在哪儿”的模因，反正这四个字代表了“ 科技 进步”，都“智能”了还能不厉害么？

但它到底是什么？能做什么？不能做什么？迫切需要智能合约专家用小白和文科生都能听懂的语言来除魅。

正好最近在现实世界的金融市场上，也发生了几件有趣的事：俄罗斯债券违约、还有金属市场上的“镍逼空事件”——所以我们干脆做一个案例分析，现场来看看智能合约到底能不能解决这些现实世界中头疼的问题。

·本期提纲·

1、365度全景式“除魅”智能合约：它到底“智能”在哪儿？是一段代码？一份合同？还是一个机器人？

2、它只能解决虚拟世界的问题，还是也能用于现实世界？

3、俄罗斯债券违约：如果用了智能合约，结果会不同吗？

4、如果主权债放在智能合约上会不同吗？智能合约能解决“信用”问题吗？

5、镍逼空事件和LME“硬分叉”：如果LME采用智能合约来自动执行，结果会不同吗？

6、区块链上的“硬分叉”和现实世界中的“硬分叉”（取消交易）有什么不同？

7、“投票”+“冷静期”的设定能避免“多数人的暴政”吗？

· 文字稿 ·

小跑 02:48

“智能合约”（smart contract）这四个字好像已经变成一个“模因”了。它是金融 科技 业界、甚至更广泛的跟 科技 、数字化相关的行业，都会听到的一个概念——反正这四个字就代表了 科技 进步、代表智能。

但它依然是一个“听起来很厉害，但不知道到底是什么”，或者“不知道到底厉害在哪儿”的概念。大部分人，包括我在内对它也是一知半解。所以今天请王玮老师用小白和文科生都能听懂的语言，给大家“除魅”一下智能合约。

另外，正好最近现实世界的金融市场上，发生了几件很有意思的事——包括俄罗斯债券违约、镍逼空事件。今天干脆拿这两件事来做一个案例分析，来看看智能合约到底能不能解决这些现实世界中的头疼问题。

先请王玮老师给大家解释一下： 智能合约它到底“智能”在哪儿？

王玮 04:26

智能合约如今不管在区块链、DeFi、还是未来的web3领域，都是最重要的核心。比特币出来时，大家都说区块链是“分布式账本”；自从以太坊诞生，大家慢慢看到智能合约在web3.0甚至metaverse领域，作用越来越大，重要性也越来越高。

我先从发生在身边的一个小故事说起。我有一位师妹，是大学计算机系教授，去年问了一个问题：区块链我都能理解，但有一个问题没想明白——智能合约到底“智能”在哪儿呢？

之所以这么问，她一定是把“智能合约”理解为“智能代码”了。因为是搞技术的，她一定是跟别的代码比较，默认“智能合约”应该比别的代码更“智能”，才配叫“智能合约”。

我的答案是： 不要把它跟计算机代码相比，而是跟现实世界当中的“合同”相比——它是一段智能的“合同”，而不是智能的“代码”， 就好理解了。把它跟代码比较，有点侮辱“智能”这个词。但跟日常经济活动中签的合同来比，逻辑就比较贴切了。

那跟合同来比，它智能在哪儿呢？

我们日常的合同有几个特征：第一，有签署的双方或多方；第二，它有合同的条款，什么情况下执行什么条件做什么事情；第三，有合同标的物，一手交钱一手交货，合同约定了提供什么商品或者服务，付多少钱；第四，合同大概还有个编号，有个标识记录这是哪份合同，哪年哪月哪日签的，谁跟谁签的等等；第五，要有一个管理手段，签署多方要各持一份，防止某方把条款改掉。这五个特征基本代表了日常执行合同的最基本条件。

从这个角度，智能合约就好理解了。

比如以太坊的智能合约： 第一，它的代码和存储的数据，其实相当于合同条款达到什么条件、怎么自动执行——大家可能都知道智能合约的这个特点。第二，它还能够让“签署双方各执一份”这件事在链上实现，签署双方都能访问到区块链的时候，其实就是都能看到合同副本，而副本不是自己能掌握或篡改的，而是链上存储的。

这就很有意思了：中本聪发明区块链，是为了防止“双花”比特币这种纯数字资产的，结果到了智能合约时代，以太坊一下子赋予了它“帮助合同所有方存储无数副本、保证不被篡改”的神奇能力。区块链是全球化的分布式存储，它能够让世界上任意多的人来共同签署和执行一个合同，而不会让有被篡改的危险——这件事在传统领域做不到。因为技术的限制，你没法让任意无数人同时签署一份合同。

第三，智能合约的每一段代码都有一个对应的“地址”，执行这段代码的入口，这个入口可以理解为合同的编号，唯一的标识。

第四，智能合约本身还能够拥有“其他的财产”。 我们日常的合同只是一张纸，一个附属品，财产仍然在人的掌控之中——合同就算约定了镍的交割，纸怎么能控制镍的移动呢？而智能合约本身却能掌控财产。合同一定要有“标的物”，有“钱”有“货”，这个标的物是可以受到智能合约所控制的，相当于是被它“所拥有”的。在这种情况下，所谓的“自动执行”才有保障，它拥有对资产的全部执行权。

小跑 11:30

相当于司法执法合二为一。

王玮 11:33

对。所以有签订方、有无数可靠的备份、有自动执行能力、有可以找到的地址和

入口、还有对于合同标的物的控制权——从这个角度，它确实比普通的合同要“智能”的多。

小跑 12:04

其实特别理解王老师师妹的想法，毕竟都是理科生，大家可能天然会从代码角度来理解。但作为非技术背景的普通人，我反而没有理解的这层障碍。

一看到“智能合约”这四个字，没有代码背景的人，天然就会先把它想象成一个合同，一个不用人来执行的“聪明的合同”。在现实世界中，比如我跟老板签了合同，但是他每个月不给我往账户里发工资，我也没办法。

另外，智能合约建在区块链上，就是说跟我签合同的人，我不用认识也行。我们之前没有做过买卖，没有建立过任何信任关系，其实也能签——因为区块链保证了“人手一份”且不能改。 这有点像我们讨论过的SWIFT——它实现了“信息”和“账户”合二为一；而智能合约是实现了合同的“内容”和“执行”合二为一，一旦建立了，执行就不用太担心了，智能合约会自动给我发工资，不用再信任老板。

可是，仔细再想的话，好像又有点琢磨不透。如果它的执行是自动的，那出了问题该怎么办呢？ 我们订立传统合同时，会有后续发展过程中修改条款的情况，或者出现特殊情况导致合同不能按照订立时的条款来执行——如果出了差错，智能合约还是会不管不顾的执行下去吗？

如果真是这样，大家在“签”智能合约，按启动键的一刹那可能就要再想想了——只要一按，后面就没有改的余地了，对吗？

王玮 15:00

先说第一个问题：智能合约最大的价值就是能让世界上相互不认识、或者没有过任何协作关系的人，能立刻签署、执行这个合约，获得结果——这跟区块链的特征是一脉相承的。

很早我们在介绍区块链时，会强调它的一个特征——能让全世界本来没有任何协作关系的人，开始转账交易。中本聪发明的防止“双花”，就是为实现——我们虽然不认识，但我转账给你，你知道这笔转账一定是真实的，而不会出现任何问题。智能合约就继承了这个特点，不会因为咱俩不认识、或者你耍赖而导致合约执行不了。

但如果是这样，签订了合同一定能执行，就意味着它肯定不会变。那我又怎么敢随便签？

这一点倒是要从技术角度看了—— 智能合约是可以“变”的，“变”从技术角度讲，跟一个软件系统的升级没有太大区别。

如果你一定要改变某个条款，就相当于原来的作废，新的合同重签。智能合约也是一样，相当于你把代码升级， 现在是版本1.0，过两天我来了个1.1版，换掉1.0版——我们从现在开始执行1.1版——这是没问题的。但是问题又来了，谁有权利来做这件事呢？如果是合同签订双方都有权利改合同，就没任何意义了，完全实现不了。

智能合约其实相当于在一个“市场”上，合约由一个第三方来创建，然后大家分为甲方乙方丙方，在合约上去签署和执行。

之所以敢签署，是因为我作为甲方，相信乙方丙方丁方改不了这个合约，必须执行。第三方就是合约发布和创建方，它是有权利来升级合约代码的。这样一个机制，有点像建立一个“卖场”， 里边的买卖双方在卖场里签合约，做买卖，但改变不了卖场的规则——只有卖场的构建者有权利来改。这也是一种必要性。

这种必要性会带来什么问题吗？

肯定也有。比如，第三方有“监守自盗”的危险，如果他发现改动合约对自己有利，也可以去篡改合约，导致签订者的损失。就算他不是出于私利，而是想改进合约的执行效率，或者改善条款，但大家是否都同意？

我们常举的例子：一个“借贷”智能合约可以规定一个利率算法，比如说年化5%；如果调整成为年化30%——表面上看，利率是借贷双方互相支付的成本，跟规则制定方的利益没有直接的关系；但也不能因为是中立方，就可以随便瞎改规则， 于是你需要给买卖双方一个“缓冲期”或者“冷静期”，或者一种投票的机制，可以让参与者共同决定。如果接受，投票通过，就可以修改规则。

如果参与者不接受，你还要改的话，那么你给我个冷却期，我要退场。所以最终整个逻辑还是完备的，还是要引入第三方的制约机制。我觉得这一点跟现有金融市场的一些规则也很类似。

小跑 20:42

这就是为什么需要专家解读。如果只看这四个字，会觉得就是个冷冰冰自动执行

的代码；但实际上背后还有一系列规则，而且这些规则大部分是可以映射到现实世界的。比如刚才的例子就很像一个“仲裁机制”。

既然如此，我们就在现实世界中找几个案例，分析一下在现实世界中出了问题的、让人挠头的情况，放在智能合约上，结果会不会不同？

我找了两个：一个是俄罗斯违约，一个是镍逼空。

先从俄罗斯开始。俄罗斯其实是个经常违约的国家，它主权债的违约次数是很频繁的：1918年沙皇帝国债券违约，1998年俄罗斯布雷迪债券几乎违约，最近俄乌战争，又把它带进另一个违约危险时期。

3月16号这一天俄罗斯两只美元债，要付1亿多美元的利息；付息前一个礼拜大家就开始担心，因为俄乌已经开打，它到底还有没有能力支付？如果支付用什么币种？用卢布吗？当时已经贬值20%。

结果是没有违约，危机暂时解除了。3月18号俄罗斯财政部已经还了，虽然晚了一天，不过仍然在30天宽限期内。但事情还没完，4月还有20多亿美元的本金偿还。所以到现在为止，会不会发生违约还是一个巨大的问号。

通常一个国家不愿意违约自己的主权债，主要原因是如果违约，市场会以某种方式惩罚你，比如失去信用，被评级机构贬为垃圾债，导致投资者在很长一段时间内不愿意碰，你就很难在市场上找钱。

但是一个国家违约的可能性实在太多了。上个世纪大量主权债的发行，其实都是为了资助战争，一旦战争爆发，肯定是要违约——因为钱都要拿去打仗。俄罗斯现在就是这么个情况，而且更棘手——不管是被动制裁，还是大家主动制裁，显然投资者已经不愿意碰了。俄罗斯基本与世界隔绝，也不能再失去更多信用，因为它几乎已经没有信用了；外汇储备被冻结，就算想还，去哪儿找美元、硬通货呢？

所以在这种情况下，“违约”这两个字究竟意味着什么？

在现实世界中，作为政府的债主，你其实是很难冻结或者强制出售一个国家资产的。这是一个信心加耐心的 游戏 ，如果你有本事在一个足够长的时间内，不停骚扰这个国家的政府，年复一年穷追猛打，就像当年保罗辛格为了追债，干脆把阿根廷的船给劫了。俄罗斯这个战斗民族不一样， 历史 经验表明，即使是最坚决的债权人，俄罗斯人也有足够的能力胜过，以死猪不怕开水烫的心态挡住所有追债。

这次还有个很有意思的地方： 这笔主权债中有一个条款，叫做“pari passu”—

—“一视同仁”原则。这是一个古老条款，一个多世纪前大家就用在债务合同中。它要求债务人对所有债权人要平等对待，不能厚此薄彼，只要跟其中任一个债主谈妥了，也要给予所有其他债主相同的偿还待遇。

自从保罗辛格利用了这个条款，向阿根廷政府讨债成功，之后大部分国家在发行主权债务时便删除了此条款——防止这些“钉子户”追债时再利用这个条款。

但是俄罗斯这笔债中却没有删除——要么是战斗民族太傲慢，觉得自己永远不会被起诉；要么就是忘了。 尽管如此，条款中关于“未来偿还“的字眼却神奇的消失了——是故意，也许是笔误，反正结果变成了：发行时会遵守“一视同仁”原则，所有债主都一样，但并不意味着“未来”还是一样的。

这个例子告诉我们，债券市场是一个完全由“样本文件”主导的“copy paste”交易，很少有人真的会看多达几百页的条款——但魔鬼也就在这里，人为的“调整”、“违约”空间太多了。

如果债发行在智能合约上，是不是就不会出现这种情况了？

王玮 28:09

这个案例特别有意思。本来还有点担心，因为区块链也好、智能合约也好，其实最不适合迎来解决债的问题。不过听了俄罗斯债务里的很多细节，又有好解决的地方了。

首先，“债务”这个东西，是一个典型的“信用”过程。从本质上，我把金融分为“信用过程”和“计算过程”两个部分。区块链、智能合约、DeFi等等，其实解决的是“计算性过程”的部分，而“债”是典型的“信用过程”。

实际上，“债券违约”这件事是最不适合于用智能合约去解决的。或者说，智能合约、区块链这些技术对于“债券违约”是最无能为力的——因为违约就是个信用丧失的过程， 就算用智能合约来写债务合约，但还债的过程涉及到还债主体，你需要把资产放入智能合约才能执行；不放进来，就执行不了。

这就回到最关键的一点：智能合约能保证自动执行的前提，是合约本身对标的物有“控制权”。但如果我未来才要还的钱——本金甚至是利息都要放在智能合约里，被它所控制，那我现在“借”钱干嘛呢？还得倒贴往里面放点利息。

在DeFi领域里，我们也看到非常多的项目和创业者，试图用智能合约来解决一个债务市场的问题，或者创建信用产品。其实没问题， 因为智能合约背后还可以有一

套其他的保障机制，比如投票等等；最终把“信用”部分转化为其他的保障机制，还是有可能的。

信用的“执行部分”不可能转化为代码层面的保障机制，但这不代表智能合约不能对债务市场有所改进。

在俄罗斯债务例子中，它把“一视同仁”条款中的“未来”字眼去掉，这是它的权利，没有办法控制；买债的人一不留神，没注意到改动就买了——这一点其实在智能合约层面可以有所改进。

首先， 智能合约作为代码规则写进来，天然就有“一视同仁”的条款，因为代码是人人都可以执行的。只要有地址，有代码固化在里面，天下人都可以执行，所以默认一定是会“一视同仁”的，你要是想不“一视同仁”，反而要去做很多手脚。

关于“债券市场是一个以模板为基础，copy paste的市场”——让我想起了过去几年，很多DeFi智能合约领域的“微创新”，也是把某些智能合约的代码全盘拷贝过来，然后改上两三个字。

但是你会发现在这种情况下，智能合约反而有价值了。为什么呢？

因为智能合约是精确的代码。一个审计机构是可以轻而易举找到改动之处的。几行代码的不同，意味着结果有什么差别，是可以精确推导和判断出来的。而在传统市场，因为自然语言是不精确的，就算让律师去审，我们也不知道这几句话改动的背后，是不是还隐含其他含义？或者导致什么意想不到的后果。

智能合约的审计机构是整个生态中非常重要的一方。这些机构往往是一些智能合约开发高手，或者白帽子黑客。他们的作用很像现实世界中的律师事务所，专门负责去审合同、审合约代码。

所以总结一下：智能合约不能解决债务的所有问题，但是它在债务的执行、和条款分析层面，仍有很大的作用。

小跑 35:47

所以我现在觉得可能俄罗斯这个案例，甚至整个主权债放在智能合约上，可能不太现实。因为对于本来就有意“不执行”的一方，可能根本不会签了。

这就引出了第二个案例：前些时候闹得沸沸扬扬的镍逼仓事件。

大概复盘一下：三八妇女节那天，市场上演了一个 历史 性的事件，我们在LME（伦敦金属交易所）市场上见证了史诗级的空头挤压。镍价创了有史以来最极端的价格波动，3月7日暴涨76%，达到每吨5万多美元；紧接着第二天突破一吨10万美元的关口。

这是一个明显的逼空。被逼仓的是青山——全球最大的镍生产商，在俄乌战争之前押错了方向。15万吨的镍空头头寸，其中5万吨是和摩根大通的OTC（场外）头寸；也就是说此刻青山已经欠JP大概10亿美金的保证金。

对于OTC的场外交易，其实大家还是有商量余地的，如果极端情况发生，各方会首先场外协商解决方法。这一次爆仓后，青山的经济上先向交易所垫付了保证金，不然清算会出现巨大问题。谈判的结果空头头寸先保留，之后LME“创造了 历史”，取消了交易，并且把镍的交易一直停到3月中旬。

从那一刻起，从全球市场的角度，LME的“信用”和“中立性”就出现了巨大的问号——突如其来的停牌影响了几千笔的交易，市场上其他参与方损失巨大。

这个案例，智能合约有可能在哪些环节会发生一些作用呢？

王玮 42:10

其实刚才在介绍智能合约的时候也提到了：我们确实可以“干预”智能合约，它并不是真的100%不能变。

从这个角度讲，LME的这种干预也可以算是“干预”的一种情况。但这里确实有一些问题：第一，智能合约的“干预”，必须要通过“有权限的人”去升级代码；或者直接去修改智能合约当中的参数来实现。这跟一个中心化的体系把交易“回滚”、“取消”还是有区别的。

智能合约的干预，不管是代码升级还是参数调整，它也只能是“向后干预”，改未来的规则，不能倒退回过去的某个阶段——区块链是不支持这种干预方式的。

当然，并不是说“向后干预”完全不能出现。举个例子，大家可能都听说过以太坊的DAO攻击事件，
为此以太坊发生了“硬分叉”——这确确实实是“回滚”，在以太坊的 历史 上就发生过这么一次。但是这次“回滚”的结果，是同时产生了ETC和ETH这两条链。

所以，在“计算性”的体系下，就算想要“回滚”，也不是100%的滚，因为仍然有人可以选择去执行那些没有被你“回滚”的合约。

但这在现实世界中没办法发生。 因为不可能有另一个平行世界的人，选择继续去成交被逼空的那些单，因为交易所只有一家，回滚就是回滚了，不会硬分叉出来两个交易所。

现实世界无法分叉，无法分叉出两个青山、两个俄罗斯、一吨镍变成二吨——两个平行世界中各一吨。这是物理世界决定的。所以智能合约、区块链这套体系，只能针对“纯数字资产”才有所谓的“保障执行”能力。

那LME这种“停止交易”、“取消交易”的情况，在智能合约领域能不能做到？

客观的说，也可以做到。一般可以通过两个手段： 第一个是投票。相当于LME的股东集体来投票，投票结果决定是否允许回滚，投票不通过就不能改。
这就是为什么现在的加密领域会推行“token economics”（通证经济学）体系，这是一套类似于股权的模型，投票结果可以绑定智能合约，自动执行结果。

第二，投票意味着什么？数字世界里的投票，是个“刚性”的结果——51%的人同意就改，但这不会引起“多数人的暴政”吗？49%的人不同意，也只能接受吗？投票不能解决问题怎么办？

答案是设定 “冷静期”或者“过渡期”——几天、几小时都可以。就算投票通过，也只能冷静期之后才能执行。不想玩的，就在这段时间内从系统里退出。改规则没有问题，但要给我离开的自由——这是最基本的自由了。

LME的做法，就是典型的“中心化”系统的弊端——就算要改规则，第一能不能让大家投个票？受到规则影响的人，起码要给一个发言的机会。第二，就算投票通过，也要给一些时间之后再改。

如果用智能合约来实现，并且遵守刚才的那套治理规则，它的信用程度肯定更高。所以从这个角度讲，智能合约在维护一个公平高效、更高信任的市场规则，是会有比较大用途的。

小跑 50:51

是的。虚拟世界中的一些机制也可以用到现实世界。
但是这些投票、冷静期等等规则有多大可实施性呢？

比如多数人的暴政。如果大家突然意识到有“多数人暴政”的可能性，比如我仇富，反正大家都是市场的韭菜，我们以数量取胜，联合起来投票，把大户账户里的钱全都转到我们账户来——如果真的按投票结果来自动执行，不是相当于“合理抢

劫”吗？

但是如果设了冷静期，15天之后再正式“执行打劫”，大户肯定会离开，总不能等着被打劫。可是大户都已经离开了，我15天之后还打劫谁呢？整个 游戏 就没有存在的意义了？

王玮 52:17

这就是区块链和加密货币的一个核心理念——就是你的行为要有经济上的合理性。

如果小散这么做，就是损人不利己。不仅没有得到钱，唯一的结果是毁灭了这个平台的价值、信用。在这种情况下，你会发现小散也没有那么傻，他们知道自己投这个票是没有意义的。

这就回到中本聪写比特币白皮书中提到的，你可以51%的算力攻击，把比特币全拿到自己手里，但是比特币也因此归零了——你买的那些机器成本也回不来了，这对你有什么好处呢？

所以某种意义上，“经济模型”是区块链领域最核心的“模因”。我们维护的这套经济模型的合理性，导致攻击是没有意义、不合理的。

小跑 54:11

我现在觉得其实任何规则和机制，虽然看起来像是补救措施，但实际上它发挥最大作用的时间——还是在事情发生之前。

大家的行为会在博弈影响下，自动找到一个最理性、“守规矩才能价值最大化”的结果来走。也就是说好的事前设计，会导致一个理性的结果。

王玮 55:13

智能合约和区块链最核心的价值，其实是“维护规则的有效性”。更适用于平台经济、或者双边市场的逻辑。 区块链和智能合约的创造者，是规则的制定者和维护者，本身并不一定是参与方。而参与方是世界上互不认识的人，共同参与 游戏 。

如果两个人认识、签一个合同、互换了合同文本、以及后续都有意愿保障执行——那这个场景下，智能合约没有太大意义。

小跑 56:55

非常同意。大家可能有各种通关升级办法，但是整个 游戏
规则大框架是可以用智能合约改进的。

— End —

播客《文理两开花》

中本聪发明了比特币。

2008年11月1日，一个自称中本聪的人在P2P foundation网站上发布了比特币白皮书《比特币：一种点对点的电子现金系统》，陈述了他对电子货币的新设想——比特币就此面世。

2009年，中本聪设计出了一种数字货币，即比特币，风风火火的比特币市场起了又落，而其创始人“中本聪”的身份一直都是个谜，关于“比特币之父”的传闻牵涉到从美国国家安全局到金融专家，也给比特币罩上了神秘光环。

扩展资料：

从比特币的本质说起，比特币的本质其实就是一堆复杂算法所生成的特解。特解是指方程组所能得到有限个解中的一组。而每一个特解都能解开方程并且是唯一的。

以钞票来比喻的话，比特币就是钞票的冠字号码，你知道了某张钞票上的冠字号码，你就拥有了这张钞票。

而挖矿的过程就是通过庞大的计算量不断的去寻求这个方程组的特解，这个方程组被设计成了只有 2100 万个特解，所以比特币的上限就是 2100 万个。

参考资料来源：百度百科——比特币

央视网消息： 商务部14日发布了《关于印发全面深化服务贸易创新发展试点总体方案的通知》，其中公布了数字人民币试点地区。目前，数字人民币试点仍是“4+1”，即先行在深圳、苏州、雄安新区、成都及未来的冬奥场景进行内部封闭试点测试，并没有变化。相关人士指出，网上传的北京、天津、上海等28个试点其实是全面深化服务贸易创新发展试点。

数字人民币到底是啥？

当前，不少国家都在进行法定数字货币的研究，但在技术路线、运行体系、投放路径上各有不同。我国法定数字货币是人民银行把数字货币和电子支付工具结合起来，目标是替代一部分现金。那么，数字人民币到底是啥？

简单说，人民银行数字货币就是人民币电子版，把数字货币看做数字化的人民币现金就不难理解数字货币的概念了。说起数字货币，大家第一反应可能是比特币，但实际上，它们之间有着本质的区别。像比特币、“天秤币”这样的虚拟货币，它本质是一种虚拟商品，它没有国家信用，不具有法偿性。而人民银行数字货币是以国家信用为担保的一种法定货币，在这一点上它跟现金是具有同样的效力的。

数字人民币怎么用？

随着移动支付深度融入我们的日常生活，对于数字人民币的使用场景应该并不陌生。那么，数字人民币到底怎么用？跟我们习惯的微信、支付宝等电子支付手段有区别吗？

从使用场景上看，央行数字货币不计付利息，可用于小额、零售、高频的业务场景，与使用纸币差别不大。不仅如此，央行的数字货币使用最新的双离线技术，即使在没有手机信号的情况下依然可以使用。

未来现金是否会被取代？

有了数字人民币，是不是就意味着未来现金将会被取代了？专家表示，未来央行数字货币会替代一部分的现金，但不会全部取代纸币。

国家金融与发展实验室特聘研究员董希淼称，在我国，纸币将长期存在，对我国这样一个幅员辽阔、经济发展水平不一的一个大国，我们的用户习惯也各有不同，现金支付、非现金支付将长期共存。

与此同时，央行发行的数字货币是从替代流通中的纸钞和硬币入手，也就是说假设现在流通的货币是100元，央行数字货币将等价替换掉这100元。

北京大学数字金融研究中心高级研究员徐远称，新的数字货币和我们以前的纸币是一对一兑换的，所以说现在商业银行要获得这个数字货币怎么办呢？必须拿以前的货币来换，并不增加总量，这是第一步，试点的时候并不增加总量。

啥时能用上数字人民币？

那么，我们到底什么时候能见到数字人民币的真面目？目前，数字人民币先行在深圳、苏州、雄安新区、成都及未来的冬奥场景进行内部封闭试点测试。如果顺利的话，北京2022年冬奥会上也许能“一睹芳容”。但数字货币的真正投放使用还需要检验理论可靠性、系统稳定性、风险可控性等多项环节，央行也多次表态，数字人民币尚没有推出的时间表。不过，我们期待不远的将来能用上便捷的数字人民币。

中新经纬客户端7月26日电 题：《黄震：数字货币发行绕不过的坎》

作者 黄震(中央 财经 大学教授、金融法研究所所长，中新经纬特约专家)

最近，脸书宣布将开发稳定币Libra及其配套钱包Calibra，声称其使命是建立一套简单的、无国界的货币和为数十亿人服务的金融基础设施。脸书作为全球最大的社交网络平台，准备动用其丰富的资源推出特别宏大的发币计划，或许将实现超主权货币与创新性技术结合，这再一次激发了颠覆世界货币金融体系的无限想象。

为什么会出现上述这种状况？首先，脸书作为全球最大的社交平台拥有庞大的活跃用户数量，一旦发币成功，将会出现前所未有的规模效应。其次，Libra白皮书中提到的应用场景、使用范围、商圈规模极其庞大，它让数字货币不再只是停留在虚拟空间，而是有更多实体场景应用。再次，更令人吃惊的是，Libra的发币计划有非常多的主流金融机构参与，特别是Visa、Mastercard等国际知名支付机构也踊跃参与，因此Libra融入主流金融市场的可能性更大。其四，脸书发币计划居然得到了美联储的默许。时至今日，美联储没有对Facebook发币计划表示反对。

针对脸书的发币计划，我们没有必要过度恐慌和过度解读，而应该进行理性反思和预测分析，提出对于数字货币现象的理论分析框架和未来全球监管框架。

从 历史 来看，数字加密货币虽然只有大约十年的时间，但是，十年间数千种数字加密货币，在没有主权国家监管控制下，如同脱缰野马一路狂奔。尤其是比特币，在各种力量炒作下价格暴涨、暴跌，堪称世界金融史上的罕见现象。比特币、以太坊等的应用范围主要局限于虚拟空间，而这一轮由脸书即将发行加密数字货币引发的大讨论，则意味着数字货币可能会进入一个新的阶段。

脸书的发币计划，是由在实体空间非常具有影响力的机构来发行数字加密货币，并且有金融机构参与其中，这将在全球范围具有极大的示范效应。如果监管当局放任其行动，拥有各种资源条件的各界大佬就可能竞相仿效，进行监管套利，由实体空间转向发行数字加密货币，可能会抢走主权国家的铸币权，导致主权国家损失铸币税，冲击现行的主权国家货币体系和国际货币体系，所以数字加密货币问题显得格外严峻。

在数字加密货币的冲击下，传统货币理论乃至整个金融理论也遭受了巨大挑战。在传统金融理论里，货币的国家化是大家习以为常的事情。货币是以国家信用背书，以国家主权强制力保障实施的一种交易凭证，近代以来已经为各国主权所控制。但是，由于主权国家往往超发、滥发货币，常常导致严重的通货膨胀，国民财富遭受损失，以及经济 社会 动荡不安。

对于各国货币当局的超发、滥发问题，很多经济学家表示了不满，也试图提出新的解决方案。其中最具代表性的理论是由哈耶克提出的货币非国家化。他指出在主权国家控制之下的信用货币超发问题是其自身无法克服的，因此应该回到货币发行的非国家化道路，比如让企业来发行货币，或让其他市场主体来发行货币。这种设想曾经激发了很多人的想象，但是一直没有找到实现方案。直到比特币的横空出世，让人们又看到了哈耶克的货币非国家化主张实现的希望。

过去的百年 历史 中，如何让货币的币值稳定？在金本位崩溃之后世界各国一直没有很好地解决这一问题。虽然有学者呼吁回归金本位，然而要回到金本位已经不可能。还有货币的寻锚问题，锚定什么样的资产才能够让货币的币值稳定？货币发行数量如何与经济发展相匹配和相适应？传统货币理论的一系列问题，在数字加密货币领域依然有待解决。

虽说比特币在其名字上冠以“币”之称，但实际上监管当局还是把它视为一种数字资产或一种虚拟货币，并不是严格意义上的货币。既然货币的金本位无法回去了，货币的发行也绕不开主权国家，那么究竟该如何来评判脸书的这种发币行为，以及对它进行下一步的预测？我们可着重从以下几个方面进行思考。

第一，数字货币是全球经济金融发展的大势所趋，任何主权国家都不能回避也无法回避。目前市面上的数字加密货币主要由互联网企业发行，并且已经形成相当大的用户规模，虽然主权国家不承认其为货币，但是事实上，它已经具备了私币特点，在一些商圈发挥了巨大作用。

第二，主权国家发行数字货币必须尽快提上议事日程，才能应对数字加密货币抢夺铸币权的挑战。主权国家是否能够推出数字货币，何时推出数字货币，推出的路径是什么等问题应该尽快研究解决。

第三，数字货币具有全球化和超主权的特征。全球化的超主权数字货币究竟由谁来主导，如何进行监管？当前各主权国家面临着重大决择。是任由比特币、Libra等发展成为事实上的世界货币或超主权的全球货币，还是由主权国家来主导、 探索形成全球货币或者世界货币？世界各国应该通力合作共同探讨解决。

就目前而言，Libra想要绕过主权国家几乎是不可能实现的跨越。如果Libra成为所

谓超主权的全球货币，那么必然会触动美国的货币政策和美元地位，乃至其他主权国家的利益，引起主权国家的抵抗。美国国会已经有议员提出对于Libra发币计划进行质询。未来，Libra发行计划是否行得通，取决于美国政府以及其他主权国家金融监管政策，以及由主权国家组成的国际货币组织的态度。

基于对以上问题的分析，对于未来全球数字货币的发展道路，笔者认为有如下三种方案可以讨论。

第一种方案：对比特币、以太坊乃至将来的Libra进行收编，将来逐步纳入监管，也就是所谓的“染色方案”。对事实上已经具有世界影响的全球货币或世界货币进行收编认可，由各主权国家逐渐纳入监管轨道。目前具备前提条件，但收编或染色有很多技术问题需要解决，主权国家对这一方案的认可有难度。

第二种方案：由现行国际货币基金组织或类似的组织发行超主权的国际货币或者全球货币。国际货币基金组织在Libra推出计划之后，也声称即将推出IMFCoin。在当前国际货币基金组织一揽子计划中推出数字货币，即中国学者姚余栋和杨涛提出的eSDR方案，或许是当前条件下数字货币推进的最佳选择。

第三种方案：由各主权国家发起创设新的数字货币国际组织，推动发行全球性的数字货币。或者，主要数字货币发行机构主动与主权国家监管当局合作，共同发起全球性质的数字货币国家组织。但是，创设新的国际组织合作协调尚需时日。

黄震

文/肖小跑

面向未来最好的姿势是问问题，问问题最好的态度是从自己最熟悉的领域问起——于是有了这篇 “未来金融三问”
。也许不太成熟，但都是我自己想了很久的问题。

1. 最有前（钱）景的地方在哪里？

我入行时的“职场圣经”是Michael Lewis老师的 《说谎者的扑克牌》 。

书中有一段，描述他拿到Salomon
Brothers债券销售的offer，第一天去报道时的感觉：

“并不像是去上班，而更像是去领彩票奖金” 。

人生第一份工作直接抛给他了一袋子金砖——他的工资是自己LSE（伦敦政治经济学院）教授的两倍多。教授年近50，已经站在了自己领域的顶峰；而他24岁，刚摸着山脚的第一块石头。

他的结论是：这个世界没有“公平”。

1985年的华尔街是世界上最有前（钱）景的地方，Salomon Brothers是当年街上最handsome的boy。后面的几十年里，“金融投行”就像希腊神话中的弥达斯，点石成金（弥达斯的触摸，The Midas touch），从华尔街到伦敦金融城到香港再到上海，它触到的东西都会变成金子。

三十多年后的今天，这个行业依然是金色的——全球金融业界共同经历了有史以来最赚钱的一年。2022年也许还有更大的红包。

但“中彩票”的惊喜感已经没有了，《说谎者的扑克牌》、《华尔街之狼》中那些“没有明天”的狂欢消失了，空气中弥漫着一种说不出的“中年疲乏感”——明天还要面对没完没了的监管，和经济学家们无时不刻不在提醒我们的“酝酿中大危机”。真正的乐趣已经不在这里了，在“别处”。

为什么曾经的金融业界会有那么巨大的虹吸力？

绝不仅仅是因为赚得多， 更因为它是一台能将“聪明”转化为“金钱”的大机器。在这里，总有人会因为解决了一个钱的难题、把一个精妙的设计变成现实、或升级成市场 游戏 高阶玩家而变得富有。《大空头》里的MBS、CDS、CDS平方、tranche、高斯定理、奇异期权这些工科天才们的杰作，虽然被贴上了“贪婪”的标签，但谁没有私下偷偷赞叹过“真牛逼”？

但这已经是“过去”了。现在的并购和投行从业者，感觉就是普通打工人。而那台神奇的机器，被搬进了市值2万亿美元的加密业界。曾经投行精英的金手指，长在了币圈、DeFi、web3开发者、和迷因NFT的“钻石手”（diamond hand）上。

空气中弥漫着一种无法言说的嫉妒、FOMO和的抑郁。

所以钱景已经从金融进入了加密行业了吗？

我的答案是否定的。证据在一首唐诗里： “商人重利轻别离，前月浮梁买茶去”。

和“商人”一样， “华尔街皈依者”其实是一个符号 ，无关领域。它代表一类特殊群体，他/她们心跳的动力来自于“波动”——茶叶、菜市场里的大葱、股票、大宗商品、债……当然还有比特币。他/她们有一门“手艺” ，能够承受任何波动、能适应任何错综复杂的市场结构。

三十年前，这个群体在大宗商品市场上享受过的所有快乐，啪，现在都没了。蓦然回首，发现快乐的影子嬉笑着，躲进了加密行业。那些在传统市场里，被“低利率” 、 “监管” 、 “冷兵器内卷”而废了武功的旧策略，都在这里重获了新生。

比如高频做市：这个在股市和大宗商品市场上近乎寡头的行业，在加密货币领域，羊毛遍地，就一把小手枪就可以“打着枣，吃到饱” 。

还有“泡菜溢价” （泡菜溢价——每次牛市，韩国人民对加密货币的强烈需求 ，都会把价格推得比别国高，是为“泡菜溢价” ）、期现套利、日间动量、统计套利。

一年又一年，只要人类依然是“单向度”的人，价值评价体系依然是“增长” ，前（钱）景就会继续向那些可以用杠杆和衍生品来“套现时间”的地方移动。

结局依然是卷。这便是“单向度人间”的必然归宿。

2. 到底什么才是“价值” ？

我们都渴望得到有“价值”的资产，拥有财富。
但“价值”是什么呢？它是真实存在的吗？

不管你的财富成分是什么，它们的“价值”映射在你心中，大概率都是价格标签上那一串“数字” 。 你拥有资产的“价值” ，只是电子屏幕上显示的数字。

“价值”看不见摸不着，不能吃不能喝，也不能对它拳打脚踢；但你仍然可以“讨论”它，用它来衡量现实世界存在的意义。

哲学中的 “唯名论” （normalist）有分教：概念不是“真实存在” ，只是谈论“真实存在”时用的“符号”和“标签” ——除了便于逻辑推理，它其实什么也不是。 而我们和动物最重要的区别，就是“人”可以相信、思考、和讨论虚构的概念，也能自己“构建”出一个世界。

“价值”也只是一个符号。你坚信的“价值”，其实是人类自己的“构建”出来的。

太抽象了。好在币圈这个神奇的地方，经常可以给你莫名其妙的启发。

去年最火的剧是《鱿鱼 游戏 》。跟着它一起爆红的，还有一款叫做SQUID（鱿鱼币）的项目。去年10月开始，它的价格一周内飙升了23万倍；然后在一个月后光速归零。

鱿鱼币是个骗局。虽然这又是一场对韭菜智商的侮辱，但其中的“反跌”设计，却奇怪地让我明白了“价值”这件事的本质：

鱿鱼币的经济模型中有一个 “反跌”（anti-dumping）的设计。买它不难，但是“卖”需要满足一些条件：

一句话总结：这是一款“买了就卖不出去的”东西。

此设计的目的昭然若揭，就是要把“卖”这个动作扼杀在摇篮中——当“买压”远远大于“卖压”，一周飙升23万倍并不是一件太难的事情。

这个案例让我此起彼伏。 “买压大于卖压” 这句话太熟悉了。不管您持有什么品类的“价值”——房子、股票、还是比特币，每当它们价签上的数字增加时，一定会有专家解读：价格上涨是因为“买家比卖家多”。

这其实是一句很正确的废话： 因为“买家比卖家多”和“涨了”是一个意思。

每个交易发生时，这笔交易中都只有一个（成交的）买家和一个（成交的）卖家。所以理论上，在某一个价格上的“买家”永远不会多于“卖家”。而如果一个卖家都没有，交易根本不会发生，也就不会有价格。

所以“买家多于卖家”的意思是：由于看到了某种“价值”，想 “拥有它”的热情更高，有更多的人愿意出价得到它——这曾经是岁月静好的时代里，我们默认的常识。

而鱿鱼币却像灭霸一样，生生地把“卖家”的人数消灭掉了一半，强制要求“买入”的数量永远多于“卖出”——于是“价值”这件事就变成了一个纯粹的数字游戏 ：

只要所有人都“买”某个东西，然后齐心协力“hold”住这个东西不卖，让“买

入”的数量永远多于“卖出”，它的价格就一定会上涨，我们就一定会发财——而这个东西到底是什么，不管是jpeg文件、GameStop一样的垃圾股票、还是狗币，都和“价值”、“上涨”、“发财”没上述文章内容就是系。

于是一个新的价值理论出现了。或者应该说是一种“新常识”和信念——这种信念的名字是“钻石手（diamond hand）”，“HODL”，以及上一篇文章（《里拉“荣誉谋杀”》）提到的（3,3）博弈最优解。

只是有一个逻辑上的小问题：如果不卖，这些”价值“就会永远留在“纸面”上。一旦试图变现，从“hold”阵营到了“卖”的阵营，“价值”就有可能会崩溃。

当然，除非这个东西已经有了规模效应。如果你在10年前用100美元买了一大堆比特币，十年后的今天卖掉一两个就可以实现财富，且“卖两个比特币”的动作对其当前价格不会产生任何影响——比特币就变成了一种价值存储。

仔细想想，世界上大部分“价值”似乎都是这么诞生的。“只能买不能卖”——可以被解读为骗局，也可以被解读为“需求”。而需求就是价值。

3. 货币体系的灵魂拷问

最后一问是来自王玮老师的 货币灵魂三问（节目全文）：

信用货币体系，尤其是”央行—商业银行”二元货币体系是人类 社会 迄今为止最合理的模型。如果颠覆掉它，用任何其他模型都回答不好三个问题。我们必须有一个“信用创造”机制，否则会陷入比通胀更悲惨的境地。

我都同意。只是： 我们是不是还要往前看？

人类 社会 已经经历过的、以及它未来将经历的东西也许是不同的。我们已经经历过一个必须利用信用货币体系来实现人类富足、保持基本物质生活水平无忧的时代。过去几十年，信用货币体系确实使地球上几十亿人口实现了物质生活保障，以至于新冠这么多年，大家大概率还是可以无忧无虑的生活，甚至到了大概率不会再出现生存问题的阶段。

如果人类已经到了这个阶段，再往后，我们还需要这么大的信用程度来支持“集中力量办大事”的机制吗？或者，我们已经实现了 历史 阶段性目标， 下个阶段是不是不再需要信用乘数来支持发展，而是倒过来，换成从主动脉到毛细血管的发展模式？

如果是这样的话，是不是真的需要一种“点对点”的、信息和价值完全绑定的货币体系？

下个阶段最理想的货币体系虽然还没出现，但至少知道现在的货币体系是有问题的——这个世界需要多少钱？明显是太多了。

我们已经习惯了“线性”思维，觉得一次只能有一个世界、一种形态。如果当下的体系发展到一定阶段，出现了某种巨大问题，它才会迭代成为另一种更好的“新形态”。然后接着再往前迭代。

但是如果现实和虚拟世界开始“并行发展”呢？会不会在信用货币发展的同时，有另外一种“自下而上”的形态同时发展？

在我有生之年，“现实世界”大概率依然会干预到“虚拟世界”。元宇宙到底长什么样子我不知道，但“现实人类 社会 ”里，一定可以找到镜子。

— End —

比特币（BitCoin）的概念最初由中本聪在2009年提出，根据中本聪的思路设计发布的开源软件以及建构其上的P2P网络。比特币是一种P2P形式的数字货币。点对点的传输意味着一个去中心化的支付系统。

与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个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，并使用密码学的设计来确保货币流通各个环节安全性。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。比特币与其他虚拟货币最大的不同，是其总数量非常有限，具有极强的稀缺性。该货币系统曾在4年内只有不超过1050万个，之后的总数量将被永久限制在2100万个。

比特币可以用来兑现，可以兑换成大多数国家的货币。使用者可以用比特币购买一些虚拟物品，比如网络 游戏 当中的衣服、帽子、装备等，只要有人接受，也可以使用比特币购买现实生活当中的物品。[1][2]

西维吉尼亚州民主党参议员乔·曼钦（Joe Manchin）2014年2月26日向美国联邦政府多个监管部门发出公开信，希望上述文章内容就是机构能够就比特币鼓励非法活动和扰乱金融秩序的现状予以重视，并要求能尽快采取行动，以全面封杀该电子货币。[3]

2017年1月24日中午12：00起，中国三大比特币平台正式开始收取交易费。[4]

中文名

比特币

外文名

Bitcoin

种类

电子货币

流通平台

网络

概念创始人

中本聪

发展历程 听语音

2008年爆发全球金融危机，当时有人用“中本聪”的化名发表了一篇论文，描述了比特币的模式。

共2张

比特币

和法定货币相比，比特币没有一个集中的发行方，而是由网络节点的计算生成，谁都有可能参与制造比特币，而且可以全世界流通，可以在任意一台接入互联网的电脑上买卖，不管身处何方，任何人都可以挖掘、购买、出售或收取比特币，并且在交易过程中外人无法辨认用户身份信息。[2]2009年，不受央行和任何金融机构控制的比特币诞生。[2]比特币是一种“电子货币”，由计算机生成的一串串复杂代码组成，新比特币通过预设的程序制造，随着比特币总量的增加，新币制造的速度减慢，直到2014年达到2100万个的总量上限，被挖出的比特币总量已经超过1200万个。[2]

每当比特币进入主流媒体的视野时，主流媒体总会请一些主流经济学家分析一下比特币。早先，这些分析总是集中在比特币是不是骗局。而现如今的分析总是集中在比特币能否成为未来的主流货币。而这其中争论的焦点又往往集中在比特币的通缩特性上。[5]

不少比特币玩家是被比特币的不能随意增发所吸引的。和比特币玩家的态度截然相反，经济学家们对比特币2100万固定总量的态度两极分化。[6]

凯恩斯学派的经济学家们认为政府应该积极调控货币总量，用货币政策的松紧来为经济适时的加油或者刹车。因此，他们认为比特币固定总量货币牺牲了可调控性，而且更糟糕的是将不可避免地导致通货紧缩，进而伤害整体经济。奥地利学派经济学家们的观点却截然相反，他们认为政府对货币的干预越少越好，货币总量的固定导致的通缩并没什么大不了的，甚至是 社会 进步的标志。

比特币网络通过“挖矿”来生成新的比特币。所谓“挖矿”实质上是用计算机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。比特币网络会自动调整数学问题的难度，让整个网络约每10分钟得到一个合格答案。随后比特币网络会新生成一定量的比特币作为赏金，奖励获得答案的人。

2009年比特币诞生的时候，每笔赏金是50个比特币。诞生10分钟后，第一批50个比特币生成了，而此时的货币总量就是50。随后比特币就以约每10分钟50个的速度增长。当总量达到1050万时(2100万的50%)，赏金减半为25个。当总量达到1575万(新产出525万，即1050的50%)时，赏金再减半为12.5个。[7]

首先，根据其设计原理，比特币的总量会持续增长，直至100多年后达到2100万的那一天。但比特币货币总量后期增长的速度会非常缓慢。事实上，87.5%的比特币都将在头12年内被“挖”出来。所以从货币总量上看，比特币并不会达到固定量，其货币总量实质上是会不断膨胀的，尽管速度越来越慢。因此看起来比特币似乎是通胀货币才对。

然而判断处于通货紧缩还是膨胀，并不依据货币总量是减少还是增多，而是看整体物价水平是下跌还是上涨。整体物价上升即为通货膨胀，反之则为通货紧缩。长期看来，比特币的发行机制决定了它的货币总量增长速度将远低于 社会
财富的增长速度。

凯恩斯学派的经济学家们认为，物价持续下跌会让人们倾向于推迟消费，因为同样一块钱明天就能买到更多的东西。消费意愿的降低又进一步导致了需求萎缩、商品滞销，使物价变得更低，步入“通缩螺旋”的恶性循环。同样，通缩货币哪怕不存入银行本身也能升值（购买力越来越强），人们的投资意愿也会升高， 社会 生产

也会陷入低迷。[5]因此比特币是一种具备通缩倾向的货币。比特币经济体中，以比特币定价的商品价格将会持续下跌。[1]

比特币是一种网络虚拟货币，数量有限，但是可以用来套现：可以兑换成大多数国家的货币。你可以使用比特币购买一些虚拟的物品，比如网络 游戏 当中的衣服、帽子、装备等，只要有人接受，你也可以使用比特币购买现实生活当中的物品。[1] [1]

2014年9月9日，美国电商巨头eBay宣布，该公司旗下支付处理子公司Braintree将开始接受比特币支付。该公司已与比特币交易平台Coinbase达成合作，开始接受这种相对较新的支付手段。

虽然eBay市场交易平台和PayPal业务还不接受比特币支付，但旅行房屋租赁社区Airbnb和租车服务Uber等Braintree客户将可开始接受这种虚拟货币。Braintree的主要业务是面向企业提供支付处理软件，该公司在去年被eBay以大约8亿美元的价格收购。

2017年1月22日晚间，火币网、比特币中国与OKCoin币行相继在各自官网发布公告称，为进一步抑制投机，防止价格剧烈波动，各平台将于2017年1月24日中午12：00起开始收取交易服务费，服务费按成交金额的0.2%固定费率收取，且主动成交和被动成交费率一致。[4]5月5日，OKCoin币行网的最新数据显示，比特币的价格刚刚再度刷新 历史 ，截止发稿前最高触及9222点高位。[8]

创始人物 听语音

2008年11月1日，一个自称中本聪（Satoshi Nakamoto）的人在一个隐秘的密码学评论组上贴出了一篇研讨陈述，陈述了他对电子货币的新设想——比特币就此面世，比特币的首笔交易完成。比特币用揭露散布总账摆脱了第三方机构的制约，中本聪称之为“区域链”。用户乐于奉献出CPU的运算能力，运转一个特别的软件来做一名“挖矿工”，这会构成一个网络共同来保持“区域链”。这个过程中，他们也会生成新货币。买卖也在这个网络上延伸，运转这个软件的电脑真相破解不可逆暗码难题，这些难题包含好几个买卖数据。第一个处理难题的“矿工”会得到50比特币奖赏，相关买卖区域加入链条。跟着“矿工”数量的添加，每个迷题的艰难程度也随之进步，这使每个买卖区的比特币生产率保持约在10分钟一枚。

京都大学数学教授望月新一

2009年，中本聪设计出了一种数字货币，即比特币，风风火火的比特币市场起了又落，而其创始人“中本聪”的身份一直都是个谜，关于“比特币之父”的传闻牵

涉到从美国国家安全局到金融专家，也给比特币罩上了神秘光环。

据外媒报道称，计算机科学家TedNelson周日在网络上发布视频称，他已经确定出，比特币的创始人是京都大学数学教授望月新一（ShinichiMochizuki）。比特币的创始人一直以来使用的都是中本聪（SatoshiNakamoto）的假名，互联网领域也对其真实身份展开了大量推测。纳尔逊发布视频称，他已确定望月新一就是比特币的真正创始人。[9]

望月新一2013年因为证明ABC猜想而名声大噪。他高中时就读于菲利普埃克塞特学院，后者是美国最具声望的高中之一，仅仅两年后就毕业。望月新一16岁进入美国普林斯顿大学，22岁时以博士身份离校，33岁就成为正教授，这么年轻就获得正教授职称在学术界极为罕见。这个数学界的巨星可能已经攻破了该领域最为重要的难题之一。

中本聪本人在互联网上留下的个人资料很少，尤其是近几年几乎完全销声匿迹，因此其身世也变成了一个迷。2014年3月7日，当比特币创始人多利安·P·中本聪被找到的新闻传出后，迅速成为互联网上最吸引人的消息。

与外界揣测其可能是个虚构的名字不同，“中本聪”是个真实的名字，他是一名64岁的日裔美国人，他喜欢收集火车模型，曾供职大企业和美国军方，从事机密工作。在过去的40年中，中本聪从不在生活中用他的真名。根据美国洛杉矶地方法院1973年的档案，在他23岁从加州州立理工大学毕业时，将自己的名字改为了多利安·普伦蒂斯·中本聪（DorianPrenticeSatoshiNakamoto）。从那时起，他不再使用“聪”这个名字，而用多利安·中本S（DorianS.Nakamoto）作为签名。[9]

产生原理 听语音

从比特币的本质说起，比特币的本质其实就是一堆复杂算法所生成的特解。特解是指方程组所能得到无限个（其实比特币是有限个）解中的一组。而每一个特解都能解开方程并且是唯一的。[10]以人民币来比喻的话，比特币就是人民币的序列号，你知道了某张钞票上的序列号，你就拥有了这张钞票。而挖矿的过程就是通过庞大的计算量不断的去寻求这个方程组的特解，这个方程组被设计成了只有 2100 万个特解，所以比特币的上限就是 2100 万。[10]

疯狂涨势

要挖掘比特币可以下载专用的比特币运算工具，然后注册各种合作网站，把注册来的用户名和密码填入计算程序中，再点击运算就正式开始。[11]完成Bitcoin客户端安装后，可以直接获得一个Bitcoin地址，当别人付钱的时候，只需要自己把地址贴

给别人，就能通过同样的客户端进行付款。在安装好比特币客户端后，它将会分配一个私有密钥和一个公开密钥。需要备份你包含私有密钥的钱包数据，才能保证财产不丢失。如果不幸完全格式化硬盘，个人的比特币将会完全丢失。

货币特征 听语音

去中心化：比特币是第一种分布式的虚拟货币，整个网络由用户构成，没有中央银行。去中心化是比特币安全与自由的保证 。

全世界流通：比特币可以在任意一台接入互联网的电脑上管理。不管身处何方，任何人都可以挖掘、购买、出售或收取比特币。

专属所有权：操控比特币需要私钥，它可以被隔离保存在任何存储介质。除了用户自己之外无人可以获取。

低交易费用：可以免费汇出比特币，但最终对每笔交易将收取约1比特分的交易费以确保交易更快执行。

无隐藏成本：作为由A到B的支付手段，比特币没有繁琐的额度与手续限制。知道对方比特币地址就可以进行支付。

跨平台挖掘：用户可以在众多平台上发掘不同硬件的计算能力。

优点

完全去处中心化，没有发行机构，也就不可能操纵发行数量。其发行与流通，是通过开源的p2p算法实现。

匿名、免税、免监管。

健壮性。比特币完全依赖p2p网络，无发行中心，所以外部无法关闭它。比特币价格可能波动、崩盘，多国政府可能宣布它非法，但比特币和比特币庞大的p2p网络不会消失。

无国界、跨境。跨国汇款，会经过层层外汇管制机构，而且交易记录会被多方记录在案。但如果用比特币交易，直接输入数字地址，点一下鼠标，等待p2p网络确认交易后，大量资金就过去了。不经过任何管控机构，也不会留下任何跨境交易记录。

山寨者难于生存。由于比特币算法是完全开源的，谁都可以下载到源码，修改些参数，重新编译下，就能创造一种新的p2p货币。但这些山寨货币很脆弱，极易遭到51%攻击。任何个人或组织，只要控制一种p2p货币网络51%的运算能力，就可以随意操纵交易、币值，这会对p2p货币构成毁灭性打击。很多山寨币，就是死在了这一环节上。而比特币网络已经足够健壮，想要控制比特币网络51%的运算力，所需要的cpu/gpu数量将是一个天文数字。

缺点

交易平台的脆弱性。比特币网络很健壮，但比特币交易平台很脆弱。交易平台通常是一个网站，而网站会遭到黑客攻击，或者遭到主管部门的关闭。

交易确认时间长。比特币钱包初次安装时，会消耗大量时间下载 历史 交易数据块。而比特币交易时，为了确认数据准确性，会消耗一些时间，与p2p网络进行交互，得到全网确认后，交易才算完成。

价格波动极大。由于大量炒家介入，导致比特币兑换现金的价格如过山车一般起伏。使得比特币更适合投机，而不是匿名交易。

大众对原理不理解，以及传统金融从业人员的抵制。活跃网民了解p2p网络的原理，知道比特币无法人为操纵和控制。但大众并不理解，很多人甚至无法分清比特币和Q币的区别。“没有发行者”是比特币的优点，但在传统金融从业人员看来，“没有发行者”的货币毫无价值。[12]

货币交易 听语音

购买方法

用户可以买到比特币，同时还可以使用计算机依照算法进行大量的运算来“开采”比特币。在用户“开采”比特币时，需要用电脑搜寻64位的数字就行，然后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，如果用户的电脑成功地创造出一组数字，那么就将会获得25个比特币。

由于比特币系统采用了分散化编程，所以在每10分钟内只能获得25个比特币，而到2140年，流通的比特币上限将会达到2100万。换句话说，比特币系统是能够实现自给自足的，通过编码来抵御通胀，并防止他人对这些代码进行破坏。

交易方式

比特币是类似电子邮件的电子现金，交易双方需要类似电子邮箱的“比特币钱包”和类似电邮地址的“比特币地址”。和收发电子邮件一样，汇款方通过电脑或智能手机，按收款方地址将比特币直接付给对方。下列表格，列出了免费下载比特币钱包和地址的部分网站。

比特币地址是大约33位长的、由字母和数字构成的一串字符，总是由1或者3开头，例如”1DwunA9otZZQyhkVvkLJ8DV1tuSwMF7r3v”。比特币软件可以自动生成地址，生成地址时也不需要联网交换信息，可以离线进行[2]。可用的比特币地址超过2个。形象地说，全世界约有2粒沙， 如果每一粒沙中有一个地球，那么比特币地址总数远远超过所有这些“地球”上的所有的沙子的数量。

比特币地址和私钥是成对出现的，他们的关系就像银行卡号和密码。比特币地址就像银行卡号一样用来记录你在该地址上存有多少比特币。你可以随意的生成比特币地址来存放比特币。每个比特币地址在生成时，都会有一个相对应的该地址的私钥被生成出来。这个私钥可以证明你对该地址上的比特币具有所有权。我们可以简单的把比特币地址理解成为银行卡号，该地址的私钥理解成为所对应银行卡号的密码。只有你在知道银行密码的情况下才能使用银行卡号上的钱。所以，在使用比特币钱包时请保存好你的地址和私钥。

比特币的交易数据被打包到一个“数据块”或“区块”（block）中后，交易就算初步确认了。当区块链接到前一个区块之后，交易会得到进一步的确认。在连续得到6个区块确认之后，这笔交易基本上就不可逆转地得到确认了。比特币对等网络将所有的交易 历史 都储存在“区块链”（blockchain）中。区块链在持续延长，而且新区块一旦加入到区块链中，就不会再被移走。区块链实际上是一群分散的用户端节点，并由所有参与者组成的分布式数据库，是对所有比特币交易 历史 的记录 。 中本聪预计，当数据量增大之后，用户端希望这些数据并不全部储存自己的节点中。为了实现这一目标，他采用引入散列函数机制。这样用户端将能够自动剔除掉那些自己永远用不到的部分，比方说极为早期的一些比特币交易记录。

消费方式

许多面向 科技 玩家的网站，已经开始接受比特币交易。包括Mtgox，BTCChina之类的网站，以及淘宝某些商店，甚至能接受比特币兑换美元、欧元等服务。毫无疑问，比特币已经成为真正的流通货币，而非腾讯Q币那样的虚拟货币。国外已经有专门的比特币第三方支付公司，类似国内的支付宝，可以提供API接口服务。

可以用钱来买比特币，也可以当采矿者，“开采”它们用电脑搜寻64位的数字就行。通过用电脑反复解密，与其他的淘金者竞争，为比特币网络提供所需的数字。如果电脑能够成功地创造出一组数字，就会获得25个比特币。比特币是分散化的，

需要在每个单位计算时间内创造固定数量比特币是每10分钟内可获得25个比特币。到2140年，流通的比特币上限将达到2100万。换句话说，比特币体制是可以自给自足的，译成编码可抵御通胀，防止他人搞破坏。

支付案例

在被投资者疯狂追逐的同时，比特币已经在现实中被个别商家接受。北京一家餐馆开启了比特币支付。这家位于朝阳大悦城的餐馆称，该店从2013年11月底开始接受比特币支付。消费者在用餐结束时，把一定数量的比特币转账到该店账户，即可完成支付，整个过程类似于银行转账。该餐馆曾以0.13个比特币结算了一笔650元的餐费。[13]

2014年1月，Overstock开始接受比特币，成为首家接受比特币的大型网络零售商。[14]

比特币是由中本聪创造的，(几乎可以肯定)是一个化名，迄今为止，还没有人能够确切地将比特币与一个真实的人或一群人联系起来。中本聪于2011年从互联网上消失，几乎没有留下他们可能是谁的线索。多年来，许多人都公开宣称自己是Satoshi，但都没有以无可争议的事实支持这一说法。

在一个早期的比特币论坛上，Satoshi说他们在2007年开始研究比特币，比第一个区块被开采早了两年。2009年1月3日，比特币区块链的第一个区块——创世纪区块被开采。中本聪是创世纪区块的开采者，收到了第一批投入流通的50枚比特币。然而，第一个方块的奖励是无法支付的，因为在代码中创世纪方块的表达方式有点奇怪。BitMEX研究发表了一份对比特币早期开采的分析，并得出结论认为“有人”开采了70万枚比特币。尽管许多人认为这是Satoshi，但官方仍未证实。

人们只能想象，如果他们的身份被曝光，中本聪会获得什么样的名声，更不用说他们将收集的巨额财富了(尽管佐藤似乎没有花掉他们应该开采的任何硬币)。随着时间的推移，已经有很多人声称自己是Satoshi，而其他人则被强加了这种说法。

虚假索赔

声称自己是Satoshi的最著名的例子之一是克雷格·赖特，澳大利亚学者。早在2015年，莱特就多次试图向公众展示他是比特币发明者的无可争议的证据，但直到今天他都没有成功。事实上，他的“证据”被证明是伪造的。

为什么Satoshi必须匿名

中本聪，世界上第一个分散货币的创造者，可以说应该保持匿名，因为他们创造的本质。在创建了一个没有失败中心点的协议之后，中本聪可能已经意识到，保持匿名可能会消除比特币可能存在的最后一个失败中心点:创建它的人。去除可能与比特币的出现相关联的单一身份，就去除了任何可能影响比特币社区的政治、规则或决策的单一面孔。

不管Satoshi是谁，他们无疑是我们这个时代的天才。比特币协议在所有合适的地方提供了经济激励，为拜占庭将军的问题提供了一个特殊的解决方案。中本聪运用密码学、数学、博弈论和经济学的概念，创造了一种设计精美的——也是世界上第一种——数字稀缺资产——比特币。

比特币的发明者是一位日本人，名叫中本聪，在2009年1月3日，世界上第一批比特币诞生， 数字货币也正式诞生，数字货币直到2013年年底价格才飞速上涨，从前期的10美元左右一下涨高到九百多美元，在2016年，比特币热度才真正起来，价格一路飙升，被称为“数字黄金”。 比特币为什么这么值钱呢?

1、挖矿难度大，比特币挖矿需要进行特定的运算，运算时间成本很高，前期的物质投入也非常大。

2、比特币带有货币属性以及被市场信任，比特币的加密算法难以破解，保证了其唯一性。

3、比特币交易市场透明度高，市场价格都是公开透明的，在虚拟数字货中流通和交易方便快捷。

4、有一些国家的认可，国家对比特币，数字货币出台的一些政策无疑都会刺激比特币价格上涨。

物以稀为贵，比特币比较稀有，目前比较币的开采难度很高，供求关系的影响，市场上供不应求的局面等等，这些无疑对价格上涨产生了很大作用。对于在交易平台购买比特币赚取差价的朋友需要谨慎。

比特币是一种P2P形式的数字货币。点对点的传输意味着一个去中心化的支付系统。在2009年由日本人中本聪提出比特币这一概念，比特币从始发到现在价格已经高的难以想象，比特币为什么那么值钱了?

下面来简单的说说。

比特币挖矿机通过运行一种特殊的程序，运行结束后就可以获得类似任务奖励的比

特币。现在比特币的产量是很低的，每天大约产出3600个新币，数量有限;比特币挖矿价格高，自从比特币火热后，专业挖矿机从价格低的一万元左右，现在价格贵的超过三十万，前期设备投入就需要很大财力;挖矿时间长，比特币挖矿就是经过特定的复杂运算，消耗额时间非常长;比特币挖矿机消耗大，除了有自身的损耗以外，还会消耗大量用电，特币全球挖矿机日耗电量可达1.88亿千瓦时，相当于中国日发电量的百分之一。比特币数量目前还在不断增加，有机构评估，在2019年比特币挖矿耗电量将会超过美国的耗电量。

比特币的价格一直都是媒体比较关系的，这里提醒大家，比特币价格涨的快，下落也会很快，风险高，想要购买比特币赚钱的朋友一定要谨慎加入。

沉寂多日的比特币借“勒索”病毒卷土重来，并开启似曾相识的暴走模式。这种被称作“数字黄金”的虚拟货币，8年间暴涨300万倍，连中国大妈都进场了。有人认为这是一个击鼓传花式的 游戏
，有人坚信比特币会成为稀缺资产，更有人说它会是在 历史
长河中闪光的一个节点，而多数人不求甚解，只是惊叹于又一轮的财富大爆发。

爱必投认为究竟是谁创造了比特币？关于比特币的发明者一直没有定论，普遍的说法是日本人“中本聪”（Satoshi Nakamoto）。2009年1月3日，世界上第一批比特币被“挖”出，这种由一个代号为“中本聪”的人设计的数字货币正式诞生，而自那一刻起已有15个人先后被怀疑是“中本聪”。2014年美国权威媒体揭露，本名为“中本聪”的日裔美国物理学家，就是传说的“比特币之父”，但这位老教授坚决否认。图为罕见现身的中本聪被媒体围攻，不断遮挡镜头，并否认与比特币存在任何联系。

2016年5月，澳大利亚工程师、企业家克雷格·怀特（Craig Wright）公开表明他就是比特币的创造者——中本聪。但仅过了几天，怀特本人就“投降”了，发表道歉信称“拿不出关键证据”证明自己。尽管中本聪被提名为2016年诺贝尔经济学奖候选人，但他的真实面纱还未被完全揭开。图片：BBC (来自:腾讯图片)

而跟比特币扯上关系后，克雷格·怀特就被警方盯住了。图为澳大利亚联邦警方与税务人员搜查了怀特的住所与办公地点，后者的比特币相关业务存在税务方面问题。据媒体报道，神秘人物“中本聪”手握100多万个比特币，按照目前每个15000元人民币来算，他的身价超过150亿人民币。而按照最初的严格设计，比特币的总量被限制在2100万枚，目前已有1400万枚左右被开采出来。图片：路透社

中本聪，不知他真身

专家解读比特币是很多人头疼的问题，尤其是在理解和现实的冲突方面，一文读懂

比特币也同样面临着相似的问题，关注我们，为您服务，是我们的荣幸！