本文谈专家&#039；解读比特币以及比特币对应的知识点，致力于为用户带来全面可靠的币圈资讯。希望对你有帮助！

《文理两开花》锚

小小泡：《羊群的共识》作者，金融行业从业者，连载创业者，播客《墙裂坛》主播，微信官方账号小小泡经理。王玮：数学和计算机科学硕士，同时也是技术和金融方面的硕士。。几年前，&quot全包&quot区块链菲尔德成为了区块链业界著名的意见领袖之一。

单词&quot智能合同&quot似乎是一个迷因：这是一个在金融技术行业甚至所有与技术和数字化相关的行业都会听到的概念，一个&quot听起来很强大，但我不&#039；我不知道这是什么&quot或者&quot我不&#039；我不知道它在哪里&quot不管怎样，这四个字代表&quot科技进步&quot。如果他们都&quot聪明&quot，他们还能好吗？

但这是什么？你能做什么？什么能&#039；你不想吗？现在迫切需要聪明的合同专家使用小白和文科生都能理解的语言。

就在最近，在现实世界的金融市场上，发生了几件有趣的事情：俄罗斯债券违约，以及&quot镍短项目&quot在金属市场，——。所以让&#039；让我们简单地做一个案例研究，看看智能合约能否在现实世界中解决这些令人头疼的问题。。[XY002][XY001]本期概述[XY002][XY001]1。365度全景&quot魅力消除&quot智能合约：它的&quot智力&quot？是一段代码吗？一份合同？还是机器人？

2。是只能解决虚拟世界的问题，还是也可以用在现实世界？

3。俄罗斯债券违约：如果使用智能合约，结果会不同吗？

4。主权债务放在智能合约里会不一样吗？？智能合约能解决信用问题吗？

5。镍强制空运事件和LME&quot；硬叉子&quot:如果LME采用智能合约自动执行，结果会不会不一样？

6。&quot硬叉子&quot在区块链和&quot硬叉子&quot(取消交易)在现实世界中？

7。可以设置&quot投票&quot和&quot冷却期&quot避免&quot多数人的暴政&quot？

正文手稿

Trot02:48

word&quot；智能合同&quot似乎已经成为一种迷因。。是金融科技行业乃至更广泛的科技、数字化相关行业都会听到的概念。反正这四个字代表科技进步和智能。

但是它&#039；它仍然是一个&quot听起来很棒。但我不&#039；我不知道那是什么，或者我不知道。我不知道它在哪里。大多数人，包括我在内，对它的了解很少。所以今天，请王玮先生来&quot醒悟&quot这份智能合同使用了小白和文科生都能理解的语言。此外最近，在现实世界的金融市场上，发生了几件非常有趣的事情，包括俄罗斯债券违约和镍做空。今天，让&#039；让我们将这两件事作为案例研究，看看智能合约是否能解决现实世界中的这些令人头疼的问题。

首先，请王玮先生向您解释：&quot智力&quot智能合约？

王玮04:26

智能合约现已进入区块链、DeFi和futureweb3领域。，是最重要的核心。比特币出来的时候，大家都说区块链是一个&quot分布式分类帐&quot；以太坊诞生以来，人们逐渐看到智能合约在web3.0乃至元宇宙领域发挥着越来越重要的作用。

先说一个发生在我身边的小故事。我有一个学姐，是大学计算机系的教授。去年，我问了一个问题：我能理解区块链，但我没有&#039；有一个问题我不明白。哪里是&quot智力&quot——智能合约？

为什么这么问？她一定明白&quot智能合同&quotas&quot智能代码&quot。因为她是搞技术的，肯定要和其他代码比。默认情况下，&quot智能合同&quot应该更&quot聪明&quot在它被称为&quot智能合同&quot。

我的答案是：唐&#039；不要把它与计算机代码进行比较，而是与现实世界中的合同进行比较。是智能合约，不是智能代码，所以很好理解。将它与代码进行比较有点侮辱了&quot智力&quot。但与日常经济活动中签订的合同相比，逻辑更为恰当。

相比契约，它的智能在哪里？

我们日常的合同有几个特点：一是有两个或两个以上的当事人签订；第二，它有合

同条款。在什么情况下，实施什么条件，做什么事情；三是有合同标的，合同规定提供什么商品或服务，支付多少；第四，合同大概有编号，有鉴定记录是哪份合同，是哪年哪月哪日签的。，谁跟谁签的等等。第五，要有管理工具，每个签字人各持一份，防止一方更改条款。这五个特征基本代表了日常合同执行的最基本条件。

从这个角度来看，智能合约很好理解。

比如以太坊的智能合约：第一，它的代码和存储的数据实际上等同于合约条款满足什么条件，如何自动执行——。大家可能都知道智能合约的这个特性。其次，它还可以使&quot每个签字人持有一份&quot在链条中实现。当两个签名者都可以访问区块链时，他们实际上可以看到合同的副本，并且副本不是他们可以掌握或篡改的东西，而是存储在链中。这很有趣：中本聪发明了区块链。为了防止纯数字资产&quot双花&quot比特币，结果在智能合约时代，以太坊突然赋予了它神奇的能力&quot帮助合同各方存储无数的副本，并确保它们不会被篡改&quot。区块链是一种全球分布式存储。它使世界上任何数量的人能够共同签署和执行合同，而不会使传统领域中的合同无法被篡改。因为技术的限制，你可以&#039；不要让任何数量的人同时在合同上签字。第三种智能合约中的每段代码都有相应的&quot地址&quot以及执行这段代码的入口，这段代码可以理解为合同号和唯一标识。

第四，智能合约本身也可以拥有&quot其他财产&quot。。我们的日常合同只是一张纸，一个附属品，财产还在人&#039；s控制。即使合同规定了镍的交割，纸怎么能控制镍的运动呢？智能合约本身可以控制财产。合同必须有&quot主题&quot，&quot钱&quot和&quot商品&quot该标的物可由智能合约控制，相当于被&quot拥有&quot靠它。在这种情况下，所谓的&quot自动执行&quot是有保障的，并且拥有资产的完全执行权。在11:30小跑

相当于司法强制的结合。

王玮11:33

对。于是就有了签字人，无数可靠的备份，自动执行能力，可访问的地址和入口，对合同标的物的控制权。从这个角度来看，它确实要大得多&quot智能&quot比普通合同更好。12点04分小跑

其实我特别理解王小姐的想法&#039；她的妹妹。毕竟都是理科生，大家可能从代码的角度自然理解。但是作为一个非技术出身的普通人，我不&#039；没有理解的障碍。一看到这个词&quot智能合同&quot没有代码背景的人自然会先把它当成一个契约，一个&quot智能合同&quot没有人需要执行。例如，在现实世界中，我和老板签了合同，但他没有&#039；Idon’我不能每个月都把钱支付到我的账户上

，我也不能。没办法。此外智能合约是建立在区块链上的，这意味着我不&#039；我不需要认识和我签合同的人。我们还没有&#039；我们以前没有做过生意，现在也没有。没有建立任何信任关系。事实上，我们可以签署——，因为区块链保证&quot一人&quot并且不能被改变。。这有点像我们讨论的SWIFT——，实现了&quot信息&quot和&quot帐户&quot；智能合同就是要实现&quot内容&quot和&quot执行&quot的合同。一旦它成立，我不&#039；你不必太担心执行的问题。智能合约会自动支付给我，所以我不&#039；我不必再相信我的老板了。。

不过仔细想想，好像有点混乱。如果它的执行是自动的，出了问题怎么办？当我们订立一份传统合同时，在后续的开发过程中会有条款的变更。或者有特殊情况导致合同不能按订立时的条款履行。——如果出了问题，智能合约会不管不顾的执行吗？如果是这样，每个人都是&quot签名&quot一份精明的合同。当你按下开始键的那一刻，你可能不得不重新思考。只要按了，就没有改变的余地了吧？王玮15点

让&#039；谈谈第一个问题：智能合约的最大价值在于，世界上那些不&#039；彼此不认识或从未有过任何合作关系的人可以立即签署并执行此合同并得到结果——，这符合区块链的特点。

很久以前我们介绍区块链的时候，会强调它的一个特点，——，让全世界没有合作关系的人都可以开始转账交易。中本聪发明了防止&quot双花&quot为了实现——。虽然我们不&#039；不认识，我给你转钱。你知道这次转会一定是真的，不会有任何问题。智能合约继承了这个特性，而合约不能被执行，因为我们没有&#039；不要互相了解，否则你会作弊。

但如果是这样，合同肯定会执行。，也就是说肯定不会变。那我怎么敢随便签呢？

这个点要看技术角度。——智能合约可以是&quot已更改&quot。从技术角度来看，&quot已更改&quot与软件系统的升级没有太大区别。

如果一定要更改某一条款，就意味着原合同作废，重新签订新的合同。智能合约也是一样，相当于升级代码。现在是1.0版本，过几天我会有1.1版本。替换1.0版——我们从现在开始实施1.1版3354，没问题。但是问题又来了。谁有权利做这件事？如果合同双方都有权变更合同，那就毫无意义，完全不可能。

智能合约实际上相当于一个&quot市场&quot，由第三方创设合同，然后大家分成甲、乙、丙三方签订、执行合同。

我敢签署本合同，是因为我作为甲方，相信乙方、丙方、丁方能够&#039；不要更改这份合同。，必须执行。第三方是合同发布者和创建者，它有权升级合同代码。

这种机制有点像建立一个&quot商店&quot，在这种模式下，买卖双方签订合同，做生意，但店铺的规则不能改变。只有商店的建造者有权改变它。。这也是一种必然。

这种必要性会带来什么问题吗？

肯定有。例如，第三方处于&quot从里面偷东西&quot。如果他发现更改合同对自己有利，也可以篡改合同，造成签约人的损失。。即使他想提高合同的执行效率或者改进条款，但不是出于私利，大家都同意吗？

我们经常举一个例子：a&quot贷款&quot智能合约可以指定利率算法。比如年化5%；如果调整为年化303354，表面上看，利率是借贷双方付出的成本，与规则制定者的利益没有直接关系；但是你可以&#039；不要因为你是中立的一方就改变规则。所以你需要给买家和卖家一个&quot缓冲期&quot或者一个&quot冷却期&quot，或者一个投票机制，让参与者共同做出决定。如果它被接受和投票，规则可以被修改。

如果参与者不&#039；不接受它，你必须改变它。然后你给我一个冷静期，我&#039；我不干了。所以最后整个逻辑还是完整的，还是要引入第三方制约机制。我觉得这和现有金融市场的一些规则差不多。20点42分小跑

这就是为什么需要专家解释的原因。如果只看这四个字，会觉得是冷冰冰的自动代码；但这背后其实有一系列的规则，而这些规则大部分是可以映射到现实世界的。例如，刚才的例子非常类似于一个&quot仲裁机制&quot。在这种情况下，让&#039；s找几个现实世界中的案例，分析一下现实世界中让人挠头的问题。如果我们将它们放在智能合约上，结果会有所不同吗？

我发现了两个：一个是俄罗斯&#039；的违约，另一个是镍&#039；强制通风。。

Let&#039；让我们从俄罗斯开始。其实俄罗斯是一个经常违约的国家，主权债务违约频繁：1918年沙皇帝国的债券违约，1998年布雷迪债券差点违约，还有最近的俄乌战争。并将其带入另一个危险的违约期。

3月16日，俄罗斯为两笔美元债务支付了超过1亿美元的利息。付息前一周，大家就开始担心了，因为俄罗斯和乌克兰已经开战了，现在还能还吗？如果付款是用什么货币？你使用卢布吗？它已经贬值了20%。

结果是没有违约，危机暂时解除。3月18日，俄罗斯财政部还了。虽然晚了一天，

但还是在30天的宽限期内。但是事情还没有结束。4月份，有超过20亿美元的本金偿还。。所以到现在为止，会不会违约还是一个巨大的问号。

通常，一个国家不愿意对其主权债务违约。主要是如果违约，市场会以某种方式惩罚你，比如失去信用，被评级机构降级为垃圾债。如果投资者长期不愿意碰，你就很难在市场上找到钱。但是一个国家违约的可能性太多了。在上个世纪，大量发行主权债券为战争融资。一旦战争爆发，，肯定是违约——因为所有的钱都会用于战争。俄罗斯现在就是这样，更难。无论是被动制裁还是主动制裁，投资者显然都不愿意去碰。俄罗斯基本上与世界隔绝，可以&#039；不要失去更多的信用。因为它几乎没有信用；外汇储备被冻结，就算想还，上哪找美元和硬通货？

那么在这种情况下，单词&quot违约&quot刻薄？

在现实世界中，作为政府的债权人，你实际上很难冻结或强制出售一个国家&#039；的资产。这是一场信心和耐心的比赛。如果你有能力骚扰这个国家的政府足够长的时间，你就会年复一年地追究下去，就像保罗辛格为了讨债，干脆抢劫阿根廷的船。。俄罗斯，一个战斗的民族，是不同的。历史经验表明，即使是最坚定的债权人，俄罗斯人也有足够的能力超越他们，用死老鼠的感觉阻止所有的讨债&#039；的心态。

这次还有一个有趣的点：这个主权债务里面有一个条款，叫做&quot同等待遇&quot——&quot平等对待&quot原则。这是一个古老的条款，在一个多世纪以前的债务合同中使用。它要求债务人平等对待所有债权人。你可以&#039；不要厚此薄彼。只要和任何一个债权人谈判，也要给其他所有债权人同等的还款待遇。

自从保罗辛格利用这一条款成功向阿根廷政府讨债之后。之后，大多数国家在发行主权债务时删除了这一条款，以防止这些&quot钉子户&quot收债时不要再用这个条款。然而，33，354并没有从俄罗斯的债务中删除。要么是战斗民族太嚣张，觉得永远不会被起诉；还是算了吧。。尽管如此，单词&quot未来还款&quot条款神奇地消失了。——这是故意的，也许是笔误。不管怎样，结果变成了：所有债权人都会遵循&quot平等对待&quot发行时，但并不意味着&quot未来&quot还是老样子。

这个例子告诉我们，债券市场是一个&quot复制粘贴&quot交易由&quot样本文档&quot。很少有人真的去读长达数百页的——条款，但魔鬼就在这里，人为的空间太大&quot调整&quot和&quot默认&quot。

如果债券是根据智能合约发行的，不会&#039；不会发生这种事吗？

王玮28:09

这个案例特别有意思。我仍然有点担心，因为区块链和智能合同。其实是最不适合解决债务问题的。不过听了很多俄罗斯债务的细节，有一个解决的好地方。

首先，&quot债务&quot是典型的&quot信用&quot过程。本质上我把金融分为&quot信贷流程&quot和&quot计算过程&quot。区块链、智能合约、DeFi等。实际上解决了&quot计算过程&quot，并且&quot债务&quot是典型的&quot信贷流程&quot。

实际上，关于&quot债券违约&quot是最不适合用智能合约解决的。换句话说，智能合约和区块链是对&quot债券违约&quot，因为违约是一个信用丧失的过程，即使用智能合约来写债务合约。但是，还债的过程涉及到还债的主体，你需要把资产放到智能合约里面去执行；如果你不&#039；你不能把它放进去。不要执行它。

这又回到了最关键的一点：智能合约能够保证自动执行的前提是合约本身具有&quot控制&quot关于这个主题。。但如果我将来要还的33，354本金甚至利息都放在智能合约里，由它控制，那我为什么要&quot借&quot现在有钱了？你必须把一些兴趣倒过来。

在DeFi领域，我们也看到很多项目和创业者。，试图利用智能合约解决债务市场问题，或创造信贷产品。其实没有问题，因为智能合约背后可以有一套其他的保障机制，比如投票等等；仍然有可能最终改变“的信用&quot部分纳入其他保障机制。

The&quot；执行部分&quot信用证可以&#039；t被转换成代码级的安全机制，但这并不&#039；这并不意味着智能合约可以&#039；不要改善债务市场。就俄罗斯的债务而言，它有权去掉这个词&quot未来&quot从&quot平等对待&quot条款。没有办法控制；买债的人买了——没注意找零，这其实可以在智能合约的层面上改善。

首先，智能合约写成代码规则，自然有&quot平等对待&quot。因为代码每个人都可以执行。只要有一个地址，代码固化在其中，世界上的每个人都可以执行它，所以默认情况下它将&quot平等对待&quot。如果你不&#039；我不想成为&quot平等对待&quot，你要做很多花样。

关于&quot债券市场是一个基于模板的复制粘贴市场&quot——让我想起了许多&quot微创新&quot前几年在DeFi智能合约领域，也是把一些智能合约的代码完全复制然后改成两三个字。

但是你会发现，在这种情况下，智能合约是有价值的。为什么？

因为智能合约是准确的代码。审计机构很容易发现这些变化。不同的代码行意味着不同的结果。，可以准确推导判断。在传统市场上，因为自然语言不精确，即使允许律师尝试，我们也不&#039；Idon’我不知道这些变化背后是否还隐含着其他意义。或者导致任何意想不到的后果。

智能合约的审核机构是整个生态中非常重要的一方。这些机构通常是聪明的合同开发者或白帽黑客。他们的角色非常类似于现实世界中的律师事务所，他们负责审查合同和合同代码。

总而言之，智能合约可以&#039；虽然不能解决债务的所有问题，但它们仍然在债务执行和条款分析中发挥着巨大的作用。

小跑35:47

所以现在我觉得可能是俄罗斯的情况。将全部主权债务放在智能合约上可能不太现实。因为对于原本打算&quot未实现&quot，可能根本不签。

这就引出了第二个案例：前段时间闹得沸沸扬扬的镍逼仓事件。

让&#039；让我们回顾一下：关于女性&#039；这一天，市场上演了一个历史性的事件，我们目睹了LME市场史诗般的空头挤压。镍的价格创下了历史上最极端的价格波动，3月7日飙升了76%。，达到每吨5万美元以上；然后第二天就突破了10万美元一吨的大关。

这是明显的空白。青山——，世界&#039；在俄乌战争之前，美国最大的镍生产商被迫选择了错误的方向。15万吨镍空头头寸，其中5万吨是摩根大通的场外头寸；也就是说，此时此刻，青山已欠JP约10亿美元保证金。

对于场外交易，还有讨论的空间。如果极端情况发生，双方将首先在场外协商解决方案。这次爆炸后，青山在经济上向交易所缴纳了保证金，否则清算会出现巨大问题。作为协商的结果，空头头寸首先被保留，然后LME&quot；创造历史&quot取消了交易。并在3月中旬之前停止了镍的交易。

从那一刻起，从全球市场的角度来看，LME&#039；s&quot信用&quot和&quot中立&quot出现了一个巨大的问号。突然暂停交易影响了数千笔交易，市场的其他参与者也遭受了巨大损失。

在这种情况下，智能合约可能在哪里发挥一些作用？

王玮42:10

其实刚才在介绍智能合约的时候，我们也提到了我们真的可以&quot干涉&quot智能合约。它&#039；这并不是100%不变的。从这个角度来看，LME的这次干预也可以看作是一种&quot干预&quot。但这里也存在一些问题：首先，&quot干预&quot智能合约。，您必须通过&quot授权人员&quot；或者直接修改智能合约中的参数。这不同于中央集权制。回滚&quot或者&quot取消&quot交易。

智能合约的介入，无论是代码升级还是参数调整。，只能是&quot逆向干预&quot，改变未来的规则，并且可以&#039；不要回到过去的某个阶段。——区块链不支持这种干预。

当然，它没有&#039；我不是说&quot逆向干预&quot能&#039；根本不会出现。例如你们可能都听说过道对以太坊的攻击，正因如此，以太坊才有了&quot硬叉子&quot——，这真是一个&quot回滚&quot，以太坊历史上发生过一次。然而，这样的结果&quot回滚&quotETC和ETH链是同时产生的。因此，在&quot计算的&quot，即使你想&quot回滚&quot，它不是100%回滚，因为仍然有人可以选择执行那些没有&quot已回滚&quot被你。

但是这个可以&#039；这不会发生在现实世界中。。因为另一个平行世界的人是不可能选择继续交易那些已经被强行清空的订单的，因为只有一个交易所，而回滚就是回滚，两个交易所是不会硬分叉的。现实世界是不可分的。不可能叉出两座青山，两个俄罗斯人，一吨镍变成两吨，——两个平行世界各一吨。这是由物理世界决定的。因此，智能合约和区块链系统只能有所谓的&quot保证执行&quot对&quot纯数字资产&quot。

LME能&#039；s&quot停止交易&quot和&quot取消交易&quot在智能合约领域做的怎么样？

客观来说也可以。一般有两种手段：第一种是投票。这相当于LME股东的集体投票。投票结果决定是否允许回滚。如果投票没有通过，就不能更改。这就是为什么当前的加密领域将实现&quot代币经济学&quot系统，这是一种类似于股权的模式。投票结果可以绑定到智能合约并自动执行。。

二、投票是什么意思？在数字世界中投票是一件&quot刚性&quot结果，——51%的人同意改变它，但赢了&#039；这会导致&quot多数人的暴政&quot？49%的人不同意只能接受？如果投票可以&#039；解决不了问题？

答案是设置一个&quot冷却期&quot或者一个&quot过渡期&quot可能是几天或几个小时。即使表决通过，也只能在冷静期后实施。如果你不&#039；不想玩了，这段时间退出系统就行了。改变规则没有问题。但请给我离开的自由。这是最基本的自由。LME&#039；的做法是典型的&quot集中&quot系统。——就算要改规则，大家可以先投票吗？那些受规则影响的人至少应该有机会发言。第二即使投票通过，也需要一段时间来改变。

如果是通过智能合约实现的，并且遵守了刚才的治理规则，那么它的信用度肯定会更高。所以从这个角度来说，智能合约是在维护一个公平高效的市场规则，具有更高的信任度。，它会有很大用处的。

trot50:51

是。虚拟世界中的一些机制也可以用在现实世界中。但这些投票、冷静期等规则的实用性如何？

比如多数人的暴政。如果每个人都突然意识到&quot多数人的暴政&quot，比如我讨厌有钱人，反正我们都是市场上的韭菜，所以我们以号取胜，一起投票。把大账户里的钱全部转到我们的账户。——如果是根据投票结果自动执行，isn&#039它相当于&quot合理抢劫&quot？

但是如果设置冷静期，15天后正式实施抢劫，大户肯定会离开，可以&#039；不要等着被抢劫。。但是大家都走了。15天后我去抢谁？整个游戏毫无意义？王玮52:17

这是区块链和加密货币的一个核心概念，——就是你的行为要经济合理。

小三这样做，损人不利己。不仅没有拿到钱，唯一的结果就是毁掉了这个平台的价值和信用。。在这种情况下，你会发现小三并没有那么傻，他们知道投他的票没有意义。

这要追溯到中本聪&#039；的比特币白皮书。可以用51%的计算能力攻击，把比特币全部掌握在自己手里。不过比特币也已经归零到——了，你买的那些机器的成本可以&#039；不要回来。这对你有什么好处？

所以在某种意义上，&quot经济模型&quot是核心&quot迷因&quot在区块链场。我们坚持的这种经济模式的合理性。，导致攻击毫无意义，毫无道理。

Trot54:11

我现在觉得，其实任何规则和机制虽然看起来都是补救措施，但其实它们发挥最大作用的时候都是在事情发生之前。。

在游戏的影响下，大家&#039；的行为会自动找到最理性的&quot遵守规则可以实现最大价值&quot。也就是说，事先的良好设计会导致一个理性的结果。王玮55:13

智能合约和区块链的核心价值实际上是&quot保持规则的有效性&quot。更适合平台经济，或者说双边市场的逻辑。区块链和智能合约的创造者是规则的制定者和维护者，他们自己不一定是参与者。。参与者都是不&#039；世界上不认识，一起参与游戏。

如果两个人认识，签了合同，交换了合同文本，并且愿意保证以后——的执行，那么智能合同在这个场景下没有太大意义。

我非常同意。你可能有各种方式升级通关，但是游戏规则的整个框架都可以通过智能合约来完善。

—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基金会网站上发表了一篇关于比特币的白皮书。，陈述他对电子货币的新想法，——比特币出来了。

2009年，中本聪设计了一种数字货币，即比特币。比特币市场跌宕起伏，其创始人的身份&quot中本聪&quot一直是个谜。关于&quot比特币之父&quot涉及从国家安全局到金融专家的方方面面，也给比特币蒙上了一层神秘的光环。

扩展资料：

从比特币的本质来说，比特币的本质其实是一堆复杂算法生成的特殊解。。特解是指一组可以由方程得到的有限解。而且每个特解都能解方程，是唯一的。

如果拿一张钞票来类比，比特币就是钞票的冠字号码。如果你知道一张钞票上的冠字号码，你就会拥有这张钞票。

挖掘的过程就是通过庞大的计算不断寻求这个方程组的特解。这个方程组被设计成只有2100万个特解，所以比特币的上限是2100万。

参考来源：百度百科——比特币

央视网消息：商务部14日发布《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》，公布了数字人民币试点地区。目前，数字人民币的试点项目仍然&quot41&quot；也就是说，内部封闭的试点试验是在深圳、苏州、熊&#039；一个新的区域，成都和未来冬奥会的场景，并没有什么变化。有关人士指出，网上上传的北京、天津、上海的28项试点，实际上是全面深化服务贸易创新发展的试点。

到底什么是数字人民币？

目前很多国家都在研究法定数字货币，只是在技术路线、操作体系、交付路径上有所不同。中国&#039；美国法定数字货币是数字货币和电子支付工具的结合体，由人民&#039；中国银行。目标是替换一些现金。那么，数字人民币到底是什么？

简单来说，数字货币，人民&#039；sBankofChina，是电子版人民币，把数字货币当成数字人民币现金就不难理解数字货币的概念了。说到数字货币每个人&#039；的第一反应可能是比特币，但其实两者有本质区别。比特币、天秤币等虚拟货币本质上是一种虚拟商品，没有国家信用，也没有法律赔偿。数字货币，人民&#039；中国银行发行的纸币是由国家信用担保的法定货币。在这一点上，它和现金有着相同的作用。

如何使用数字人民币？

随着移动支付深度融入我们的日常生活，使用数字人民币应该不陌生。因此数字人民币到底怎么用？和我们习惯的电子支付方式，比如微信、支付宝有区别吗？

从使用场景来看，数字货币，央行，不付利息，可以在小额、零售、高频业务场景下使用，和使用纸币没有太大区别。不仅如此；不央行的数字货币采用最新的双离线技术，即使没有手机信号也可以使用。

未来现金会被取代吗？

有了数字人民币，是否意味着以后会取代现金？？专家表示，未来数字货币，也就是央行，会替代部分现金，但不是全部纸币。

国家金融与发展实验室特聘研究员董希淼表示，在中国，纸币将长期存在。对于一

个幅员辽阔、经济发展水平不同的大国来说，我们的用户习惯也是不一样的，现金支付和非现金支付会长期共存。

与此同时，央行发行的数字货币是从替代流通中的纸币和硬币开始的。也就是说，假设现在流通的货币是100元，央行数字货币会等价替代这100元。

北京大学数字金融研究中心高级研究员徐苑说，新的数字货币和我们以前的纸币是一张一张地交换的。那么商业银行现在要想得到这种数字货币应该怎么做呢？需要在不增加总额的情况下兑换之前的货币。这是第一步，试点期间不会增加总量。

什么时候可以使用数字人民币？

所以究竟什么时候才能看到数字人民币的真面目？目前，数字人民币已经在深圳、苏州、熊&#039；一个新的区域，成都和未来的冬奥会。如果进展顺利，北京也许能够&quot看美女&quot在2022年冬奥会上。。但数字货币的真正使用还需要测试理论可靠性、系统稳定性、风险可控性等环节，央行也多次表示数字人民币的推出没有时间表。然而，我们期望在不久的将来使用方便的数字人民币。

中新经纬客户端7月26日专题：《黄震：数字货币发行绕不过的坎》

作者黄镇(中央财经大学教授、金融法研究所所长、中新经纬特聘专家)

近日脸书宣布将开发稳定货币Libra和匹配钱包Calibrata，声称其使命是建立一种简单、无国界的货币和服务于数十亿人的金融基础设施。作为全球最大的社交网络平台，脸书。它准备利用自己丰富的资源，推出一个特别宏大的硬币发行计划，可能实现超主权货币与创新科技的结合，再次激发颠覆世界货币金融体系的无限想象。

为什么会这样？第一作为全球最大的社交平台，脸书拥有数量庞大的活跃用户。货币一旦发行成功，将会产生前所未有的规模效应。其次，天秤座白皮书中提到的应用场景、应用范围、商业圈都是极其庞大的，这使得数字货币不再仅仅停留在虚拟空间。物理场景应用比较多。第三，更令人惊讶的是，有许多主流金融机构参与Libra&#039s硬币发行计划，尤其是Visa、Mastercard等国际知名支付机构。所以天秤座更容易融入主流金融市场。第四，脸书&#039；美国的硬币发行计划实际上已经得到了美联储的默许。直到今天，美联储也没有表示反对脸书&#039；的资金分配计划。

脸书资金分配计划我们没有必要恐慌和过度解读。而是应该进行理性的反思和预测性的分析，提出数字货币现象的理论分析框架和未来的全球监管框架。

从历史上看，数字加密货币只有十年左右的历史，但是十年来，成千上万的数字加密货币，没有主权国家的监管和控制，就像一路狂奔的野马。尤其是比特币，在各种力量的炒作下，价格暴涨暴跌，是世界金融史上罕见的现象。比特币和以太坊的应用范围主要局限在虚拟空间。而这一轮讨论由脸书&#039；即将发布的加密数字货币意味着数字货币可能进入一个新的阶段。脸书&#039；s的货币分发计划是由在物理空间有较大影响力的机构分发数字加密货币，金融机构参与其中。这将在全球范围内产生巨大的示范效应。如果监管部门放任其行为，拥有各种资源条件的各行各业大亨可能会跟风进行监管套利，从物理空间转向发行数字加密货币，这可能会剥夺主权国家的铸币权，导致铸币税流失。，冲击现行的主权货币体系和国际货币体系，所以数字加密货币的问题尤为严重。

在数字加密货币的冲击下，传统的货币理论乃至整个金融理论也受到了极大的挑战。在传统金融理论中，货币国有化是大家都习以为常的事情。货币是以国家信用为背书，以国家主权强制力为担保的交易凭证，近代以来一直由各国主权支配。但由于主权国家经常超支、滥用货币，往往会导致严重的通货膨胀。国家财富流失和经济社会动荡。

许多经济学家对各国货币当局滥发滥发的问题表示不满，也试图提出新的解决方案。最有代表性的理论之一是哈耶克提出的货币非国有化。。他指出，主权国家控制下的信用货币过多的问题靠自身是无法克服的，应该回归到货币发行的非国家化道路，比如让企业发行货币，或者让其他市场主体发行货币。这个想法激励了许多人&#039；的想象力。但是我们还没有&#039；我没有找到解决办法。直到比特币的出现，人们看到了哈耶克的希望&#039；美国的货币非国有化思想。

近百年来如何稳定币值？？金本位崩溃后，世界各国都没有很好地解决这个问题。虽然有学者呼吁回归金本位，但回归金本位是不可能的。还有一个为货币找到锚的问题。什么样的资产可以锚定币值稳定？？货币发行数量如何与经济发展相匹配、相适应？传统货币理论的一系列问题在数字加密货币领域仍然需要解决。

虽然比特币被称为&quot硬币&quot以它的名义，但实际上，监管部门仍将其视为数字资产或虚拟货币，而非严格意义上的货币。既然金本位货币可以&#039；不能回头，货币的发行可以&#039；不回避主权国家，我们应该如何判断脸书&#039；发行货币的行为？并对其做进一步的预测？可以重点从以下几个方面入手。

第一，数字货币是全球经济金融发展的大势所趋，任何一个主权国家都无法回避。目前市面上的数字加密货币主要由互联网公司发行。，并且已经形成了相当大的用户规模，虽然主权国家不承认它是货币，但实际上它已经具备了私人货币的特征，并在一些商业圈子中发挥了巨大的作用。

第二，一个主权国家发行数字货币必须尽快提上日程。为了应对数字加密货币抢币权的挑战。一个主权国家能不能推出数字货币，什么时候推出数字货币，路径是什么，都应该尽快研究解决。

第三，数字货币具有全球化和超主权的特征。。谁来主导全球超主权数字货币，如何监管？目前，主权国家面临重大选择。就是让比特币和天秤发展成事实上的世界货币或者超主权的全球货币。还是主权国家在主导和探索一种全球货币或世界货币的形成？世界各国应该共同努力，讨论和解决这个问题。

目前天秤座绕过宗主国几乎是不可能的。。如果天秤成为所谓的超主权全球货币，必然会触及美国的货币政策和美元的地位，甚至其他主权国家的利益，引起主权国家的抵制。一些美国国会议员对Libra&#039的硬币发行计划。将来的Libra发行计划是否可行，取决于美国政府和其他主权国家的金融监管政策，以及主权国家组成的国际货币组织的态度。

基于上述问题的分析，对于全球数字货币未来的发展路径，在我看来，有三个方案可以讨论。

第一种方案：将比特币、以太坊甚至未来的天秤纳入监管，未来逐步纳入监管，也就是所谓的&quot染色方案&quot。。全球货币或实际上已经具有世界影响力的世界货币的纳入和认可，将由主权国家逐步纳入监管轨道。目前是有前提条件的，但是无论是编制还是染色都有很多技术问题需要解决，主权国家也很难认可这个方案。

第二种方案：现行国际货币基金组织或类似组织发行超主权国际货币或全球货币。Libra推出计划后，国际货币基金组织也声称IMFCoin即将推出。。在目前国际货币基金组织的一揽子方案，即中国学者姚宇东和杨涛提出的eSDR方案下，推进数字货币可能是最佳选择。

第三种方案：由主权国家发起创建新的数字货币国际组织。推动全球数字货币的发行。或者，主要的数字货币发行者主动与主权国家的监管部门合作，共同发起一个全球性的数字货币组织。然而，创建新的国际合作与协调组织需要时间。黄镇

文/肖小跑

对未来最好的姿势就是提问。提问最好的态度是从你最熟悉的领域问——，所以本

文&quot未来金融三问&quot应运而生。也许它&#039；它不成熟，但它&#039；这都是一个问题。我想了很久。

1。最有前途的地方在哪里？

当我开始职业生涯时，我的&quot职场圣经&quot是迈克尔刘易斯的《说谎者的扑克牌》。

书中有一段描述他得到了所罗门兄弟公司债券销售的报价。报道的第一天，我觉得：&quot它&#039；这不像是去上班，更像是中了彩票。"

人生第一份工作直接扔给他一袋金砖——，工资是他LSE(伦敦政治经济学院)教授的两倍多。这位教授将近50岁了。，已经站在了自己领域的巅峰；而他24岁，刚刚摸到山脚下的第一块石头。他的结论是不存在&quot公平&quot在这个世界上。1985年的华尔街是世界上最有希望的地方。所罗门兄弟是那年街上最帅的男孩。在接下来的几十年里金融投资银行&quot就像希腊神话中的迈达斯，把石头变成金子(迈达斯&#039；stouch)。从华尔街到伦敦金融城到香港到上海，它接触到的一切都会变成黄金。

30多年后的今天，这个行业依然是黄金。全球金融业经历了有史以来最赚钱的一年。2022年可能会有更大的红包。

但是彩票中奖的惊喜感已经消失了。&quot的狂欢没有明天&quot在《说谎者的扑克牌》和《华尔街之狼》已经消失了，空气中弥漫着一种难以形容的&quot中年疲劳&quot.——明天将面临无休止的监管。经济学家不断提醒我们酝酿危机&quot。真正的乐趣不再于此，而在别处。

为什么金融行业曾经有如此巨大的虹吸力？

It&#039；这不仅仅是因为你挣得多。因为它是一台可以转动的大机器&quot聪明&quot变成&quot钱&quot。在这里，总有人会因为解决一个钱的问题，把一个精妙的设计变成现实，或者在市场游戏中升级为高级玩家而变得富有。。虽然《大空头》中的MBS、CDS、CDS平方、tranche、高斯定理、奇异期权等工程天才的代表作都被贴上&quot贪婪&quot，谁没有&#039；t暗暗称赞&quot真的很棒&quot？

但这是过去。。当前的并购。a和投行从业人员感觉就像普通工人。而那台神奇的机器，被搬到了市值2万亿美元的加密行业。前投资银行精英的金手指，从小在币圈长大，DeFi，web3开发者，还有memeNFT&#039；s&quot钻石手&quot。

空气中弥漫着一种说不出的嫉妒、FOMO和沮丧。

所以钱景已经从金融领域进入加密行业了？我的答案是否定的。证据在一首唐诗中：&quot一个月前，他先去浮梁买茶叶，不小心丢下了她。

喜欢&quot商人&quot"华尔街皈依者&quot实际上是一个符号，与领域无关。它代表了一个特殊的群体，他们的心跳是由&quot波动&quot——茶叶，蔬菜市场的大葱，股票，商品，债务.当然还有比特币。他/她有一个&quotcraft&quot能够承受任何波动，适应任何复杂的市场格局。

三十年前，这个群体在商品市场上享受到的所有快乐，砰，现在都没有了。蓦然回首，发现幸福的影子笑着躲在加密行业。传统市场上的那些被&quot低利率&quot，&quot监督&quot和&quot冷兵器卷&quot都在这里重生了。

比如高频做市：这个行业在股票市场和商品市场几乎是寡头垄断，在加密货币领域则是遍地羊毛。用一支小手枪，你可以&quot打枣吃到饱。"

还有一个&quot泡菜高级&quot(泡菜溢价——)。每次出现牛市，韩国人民&#039；美国对加密货币的强劲需求将推动价格高于其他国家。它是&quot泡菜高级&quot)，期现套利，日间动量和统计套利。年复一年，只要人类还&quot一维&quot，价值评价体系仍然&quot成长&quot。前景(资金)将继续流向可以利用杠杆和衍生品的地方。兑现时间&quot。

结尾还是一卷。这是&quot一维世界&quot。

2。到底什么是&quot价值&quot？

我们都渴望得到&quot有价值的&quot资产和拥有财富。但是什么是&quot价值&quot？是真的吗？不管你的财富构成是什么，它们的&quot价值&quot被映射在你的脑海中，并且很有可能是&quot数字&quot在价格标签上。。&quot价值&quot你的资产只不过是电子屏幕上显示的数字。

&quot；价值&quot能&#039；不要被人看见或触摸，你不能&#039；不吃不喝，你也不能&#039；t拳打脚踢；但是你仍然可以&quot讨论&quot它并用它来衡量现实世界存在的意义。

The&quot；正常主义者&quot在哲学中分为两部分：概念不是&quot真实存在&quot，但只有&quot符号&quot和&quot标签&quot用于谈论&quot真实存在&quot。除了便于逻辑推理，其实没什么。我们和动物最重要的区别是即&quot人民

&quot可以相信、思考和讨论虚构的概念，也可以&quot构建&quot一个独立的世界。

&quot；价值&quot只是一个象征。&quot价值&quot你坚信的其实是&quot构造&quot被人类自己。

太抽象了。。好在币圈的神奇之处，往往能给你莫名的灵感。

去年最火的剧是《鱿鱼游戏》。与之相伴的，还有一个项目叫鱿鱼(鱿鱼币)。从去年十月开始。其价格一周内暴涨23万倍；然后一个月后，光速为零。

鱿鱼币是骗局。虽然这是对韭菜智商的又一次侮辱。防摔&quot奇怪的是，它的设计让我明白了&quot价值&quot:

有一个&quot反倾销&gt；鱿鱼币经济模型的设计。买它并不难，但是&quot销售&quot需要满足一些条件：

总之，这是可以&#039；一旦买了就不能卖。

这样设计的目的很明显，就是扼杀&quot销售&quot在摇篮里。当&quot购买压力&quot远远大于&quot抛售压力&quot，一周飙升23万次不是太难。

这个案子给我带来了一个又一个。。短语&quot买入压力大于卖出压力&quot太熟悉了。不管什么样的&quot价值&quot——你持有的房子、股票或比特币，每当它们价格标签上的数字增加时，都会有专家将其解读为&quot买方多于卖方&quot。

这其实是一句非常正确的废话：因为&quot买家比卖家多&quot和&quot向上&quot都是一样的意思。

每一笔交易发生时，在这笔交易中只有一个买方和一个卖方。所以理论上来说，再也不会有&quot买家&quot比&quot卖家&quot以一定的价格。而如果没有卖家，交易永远不会发生，也就没有价格。

所以&quot买家比卖家多&quot意思是：因为你看到了某种&quot价值&quot，你对&quot拥有它&quot。更多的人愿意竞标。这曾经是我们在平静时代默认的常识。

鱿鱼币和灭霸一样，消灭了一半的&quot卖家&quot。&quot的数量购买&quot总是比&quot销售&quot——，所以&quot价值&quot变成了纯粹的数字游戏：

只要大家&quot购买&quot有事的话，齐新会一起努力&quot保持&quot而不是卖掉它。让&quot购买&quot总是超过&quot销售&quot，而且它的价格一定会涨，我们一定会发财。这是什么东西，是jpeg文件，还是GameStop之类的垃圾股，还是狗币？它们都与&quot价值&quot，&quot上升&quot和&quot发大财&quot。

于是出现了新的价值理论。或者应该说是一种&quot新常识&quot和信仰。这个信念的名字是&quot钻石手&quot，&quotHODL&quot；以及上一篇文章(《里拉“荣誉谋杀”》)提到的(3，3)博弈最优解。

只有一个逻辑上的小问题：如果你不&#039；别卖了，这些&quot价值观&quot将保持在&quot纸张&quot永远。一旦你试图兑现从&quot保持&quot露营到&quot出售&quot营地，&quot价值&quot可能会崩溃。

当然除非这个东西已经有了规模效应。如果10年前你用100美元买了很多比特币，10年后卖出一两个就可以实现财富。和&quot卖两个比特币&quot不会对其现价产生任何影响。——比特币成为一种价值储存。

仔细想想，大多数&quot价值观&quot世界上似乎生来就是这样。"只能买不能卖&quot——可以解释为骗局。也可以解释为&quot需求&quot。而需求就是价值。

3。货币体系灵魂的拷问

最后一个问题是来自王玮的货币灵魂三问(节目全文):

信用货币体系，尤其是&quot中央银行-商业银行&quot二元货币体系，是迄今为止人类社会最合理的模式。如果被颠覆，没有其他模式能很好地回答三个问题。我们必须有一个&quot信用创造&quot机制否则会陷入比通货膨胀更悲惨的境地。我什么都同意。只是：我们必须向前看吗？

人类社会经历过的和未来将要经历的可能是不一样的。。我们经历了一个必须用信用货币体系实现人类繁荣，维持基本物质生活水平无忧的时代。在过去的几十年里，信用货币体系确实保证了地球上几十亿人的物质生活，以至于新冠肺炎这么多年。每个人大概率还是能过上无忧无虑的生活，甚至到了大概率不会再有生存问题的阶段。

如果人类已经到了这个阶段，我们还需要这么大程度的信用来支撑&quot集中力量办大事&quot以后呢？或者我们实现了历史阶段目标。我们是否不再需要信贷乘数

来支持下一阶段的发展，而是切换到从主动脉到毛细血管的发展模式？

如果有。你真的需要一个&quot点对点&quot信息与价值完全绑定的货币体系？

虽然下一阶段最理想的货币体系还没有出现，但至少我们知道目前的货币体系是有问题的。世界需要多少？它&#039；这显然太多了。

我们习惯于&quot线性&quot思考和感觉一次只能有一个世界和一种形式。如果现在的系统发展到一定阶段，出现了巨大的问题，就会迭代成为另一个更好的&quot新表单&quot。然后向前迭代。

但是如果现实世界和虚拟世界开始&quot平行发展&quot？还会有另一个&quot自下而上&quot与信用货币的发展同步发展的形式？在我的一生中。真实世界&quot仍然会干扰&quot虚拟世界&quot很有可能。。我不&#039；我不知道超宇宙是什么样子，但是在&quot真实的人类社会&quot，绝对能找到镜子。

-end-

比特币的概念最早由中本聪在2009年提出。根据中本聪&#039；的思想，设计并发布开源软件，并在其上构建P2P网络。比特币是一种P2P数字货币。点对点传输意味着一个分散的支付系统。

与大多数货币不同，比特币不是由特定的货币机构发行的。它是根据特定的算法通过大量的计算产生的。比特币经济利用整个P2P网络中众多节点组成的分布式数据库来确认和记录所有交易行为，并利用密码学设计来保证货币流通中各个环节的安全。。P2P的去中心化特性和算法本身可以保证货币不能被人为操纵，大量制造比特币。基于密码学的设计可以使比特币只被真正的所有者转移或支付。这也保证了货币所有权和流通交易的匿名性。。比特币与其他虚拟货币最大的区别在于其总量非常有限，极其稀缺。货币体系一度四年不超过1050万，之后总数将永久限制在2100万。

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

2014年2月26日，西弗吉尼亚州民主党参议员乔曼钦(JoeManchin)向美国联邦政府的多个监管部门发出公开信，希望上述文章的内容是机构能够关注比特币鼓励非法活动、扰乱金融秩序的现状。并要求尽快采取行动彻底取缔电子货币。[3]

2017年1月24日中午12:00起，国内三大比特币平台正式开始收取交易费用。[4]

中文名

比特币

mbth

硬币

类别

电子货币

流通平台

网络[

听声音的发展历程

2008年，全球金融危机爆发。当时，有人以&quot中本聪&quot并描述了比特币的模型。

有两个

比特币

与法定货币相比，比特币没有集中的发行者，而是由网络节点计算产生。任何人都可以参与制造比特币，它可以在世界各地流通，可以在任何一台联网的电脑上买卖，无论他们身在何处。任何人都可以开采、买卖或收集比特币，外国人也可以&#039；t识别用户&#039；的身份信息。[2]2009年，不受央行或任何金融机构控制的比特币诞生。[2]比特币是一种&quot电子货币&quot，由计算机生成的一系列复杂代码组成，通过预设的程序制造出新的比特币。随着比特币总量的增加，制造新比特币的速度变慢，直到2014年达到2100万比特币的上限，挖出的比特币总数已经超过1200万。[2]

每当比特币进入主流媒体&#039；的视野，主流媒体总是请一些主流经济学家来分析比特币。此前，这些分析总是聚焦于比特币是否是骗局。现在的分析总是聚焦于比特币能否成为未来的主流货币。。这场争论的焦点往往集中在比特币的通缩特性

上。[5]

很多比特币玩家被比特币不能随意发行的事实所吸引。与比特币玩家的态度相反，经济学家对2100万比特币的固定金额持两极分化的态度。。[6]

凯恩斯主义经济学家认为，政府应该积极调控货币总量，利用货币政策的松紧在适当的时候给经济加油或刹车。因此，他们认为比特币&#039；固定的资金总量牺牲了可调整性。更糟糕的是，这必然会导致通货紧缩，从而损害整体经济。奥地利学派的经济学家持相反的观点。他们认为政府对货币的干预越少越好。货币总量固定导致的通货紧缩不是什么大事，甚至是社会进步的标志。

比特币网络通过&quot采矿&quot。所谓的&quot采矿&quot本质上是用计算机解决一个复杂的数学问题，以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。让全网大概每10分钟得到一个合格的答案。然后比特币网络会产生一定数量的比特币作为奖励，奖励得到答案的人。

2009年比特币诞生的时候，每份赏金是50个比特币。出生后十分钟第一批50个比特币产生，此时的货币总量为50。然后比特币以每10分钟50个左右的速度增长。当总额达到1050万(2100万的50%)时，奖励减半至25。当总量达到1575万时(新增产量525万)，也就是1050的50%)，奖励减半到12.5。[7]

首先，根据其设计原理，比特币的总量会不断增长，直到100多年后达到2100万。但是后期比特币总量的增长速度会很慢。。事实上，87.5%的比特币将&quot挖&quot在最初的12年。所以从货币总量来看，比特币不会达到一个固定的量，本质上它的货币总量会继续扩大，虽然速度越来越慢。所以看起来比特币是一种通货膨胀的货币。

但是，判断通货紧缩还是通货膨胀，不是根据货币总量是减少还是增加，而是根据物价总水平是下降还是上升。整体物价上涨就是通货膨胀，反之就是通货紧缩。长期的比特币的发行机制决定了其货币总量的增速会远低于社会财富的增速。

凯恩斯主义经济学家认为，物价下跌会使人们倾向于延迟消费，因为同样的一美元明天可以买到更多的东西。。消费的减少将进一步导致需求萎缩和商品滞销，使价格走低，进入&quot通货紧缩螺旋&quot。同样，通缩的钱即使不存银行本身也能升值(购买力越来越强)，人&#039；美国的投资意愿也会增加。社会生产也会陷入低迷。[5]因此，比特币是一种具有通货紧缩倾向的货币。在比特币经济中，用比特币定价的商品价格会继续下跌。[1]

比特币是一种网络虚拟货币，数量有限。但是它可以用来兑换现金：它可以兑换成

大多数国家的货币。可以用比特币购买一些虚拟物品，比如网游中的衣服帽子装备等。只要有人接受，你也可以用比特币购买现实生活中的物品。[1][1]

2014年9月9日，美国电子商务巨头易贝宣布，其支付处理子公司Braintree将开始接受比特币支付。该公司已与比特币交易平台比特币基地达成合作。，开始接受这种相对较新的支付方式。

虽然易贝市场交易平台和PayPal业务不接受比特币支付。然而，旅行租赁社区Airbnb和汽车租赁服务公司优步等Braintree的客户将开始接受这种虚拟货币。布伦特里&#039；的主要业务是为企业提供支付处理软件。该公司去年被易贝以大约8亿美元收购。

2017年1月22日晚间，Huobi.com、btc中国、OKCoin相继在各自官网发布公告称，为进一步抑制投机行为，防止价格大幅波动，各平台将于2017年1月24日中午12:00开始收取交易服务费。服务费将按交易额的0.2%的固定费率收取，主动和被动交易费率相同。[4]5月5日，OKCoin币网最新数据显示，比特币的价格刚刚刷新纪录，在截稿前触及9222点的高点。[8]

创始人听声音

2008年11月1日一名自称中本聪的男子在一个秘密的密码学评论小组上发布了一份讨论声明，陈述了他对电子货币的新想法。——比特币出来，比特币第一笔交易完成。。比特币通过揭示和分配总账摆脱了第三方机构的约束，中本聪称之为&quot区域链&quot。用户愿意奉献CPU的计算能力，运行一个特殊的软件成为一个&quot挖掘者&quot，这将形成一个网络来维持一个&quot区域链&quot。在这个过程中，他们也将产生新的钱。交易也在这个网络上延伸，运行这个软件的计算机真正解决了不可逆的密码问题，里面包含了几个交易数据。第一个&quot矿工&quot处理问题将获得50个比特币的奖励，相关交易区将加入链条。。随着&quot数量的增加矿工&quot，每个谜题的难度也有所提升，使得每个交易区的比特币生产力保持在10分钟左右。

京都大学数学教授ShinichiMochizuki[XY002][XY001]2009年，中本聪设计了一种数字货币。也就是比特币，蓬勃发展的比特币市场大起大落，其创始人的身份&quot中本聪&quot一直是个谜。关于&quot比特币之父&quot把从美国国家安全局到金融专家的人都牵扯进来，也给比特币蒙上了一层神秘的光环。

据国外媒体报道，计算机科学家泰德尼尔森(TedNelson)周日在网上发布视频称，他已经确定比特币的创始人是京都大学数学教授ShinichiMochizuki。。比特币的创始人一直使用中本聪(SatoshiNakamoto)的笔名，互联网领域对其真实身份一直

有很多猜测。纳尔逊发布了一段视频，称他已经认定望月新一(ShinichiMochizuki)是比特币的真正创始人。[9]

望月新一2013年因证明ABC猜想而成名。高中时，他就读于美国最负盛名的高中之一菲利普埃克塞特学院，两年后才毕业。望月新一16岁进入普林斯顿大学，22岁离开学校成为一名医生。33岁成为正教授，如此年轻就获得正教授头衔，在学术界极为罕见。这位数学界的超级巨星可能已经解决了这个领域最重要的问题之一。中本聪本人在互联网上几乎没有留下什么个人信息。尤其是近几年，它几乎完全消失了，所以它的身世成了一个谜。2014年3月7日，比特币创始人多里安中本聪(Dorian p.Schmidt)被找到的消息一出，迅速成为互联网上最吸引人的新闻。

与猜测相反，这可能是一个虚构的名字，&quot中本聪&quot是真名。他是一名64岁的日裔美国人，喜欢收集火车模型。曾供职于大型企业和美军，从事保密工作。在过去的40年里，中本聪在生活中从不使用真名。根据1973年洛杉矶地方法院的档案，当他23岁从加州州立理工大学毕业时，，改名为DorianPrenticeSatoshiNakamoto。从那以后，他不再使用&quot丛&quot，并与多里安本S(多里安。中本聪)为署名。[9]

产生原理听拼读法

从比特币的本质来说，比特币的本质其实是一堆复杂算法生成的特殊解。。特解是指通过一个方程组可以得到的一组无限(实际上比特币是有限的)解。而且每个特解都能解方程，是唯一的。[10]人民币方面，比特币是人民币的序列号。你知道钞票上的序列号。，你有这个账单。挖掘的过程就是通过庞大的计算不断寻求这个方程组的特解。这个方程组被设计成只有2100万个特解，所以比特币的上限是2100万。[10]

疯狂上涨

挖矿比特币，可以下载专门的比特币操作工具，然后注册各种合作网站，在计算程序中填写注册用户名和密码，然后点击操作正式开始。[11]完成比特币客户端安装后。，可以直接得到一个比特币地址。别人支付的时候，你只需要把地址贴给别人，就可以通过同一个客户端支付。安装比特币客户端后，它会分配一个私钥和一个公钥。。您需要备份包含私钥的钱包数据，以确保您的财产不会丢失。如果硬盘不幸被完全格式化，个人比特币将彻底丢失。

货币特征

去中心化：比特币是第一种分布式虚拟货币。整个网络由没有中央银行的用户组成

。去中心化是比特币安全和自由的保障。

全球流通：比特币可以在任何联网的电脑上进行管理。无论你在哪里，任何人都可以开采、买卖或收藏比特币。

独占所有权：操纵比特币需要一个私钥，私钥可以被隔离存储在任何存储介质中。除了用户自己，没有人能得到。

交易成本低：比特币可以免费汇出。但最终每笔交易会收取1bit左右的交易费，以保证交易更快的执行。

无隐性成本：比特币作为从A到B的支付手段，没有复杂的限额和手续。你可以通过了解对方来支付&#039；的比特币地址。

跨平台挖掘：用户可以在许多平台上探索不同硬件的计算能力。

优点

完全去中心化，没有发行人，就无法操纵发行数量。它的分发和流通是通过开源的p2p算法实现的。

匿名、免税、免监管。

鲁棒性。比特币完全依靠p2p网络，没有分发中心，无法对外关闭。比特币价格可能会波动和崩溃，许多政府可能会宣布它是非法的。但是比特币和比特币&#039；庞大的p2p网络不会消失。

无边框和跨界。跨境汇款会经过层层外汇管制机构，交易记录会被多方记录。但如果用比特币交易，只需输入数字地址，点击鼠标即可。等p2p网络确认交易后，很多钱就过去了。不经过任何监管机构，不会留下任何跨境交易记录。

山寨的人很难生存。因为比特币算法是完全开源的，任何人都可以下载源代码，修改一些参数，重新编译。，你可以创建一个新的p2p货币。然而，这些假币非常脆弱，容易受到51%的攻击。任何个人或组织，只要控制了一个p2p货币网络51%的计算能力，就可以随意操纵交易和币值，这将对p2p货币造成毁灭性的打击。很多仿冒品，是死在这个环节上的。比特币网络足够健壮，控制比特币网络51%的计算能力所需的cpu/gpu数量将是天文数字。

缺点

交易平台漏洞。比特币网络非常健壮。但是比特币交易平台非常脆弱。交易平台一般是网站，网站会被黑客攻击或者被主管部门关闭。

交易确认时间长。比特币钱包刚安装的时候，下载历史交易数据块会花费很多时间。。在交易比特币的时候，为了确认数据的准确性，需要花费一定的时间与p2p网络进行交互，经过全网确认后交易才算完成。价格波动很大。由于大量投机者的介入，比特币兑换现金的价格出现了过山车般的波动。。让比特币更适合投机而不是匿名交易。

公众不理解这一原则，传统金融从业者抵制这一原则。活跃的网民了解p2p网络的原理，知道比特币是无法人为操纵和控制的。但是公众不知道。我不明白很多人可以&#039；我甚至分不清比特币和q币的区别。"没有发行者&quot是比特币的优势，但在传统金融从业者眼中，没有发行方的货币一文不值。[12]

听货币交易之声

购买方法

用户可以购买比特币，同时可以使用计算机根据算法进行大量运算，以&quot我的比特币。当用户&quot我的比特币，他们需要用电脑搜索64位数字，然后通过反复解谜与其他淘金者竞争。为比特币网络提供所需的号码。如果用户&#039；的计算机成功创建了一组数字，那么将获得25个比特币。

由于比特币系统采用去中心化编程，每10分钟只能获得25个比特币，到2140年，流通中的比特币上限将达到2100万。换句话说，比特币系统可以自给自足，编码以抵抗通货膨胀，并防止其他人破坏这些代码。

交易方式

比特币是类似电子邮件的电子现金。双方都需要一个&quot比特币钱包&quot类似于电子邮件地址和&quot比特币地址&quot类似于电子邮件地址。就像收发邮件一样，发件人根据收件人直接向对方支付比特币&#039；你可以通过电脑或智能手机找到他的地址。下表，里面列出了一些免费下载比特币钱包和地址的网站。

比特币地址是一串大约33位长的字母和数字，总是以1或3开头。例如，&quot1dwuna9otzzqyhkvklj8dv1tuswmf7r3v&quot；比特币软件可以自动生成地址，生成地址时不需要在线交换信息，线下即可完成[2]。可用的比特币地址超过2个。形象地说世界上大约有2粒沙子。如果每一粒沙子里都有一个地球，那么比特币地址的总数将远远超过所有这些沙子的总数&quot地球&quot。

比特币地址和私钥是成对出现的，它们的关系就像银行卡号和密码。。比特币地址就像一个银行卡号，记录你在那个地址有多少比特币。你可以随意生成一个比特币地址来存储比特币。每生成一个比特币地址，都会生成该地址对应的私钥。。这个私钥可以证明你拥有这个地址的比特币的所有权。我们可以简单的把比特币地址理解为银行卡号，地址的私钥理解为对应银行卡号的密码。只有知道银行密码，才能使用银行卡号上的钱。因此使用比特币钱包时请保管好自己的地址和私钥。

比特币的交易数据打包成一个&quot数据块&quot或者一个&quot阻止&quot，交易被初步确认。当一个区块链接到前一个区块时，交易将被进一步确认。。被连续六块确认后，交易基本确认不可逆。比特币点对点网络将所有交易历史存储在一个&quot区块链&quot。区块链继续扩张，一旦区块链增加了新的区块，，它将不会被再次删除。区块链实际上是一组分散的客户端节点，是一个由所有参与者组成的分布式数据库，是所有比特币交易历史的记录。中本聪预测，当数据量增加时，客户端希望所有这些数据不会存储在自己的节点上。。为了达到这个目的，他采用了引入哈希函数的机制。通过这种方式，客户端将能够自动消除那些永远不会使用的部分，例如一些非常早期的比特币交易记录。

消费模式

很多技术玩家的网站。，已经开始接受比特币交易。包括Mtgox、BTCChina等网站，以及淘宝的一些店铺，甚至可以接受比特币兑换美元、欧元等服务。毫无疑问，比特币已经成为流通中的真实货币，而不是腾讯q币那样的虚拟货币。。国外有专门的第三方支付公司，类似于国内的支付宝，可以提供API接口服务。

你可以用钱买比特币，也可以当矿工&quot我的通过用计算机搜索64位数字。通过用计算机反复解密，与其他掘金者竞争，为比特币网络提供所需数字。如果计算机能够成功创建一组数字，它将获得25个比特币。比特币是去中心化的，每单位计算时间需要创造固定数量的比特币，每10分钟可以获得25个比特币。。到2140年，流通中的比特币上限将达到2100万。换句话说，比特币系统是自给自足的，翻译成代码可以抵御通货膨胀，防止别人破坏它。

支付案例

在被投资人疯狂追逐的同时，比特币在现实中已经被个体商家接受。北京一家餐厅开始比特币支付。朝阳大悦城的餐厅表示，2013年11月底开始接受比特币支付。用餐结束时，消费者将一定数量的比特币转入商店账户。，就可以完成支付，整个过程和银行转账差不多。餐厅曾经用0.13比特币结算了一顿饭650元。[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]

比特币是中本聪(几乎可以肯定)作为别名创造的。到目前为止，还没有人能够准确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年从互联网上消失了。，几乎没有留下他们可能是谁的线索。这些年来，很多人都公开声称自己是Satoshi，但都没有用不争的事实来支持这种说法。

在一个早期的比特币论坛。Satoshi说，他们从2007年开始研究比特币，比第一个区块开采早两年。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矿工。，获得了首批投入流通的50枚比特币。但是第一个盒子的奖励是不能支付的，因为代码中创世纪盒子的表述有点奇怪。BitMEXresearch发表了对比特币早期剥削的分析。得出的结论是&quot有人&quot挖掘了70万个比特币。虽然很多人认为是Satoshi，但官方并未证实。人们只能想象如果他们的身份暴露，中本聪会得到什么样的名声。更不用说他们将收集的巨额财富(虽然佐藤没有&#039；似乎没有花掉任何他们应该开采的硬币)。久而久之，很多人都自称是Satoshi，也有人是被迫的。虚假索赔自称是智的最著名的例子之一是澳大利亚学者中本聪。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辩驳的证据，但直到今天也没有成功。实际上他的&quot证据&quot证明是伪造的。

为什么聪必须保持匿名

中本聪，世界&#039；的第一个分散货币的创造者，可以说是保持匿名，因为他们的创作性质。。在创建了一个没有失败中心的协议后，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：创建它的人。去掉可能与比特币的出现有关联的单一身份。它消除了任何可能影响比特币社区政治、规则或决策的单一面孔。

不管Satoshi是谁，他们无疑都是我们这个时代的天才。比特币协议在任何合适的地方都提供了经济激励。它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，创造了一个设计精美的——比特币，这也是世界&#039；s首个——数字稀缺资产。

比特币的发明者是一个叫中本聪的日本人。2009年1月3日，世界上第一批比特币诞生，数字货币正式诞生。数字货币的价格直到2013年底才迅速上涨，从前期的10美元左右涨到900多美元。2016年比特币的热度真的起来了，价格一路飙升，被称为&quot数字黄金&quot。比特币为什么这么值钱？

1。采矿很难。比特币挖矿需要具体操作，操作时间成本非常高。前期的物质投入

也很大。

2。比特币具有货币属性，受到市场信任。比特币的加密算法很难破解，保证了它的唯一性。

3。比特币交易市场透明度高，市场价格公开透明。虚拟数字商品的流动和交易方便快捷。

4。有一些国家&#039；认可，而数字货币出台的一些政策无疑会刺激比特币的价格上涨。

物以稀为贵，比特币更是凤毛麟角。目前比较币的开采难度很大，供求关系的影响，市场供不应求的局面，无疑对价格的上涨起到了很大的作用。对于在交易平台购买比特币赚取差价的朋友要谨慎。

比特币是一种P2P数字货币。。点对点传输意味着一个分散的支付系统。2009年，日本人中本聪提出了比特币的概念。自诞生以来，比特币的价格高得难以想象。比特币为什么这么值钱？

Let&#039；让我们简单地谈一谈。

比特币挖矿机通过运行特殊程序，运行后可以获得类似任务奖励的比特币。目前比特币的产量很低，每天大约生产3600枚新币，数量有限；比特币挖矿很贵，因为比特币很热。专业挖机从1万元左右的低价到30多万的高价，前期需要大量财力进行设备投入；采矿需要很长时间。比特币挖矿是特定的复杂操作，消耗时间很长；比特币矿工消耗很大，除了自己亏损。而且会消耗很多电。彼特环球矿机日耗电量可达1.88亿千瓦时，相当于中国的1&#039；的日发电量。比特币的数量还在不断增加，有机构估计，2019年，比特币挖矿的耗电量将超过美国。

比特币的价格一直和媒体有关。在这里提醒大家，比特币的价格会涨得快，跌得也快，风险大。想买比特币赚钱的朋友一定要慎重加入。

沉寂多日的比特币以&quot勒索&quot病毒。并开启熟悉的暴走模式。这种虚拟货币叫做&quot数字黄金&quot8年暴涨300万倍，连中国大妈都入市了。有人认为这是一个传包裹式的游戏，也有人坚信比特币会成为稀缺资产。甚至有人说它会是历史长河中闪耀的一个节点，但大多数人并不&#039；不求人解，只惊叹又一轮财富爆炸。

艾比托认为是谁创造了比特币？关于比特币的发明者，一直没有定论。，常用的说

法是日语&quot中本聪&quot。2009年1月3日，世界&#039；第一批比特币是&quot挖出来&quot，这个数字货币是由一个代号为&quot中本聪&quot正式诞生了。从那以后，15个人被怀疑是&quot中本聪&quot。2014年，美国权威媒体披露，这位日裔美国物理学家的真名是&quot中本聪&quot就是传说中的&quot比特币之父&quot，但老教授坚决否认。图为很少露面的中本聪被媒体包围。，不断遮挡镜头，否认与比特币有任何联系。

2016年5月，澳大利亚工程师兼企业家克雷格赖特公开表示自己是比特币的创造者，——中本聪。但仅仅几天后？怀特本人&quot投降&quot并发表道歉信说他&quot无法出示关键证据&quot为了证明自己。尽管中本聪被提名为2016年诺贝尔经济学奖候选人，但他真正的面纱还没有完全揭开。图片：BBC(来自：腾讯图片)

克雷格怀特(CraigWhite)因涉及比特币而被警方盯上。图为澳大利亚联邦警察和税务官员搜查怀特&#039；的住所和办公室，后者&#039；美国的比特币相关业务存在税务问题。据媒体报道。神秘人物&quot中本聪&quot持有超过一百万个比特币。按照现在每个15000元的价格，他的身价超过150亿元。按照最初的严格设计，比特币的总数被限制在2100万个，目前已经开采了约1400万个。。图片：路透社

中本聪，我不&#039；我不知道他到底是谁专家。对比特币的解读是很多人头疼的事情，尤其是在理解和现实的冲突中。关注我们，为您服务，也是我们的荣幸！