Source: *Lianhe Zaobao,* p15
Date: 21 May 2018

科技新视野 段锦泉

加密货币在新金融时代的角色

加密货币（cryptocurrency）是依赖区块链（blockchain）技术创造出的一种虚拟电子货币，其中以比特币（Bitcoin）最广为人知。新科技本就容易带来无限的想像空间，比特币的狂涨，对区块链科技更提供了无上的加持。今年来比特币的价格下修，并未对投资人产生足够的警醒。

本人对加密货币的前景抱持悲观的看法，但对于区块链技术则充满乐观的期待。比特币的现象，本质上如同17世纪荷兰郁金香泡沫，但穿上了新科技的华丽外衣，只有待泡沫破灭后才会察觉过往疯狂的荒谬。比特币的出现加速了对区块链技术的了解和接受度，泡沫或许是人类社会进程必须付出的代价。

比特币不是一种法定货币（fiat money），电子化的法币事实上早已存在，例如电子支付系统（PayLah!、支付宝等）、地铁卡内的储值等。它们属于一种私领域的金融服务外加信用扩张，电子化货币的发行者有倒闭的风险，自然不等同加密法币。本人认为加密法币有存在的合理性，各国央行应考虑发行加密法币取代纸钞和硬币。本文最后将提出一种可行的加密法币模式。

区块链技术是分散式账本

区块链是一种透过互联网的分散式账本，用来记录交易的公共电子资料库。透过电子住址保密交易方的身份而达到匿名效果，依赖公、私钥机制进行匿名交易。区块链采用共识机制（consensus protocol），防止资料遭到窜改。不同的共识机制决定资料的可靠度和系统的运行效率。

目前已出现的共识机制可分为两大类。一种是核准会员制，赋予区块链内有限的可信节点（trusted nodes）参加共识的权限。另一种则是开放式的系统，依赖工作量证明（proof of work），也就是所谓的挖矿。任何人都可以加入挖矿，越多矿工参与，区块链的内容越无法窜改。

要了解共识机制，必先知道散列函数（hash function）的原理和特征。将一串数目、文字放入散列函数计算，信息会被打乱，最后输出一个散列值（hash value）。由于散列函数的扩散特性，即使只略改输入值，最后的散列值仍会大幅变动，造成难以回推输入值。

一个区块包含多笔交易，每个区块记录上个区块的散列值，许多区块靠散列函数串成区块链。矿工们提出的区块，包含多笔交易和附带的交易费，同笔交易可能出现在不同的区块，被接纳的新区块是矿工间竞争的结果。区块内含的交易费就是获胜矿工的报酬，交易费的多寡自然影响矿工将各笔交易加入其区块的动机。

系统让每个矿工拿最长的区块链的最后一个区块中的散列值，加上随机数字，代入散列函数，试图产生符合特定条件的散列值；解答没有取巧途径，得靠不断地重覆尝试，直到有矿工解出为止。赢得竞赛的概率取决于电脑硬体配备。除了交易费外，矿工的报酬包含由系统发行、随时间递减的加密货币。

共识机制的关键，在看似无意义的散列函数运算，尝试改变过去的交易内容，等同和所有矿工竞赛。如果能够在区块链成功地创造一个分支（forking）取代主链，事实上交易纪录就被更动了。制造分支不难，但让分支成为主链，就需要能控制超过整个系统一半以上计算的能量，基本上是个不可能的任务。

比特币的挖矿机制是个安全但没有效率的系统，保持散列函数的难度，成为维持可靠性的必要手段。每增加一个新区块需要10到20分钟，并消耗大量电力。根据Digiconomist于2018年1月8日网站发表的估算，每年因为比特币挖矿所消耗的电力，等同卡塔尔（Qatar）全国电力的年消耗率。

权益证明（proof of stake）属于另一种开放式的区块链系统，拥有越多加密货币的参与者，越可能被选为下个链结区块的决定者，避免无谓的散列函数运算。此种区块链的资料可信度，尚需时间证明。相对于开放式的系统，可信节点的区块链可具体地减少无谓运算，交易时间和成本都可大大地降低，但控制可信节点的人或组织的可信度变得至关重要。

交易效率和负面外部效应

为了维持资料库的可信度，需要10到20分钟才能支付一个汉堡，比特币能成为实用的支付工具吗？比特币的价格波动极大，商家的利润可能瞬间消失，商家会乐意接受吗？

用经济学语言，挖矿属高耗散成本（dissipative cost）。许多矿工可转嫁设备和电力成本，成本外部化是比特币的严重缺陷。根据Quartz（2018年1月6日）的报道，有名麻省理工学院的学生，在宿舍使用学校的电脑与电力挖矿，赚了许多钱。类似成本外部化的事例，也可发生在任何大学。

比特币的疯涨促使更多人加入挖矿行列，散列函数的难度会自动调高，共识机制浪费的资源更多。让挖矿成本内部化只是种理想，在现有的结构下是个不可能的任务。据媒体报道，中国政府继禁止加密货币的交易后，已开始禁止挖矿。阻止负面外部效应的扩大本是政府的职责，中国政府的果断作为合情合理。

加密货币的前景

比特币本身不具隐含价值（intrinsic value），就如同不具隐含价值的法币。储值是货币的另一功能，可用来储值的主因是它可在未来换取商品、服务或有价资产，有限的供应量自然是一必要条件。法币是法定的交易媒介，发行的政府必须控制货币供应量，不然就会如阿根廷的比索那样的失控。若任何人都能够随意创造货币，货币必定失掉价值。

比特币的设计是在2140年达到2100万枚的最终供应量，但现已经产生了比特币现钞（Bitcoin Cash）、比特黄金（Bitcoin Gold）的分支。事实证明，比特币并没有实质上的数量限制。前文提及挖矿能有效地阻止分支，但强制分支（hard forking）属于一种规则的改变，只要足够比特币的参与者同意，可从主链某一区块开始使用新规则产生分支。强制分支不会在技术上影响到主链的进行，但会改变使用比特币的兴趣，从而影响到主链的长期发展。

加密货币可视为互补货币，政府当然只会容许互补货币的有限流通，因为大量流通等于创造了一家不需对公众负责的央行。匿名性加上不受距离、国界限制，透过比特币洗钱是必然的结果。比特币的疯涨及做为洗钱的管道，注定招徕金管单位的关注、干预。新科技的华丽外衣，让加密货币得到较大的发展空间和时间。但本人相信，时间只会证明加密货币是场超高成本的社会实验。

加密法币的可行性

金融机构账户的电子化，加上许多其他电子支付管道，法币事实上已经高度电子化了。许多电子支付能在一两秒间完成，比使用现钞方便，也大大降低商家的交易成本。大部分电子化法币留下实名电子纪录，地铁卡之类虽具匿名性，但只适用于小额交易。

电子化法币事实上具有信用风险，假如说支付宝倒闭了，账户里的法币就可能全部或部分随之消失，原因当然是支付宝信用扩张的结果。经验告诉我们，信用扩张属于企业所无法抗拒的诱惑。老牌的金融集团如雷曼兄弟倒了，当红辣子鸡如支付宝就一定可屹立不摇吗？要想创造出不具信用风险的电子化法币，非得中央银行来主导，以加密法币逐渐取代纸钞和硬币，减少印钞、铸币的成本。

央行发行加密法币具先天技术上的优势。因为银行系统本就是受监管的、互相依存的信任体系。从区块链的角度，信任节点的共识机制最为合适加密法币，银行成为自然信任节点。银行的大小可用来决定分配到的工作量，等于是信任节点加上权益证明的新共识机制。银行的确认工作没有报酬，可归为银行执照所附带的责任。因为避免了无谓的挖矿，交易效率大增。因为节点可靠，交易纪录的可靠度得到保障。越大的银行，越有资源、能力增加所需要的电子设备，也越有动机维持加密法币的稳定。

加密法币区块链仍是一个开放系统，信任节点或是其他节点都可参与组建新区块，报酬来自于每一笔交易所附代的交易费。如果希望小额交易能免除交易费，只需规定每一个区块，保留固定的空间给不含费用的小额交易。掉了电子钱包，如同掉了普通钱包内的现钞。如果电子钱包内的重要信息已有备份，遗失者不需要靠好人好事的发生，即能失而复得。简而言之，加密法币将比现钞更具优势。

虽然政府可以采用实名制的电子钱包，个人认为并不是明智的选项。只有维持匿名性，加密法币才能真正取代纸钞、硬币。现今防止洗钱的策略和措施，一样可用在加密法币上。对所有非由银行和其他合法金融机构的加密法币交易，可定一个上限，例如1万新元，同时限制个人拥有电子钱包的数量。

现今各国央行都面临伪钞的问题，加密法币有真正解决防伪的可能，是政府单位可以思考并研拟发展的方向。当然执行面会产生许多挑战，如同任何重大政策的推动，应当从试点起步，推动加密法币尤须慎重。面对金融科技的发展，政府可采不同的态度。个人认为，与其让新科技牵着鼻子走，还不如正面地拥抱，转为增加人民福祉的工具。

作者是新加坡国立大学
风险管理研究所所长
商学院怡和合发金融学讲座教授