（译者注：本文系CSW于2019年2月15日通过美国商品期货委员会官网对该委员会关于虚拟货币、ICO等监管政策公开征询的公开回复。在回复中，CSW以宣誓形式公布他就是中本聪，并对比特币的本质、比特币与以太坊的区分、比特币与现实金融经济的关系进行了深入评论，是十分重要的文献---刘晔律师）

对编号为83 FR 64353 的指令和其他公告的评论性回复

回复人：Craig S Wright

供职于：nChain 评论编号：61968

英国莱彻斯特大学 时间：2019年2月15日

以下是对美国商品期货交易委员会（CFTC）关于“加密资产的机制与市场”公开征询的一个通用格式回复。我叫Craig Wright 博士，以中本聪的化名完成了一项工程，该工程始于1997年，作为澳大利亚工业计划的一部分，相关文件已向澳政府提交并注册，该计划初始命名为Blacknet。

广泛流传的关于比特币及其他基于区块链的衍生系统（如以太坊）的错误理解和荒谬信息迫使我成为公众人物。我所创造的系统有部分可能被任何技术导向最具欺诈性的结果。对区块链功能的匮乏理解导致谬种流传、谎言泛滥。大量前新闻组和网络IPO的欺诈以ICO的旧瓶换新装形式沉渣泛起。

我已准备好在本回复范围之外回答CFTC提出的一切质询。需要特别提醒的是，在我谈到比特币或其他系统时，特指由原始白皮书和相应代码所定义的比特币。

无论比特币和以太坊如何迭代，系统的性质都是一众竞争性公司为积极执行规则而谋求支付。值得注意的是，当系统通过分叉改变并引入新规则时，其效果是，数字资产的前持有人获得了空投。此时，通常有一个主体发行了对等数量的新资产。关于去中心化的概念存在大量错误导向。去中心化只是加密货币的一种手段，仅意味着资产是去中心化的。所有的资产包括比特币都是由单一主体或组织发行的。

矿工并没有充当发行者。数字加密资产比如比特币或以太坊，其发行始于程序运行。系统规则的任何改变都应看成创造了新的完整系统，它模仿了原始系统，但给原始持有人发行了新的相同数量的通证。在以太坊网络中，少于20个节点控制了整个

系统。

在这里，我将把比特币作为一个协议进行重点讨论。由于竞争关系，多协议共存不可能形成稳定的平衡。

清算与结算

比特币（或通常说的区块链）改变了贸易的完成方式。比特币去除了中间人或中介的必要性。中间人系统充当了结算与清算的功能。

在过去，一个交易以典型的两个步骤完成。第一个步骤是签订买卖协议。在比特币中，这是系统用户一方的点对点。个人或公司可以与另外一个人甚至是交易所完成此一步骤。这允许数字商品及通证化产品包括证券在内的无缝和整合交易。此与现行的金融与贸易系统并无二致。当前，电子商务的销售亦存在数字化通证的运行。

比特币不同于这些的是，它解决了系统第二层的发行以及清算与结算。

清算所的存在是为了保证在节点交易时不会导致数字产品或通证的双花。

比特币是通过交易的结算步骤来解决此一问题的。一项买卖中，Alice和Bob达成交换100个特定数字产品的协议，也就是，Alice欲以美元计价的通证交换Bob持有的股票。

协议是资产转移与支付的相互承诺。

此时，比特币和“区块链”的概念来了。交易的第二步骤叫结算。通过银行或交易所，两个人联系在一起并进行商品交易。交易双方签订一个交换契约，承诺转移一定数量的有价通证，并按约定执行协议（此处执行，指交易双方的执行）。

通常，我们发现中间人促进并完成了交易的每一个步骤。一个节点交易应当包括无中间人时的直接销售或场外交易。基于通证销售的ICO，与此并无不同。ICO或其他通证是由中间人或直接的交易所进行销售的。又，此等执行过程与销售任何商品是相同的，也与交易所销售全部证券或非商品化的钱及票据完全一样。银行开具信用证，在单证相符时促成对受益人的远期付款。

这也适用于不需要直接以物换物的期货代理商、证券交易所或其他交易所。

我们可以把这些步骤叫做通证市场的前端，此处通证指证券、债券或可交易的商品。电子账本和电子交易所并不新鲜。目前，无纸化的债券和股票已相当完整。这些

记录于计算机的数据就是通证。当前通证的使用已相当普遍，电子商务的起源可上溯到1980年代。市场上的电子商务地面工作人也日益被电子交换通道所取代。纽约证券交易所、芝加哥商品交易所及其他交易所，都是在交易通证，在一定形式上，与任何“加密货币”交易所都是类同的。

比特币（或其他“区块链”）不会也不可能取代“前端”过程。买卖指令的完成就是这样的前端过程。比特币（或曰区块链）在于帮助消除“后端”中的中间人阶层。

后端中完成的那些指令引入了交易的下一个步骤--“结算”。在区块链中，此一步骤由矿工或“节点”控制。矿工充当了分布式的清算所和结算功能。就一项数字资产，资产在完成实际转移时，也意味着结算。对于证券化的，可作为通证交易的商品，承诺转移资产的结算动作可在区块链上执行，但是对于物理性商品的最后结算，需要后端的结算功能。

对于金融性资产、股票或证券交易，区块链可以去除对清算所功能的需求。

这就是后端。也就是，区块链完成了通证或电子化资产的实际转移，如同清算所完成现行交易所的通证化资产的转移一样（注：一切电子化发行的资产都叫通证，这是1980年代以来就存在的条款）。

中间人在后端的功能是保证资产转移的权利得以实现。投资人在达成资产交换协议后，应当被保证分别收到对方的资产，也就是，所有的交换和资金应当清算和结算。

后端的功能被忽视，也常在普通公众的视线之外。

后端功能在于保证被发行资产的投资人可以享有不必关心所持资产的质量、市场性、流动性或风险的权利。后端还提供了交易垃圾债券、一美元元以下劣质股票与交易AAA级主权债券或500美元一股优质股票的同等权利。

区块链，就象结算中间人一样，只是提供一种机制，以保证投资人在交易时的权利。

比特币，实际上就是任何区块链，在交易中充当了后端中间人的角色。

中央证券存托机构包括DTC（存款信托公司）、中央对手方清算制度包括芝商所的清算所，LVFTS（大额资金转移系统）和美联储等等，都是区块链将要取代的中间人实体机构。

没有一家后端实体在市场交易中有位置。它们提供的是市场交易的渠道，促进前端交易执行，担保结算，担保权利及资产在交易主体间的转移。

比特币在任何时候都不会取代前端功能。它起一个补充作用，允许一个更简单、更划算和经济可行的方式完成前端交易。

比特币（或任何区块链）添加了一个私人层允许后端流程化。常犯的错误是比特币取消了所有的中间人，比特币不会，一个区块链也不会作出这种夸大的承诺。后端的流程化，及有能力为电子化权利提供一种全球化的无缝、整合的清算与结算功能是无与伦比的革新。有一种观点认为比特币允许无规则、无监管的证券交易，这只是一种在“民主金融”外衣伪装下意图以虚假和无效宣传来从事非法投机生意的大而不当的愚蠢理论。需要注意的是，清算所是不用考虑正在交易的资产质量的，正如N.Aubryr在2008年所言，欧洲的金融管道就是如此。

在金融系统中引入区块链不会影响、削弱或在任一程度上减少前端功能对监管和控制的需求。实际上，比特币简化了交易调控政策在金融市场中的运用。添加日期、定义交易所的功能允许市场参与者简化合规性需求，而提供服务的同时允许参与者更快、更低的成本的清算则降低了“前端“市场的成本。其结果是提高了国内及国际贸易与交易的流动性。

我们可以按如下描述这个过程。假定Alice与Bob之间发生了一笔以美元换苹果公司股票的交易，比如达成了Alice按一股150美元从Bob手中购买1000股苹果股票的协议。这个交易在前端达成协议后将在后端完成清算。前端，无论是OTC还是在证券交易所，引入区块链后不会有任何变化，交易更快，结算无延迟，但是交易过程存在于比特币（或任何区块链）之外。

在传统的场景里，清算所和结算功能是为了保证Alice存入15万美元而Bob则放弃1000股苹果股票。后端可以保证Alice有可支付的资金，同时Bob有可交付的股票，且对这些股票拥有权利。以允许交易所完成交割。

比特币简化了后端过程。它允许Alice将资金放在一边而进入结算功能，以直接或原子交换方式获得Bob的已验证资产。系统的匿名性质意味着仅有交易双方及与交换或交易相关的主体知道Alice与Bob的身份。交易者的身份不可篡改地记录于区块链，价格的任何变化都具有法律效力，当违反法律或规则时，允许提醒股票交易者。

Bob和Alice在数分钟内直接完成结算，整个过程没有成本，没有上面人，没有浪费地加入第三方清算所。这就是比特币引入和进行的过程，也被其他区块链在模仿。

前端和后端

金融交易的前端远不同于后端。前端包括买卖证券或商品的一个合同交换。后端在传统上是基于一个已在前面完成、已经关门的关系。这种关系以账户的形式持续存在于中间人处。中间人所享有的权利和承担的义务不与任何特定时间相关联，也不与任何交易合同关联。前端表明买卖双方正进入一个合同关系。

后端通过中间人之间改变关系。例如，Alice通过摩根.斯坦利出售苹果公司股票，摩根.斯坦利用这些登记的股票在Bob账户上记账，后端交易就是账户的转移，即摩根.斯坦利在Bob的贷方账户记入与Alice借方账户同样的数额。这样，Alice在摩根斯坦利的账户余额减少，而Bob相应地增加。

同样的过程被区块链取代。不同于摩根斯坦利在他们的网络清算所中完成与验证账户功能，比特币允许账本直接同步与维持。

一个智能合约甚或一个简单的模板式交易都在区块链外完成协商，然后使用区块链进行结算，以保证交易是有效的（验证发生于挖矿过程），没有双花发生（诸如试图将同一份股票进行二次登记）。

比特币通过保留登记而充当了后端系统。用户通过签署加密消息而保存了被验证记录，该记录存于账本上。

比特币是“一次写入，多次读取”的账本。这模仿了许多现行的账本数据库。如果发生错误，账本可被修复，但回滚操作亦被写入以提示错误。

对于公司发行的通证化股票，如果法院判定某次特定的股票交易无效，比如交易对象受限，则即使是不可篡改的账本，公司仍能改正之。

这一过程是通过公开回赎。虽然交易各方对公众而言是匿名的，但公司或组织仍保留账本与记录，可以进行公开回赎交易。

比如，Alice出售给Bob100股苹果公司股票，但是法院判定Bob无权持有该等股票，该交易可通过无效交易而回赎。

如果Bob不签名交易致使回赎不能发生，则公司可简单地在注册表上签署一个正式的废止声明。此时，尽管Bob仍有加密账本的入口，但该入口不关联任何权利。Bob不能使用这个回购商品，不能出售，因为任何销售行为都是无效的，注册表将永久提示不仅Bob的入口而且由此发生的任何交易树都是无效的。

区块链允许引入简单的“撤回“表格。如果一个注册或交易的”撤回“是无效的，可能导致Alice对公司发起法律诉讼。

尽管区块链的记录不可篡改，如同WORM或一次写入多次读取的账本系统，但记录并非不可变化。

目的或功能

1.以太坊或相关网络的设计和发展归咎于Bitcoin core开发组对比特币强加的一系列限制。比特币在设计时，其脚本具有强大的、充分的潜能。比特币在事实上是图灵完备的，无任何自我限制，可以实现比以太坊更多的计算工作。

- 以太坊是产生于比特币的一个错误概念。这个概念是，所有节点应当平等地运行和计算软件，以实现“去中心化”。现实是，这限制了可计算性，阻止了扩容。
- 以太坊网络已经达到它的计算极限。当它扩容时，每一个用户都被其他用户复制。
- 反之，比特币只在链上留下简单验证，允许系统全球扩容和引入分布式的计算方法。
- 比特币不再扩容和维持临时的1M限制的唯一原因是Core迫使用户放弃不可篡改的账本。对比特币的劫持始于丝绸之路的失败。自从毒品市场崩溃，以及意识到不可篡改的账本允许政府更易追踪资金时，比特币开发者的目光开始聚焦迫使人们走向链外的替代方法。这导致侧链和闪电网络的发展。这些网络的设计允许间断结算，以通过清除记录而增加匿名性。
- 一个类似的系统正在以太坊上发展，叫plasma。
- 将记录移至链外的唯一目的是提高加密货币在暗网如毒品市场的利用潜力。
- 以太坊的合约问题类似于一个团体使用亚马逊云的计算服务，然后等待结果。问题是，亚马逊的每个客户端都需要在系统上自动运行其他客户端的代码。

2、以太坊是比特币的拙劣副本，其设计目的是完善智能合约和脚本的承诺。实际上这些功能在比特币中均已存在，但被core开发组禁止,其目的是在系统内寻求匿名交易。

3、这个网络已经达到它的极限，只能通过非法的投机性交易来吸引资金，这些投机性交易可以欺骗不懂技术的门外汉。限于计算条件或创造了以前从未出现且效率更高的ICOs，以太坊已不能释放新的技术。

4、通常，许多申请对货币进行记账的人们都在抱怨记录太难，这是误导与错误。所有加密货币在记账时都应当不可思议的简单。

5、这个市场的交易量极小，极易被操纵，没有数据是可信的。

6、

技术

7、以太坊是一个用虚似机器和高等级语言建造的比特币副本。但它是一个拙劣的副本，不能证实如果不是每一个单一节点运行每一个单一计算时，是否限制扩容和减少使用。

8、以太坊不能扩容。如果十个人寻求运行十个应用，那么全部的十个节点都要运行这十个应用。如果1百万个人运行100万个应用 ，那么所有的1百万个节点都得运行全部运用，其效应就是一台全球计算机复制了一百万次。在比特币，节点仅需验证结果，甲骨文数据库亦可建造允许无限扩容。

9、在2003年至2007年之间我实验过等效的权益证明（POS）机制。所有的权益证明机制最终都坍塌成一个单一控制并允许改变而不是创造不可篡改的记录。

10、权益证明在经济学上存在缺陷，其基础是寡头游戏。

11、没有正在工作的权益证明模式。

12、以太坊能够扩容的唯一方法是改变模式、模仿比特币。这些技术中的大部分我拥有专利。

治理

13、以太坊的治理模式是被一个中心团队所控制，该中心团队用了一个误导性的声明说他们是去中心化的，以掩盖数字证券的欺诈性发行。所有的选择都是由中心化的团队作出。

- 比特币的原初版本不存在分叉协议，此种不可改变性与主要证券的脆弱性大相径庭；
- 任何区块链的性质是不可篡改的系统和协议；
- 比特币核心（BTC）因徒劳地创造了一个匿名系统允许暗网毒品的使用与交易而颠覆了这个过程。

14、说区块链不分叉是社区试图误导政策制定者相信的。任何分裂都会创造一个完

整的、新的副本，并随新的协议而分配新的空投币。

- 区块链在在某种方式上是协议，如同互联网和IP相对于之前的NetBIOS和IPX一样是协议。
- 没有分布式的共识协议在这里工作，比如以太坊经典相比以太坊就是一个新协议，创造了一个改动很少的但模仿原初协议的全新系统。

其他

比特币及其所有衍生的系统，通过引入竞争性的挖矿机制，处理、结算先见交易并记录为有效，解决了数字资产的清算与结算问题。

除验证节点外再无其他事情，也没有所谓的民主化去中心化概念。去中心化的迷雾旨在播撒非法市场的种子。比特币或以太坊的控制权在运行节点的人手中，也就是运行大数据中心的人手中，不是在家庭网络的手中。

区块链系统上的每一份合约、每一个交易都与现行普通法系市场中的金融和法律结构类似。

追踪每一个加密货币轻而易举，在系统中画出每一次交易的地图也很简单，比如以太坊。那些推动系统的人试图传播一种基于区块链功能的错误观点，其目的是绕开法律。任何区块链系统中，所有的交易都是发生在两个人之间，这与发生在芝加哥期货交易市场的两个人之间的交易是同一种方式。比特币的全部革新在于确保交易不被重组，非因清算与结算交易不被改变。

比特币不分布交易，也不改变交易过程。任何区块链包括以太坊都不会与此不同。

如果有人私下告诉你区块链可以在法律、条例、规则之外运行，他们是在试图误导或欺骗，其目的是规避监管以建立不受监管的投机或暗网市场。

对于以上，我愿意宣誓作证。

顺颂政祺！

Dr Craig S Wright,法学硕士，哲学博士

编者：或许大幕即将拉开了呢。