蔡维德：几千万美金的教训——SWIFT的困境和出路

金融界网站 10-11 08:15

1. SWIFT的实验

SWIFT即环球同业银行金融电讯协会，是银行同业间的国际合作组织，成立于一九七三年，目前全球大多数国家的银行都使用SWIFT系统。可以说它是世界上最重要的金融组织之一。它从2016年就开展了区块链实验。2017年，SWIFT宣布和许多金融机构启动大型验证项目，并认为很快就能完成。

2018年3月，SWIFT发布报告阐述实验结果，相关媒体不断发布消息，说这次实验非常成功。SWIFT相关主管还上网络视频媒体宣告项目成功，并解释项目是如何达到目标的。但同时宣布放弃区块链计划[13]——难道是因为项目成功所以关闭了？

其实，这种项目肯定是“成功”的，因为据国外媒体估计，该项目共花费了几千万美金。而且该项目使用了“领先的分布式账本技术”，Hyperledger Fabric 1.0。所以，它必须成功。这符合美国政府的一贯传统：项目进行一半以后，是一定会成功的，不然相关官员都要负责任。所以国外项目如果已经过半，不论结果多么失败，对外多半会宣称项目成功。

所以看一个项目是否真的成功，要看项目结束后的行动。这次项目发布成功后就停止，代表它没有达到预期目标。无疑，这对区块链发展来说不是好消息。就像2017年加拿大央行宣布其区块链实验结果一样[1]，许多人都因此感到失望。

2017年加拿大央行的报告主要针对R3CEV的Corda，而这次2018年报告SWIFT使用的是Linux Foundation的Hyperledger（超级账本），这两个都是专为金融场景设计的，它们的失败代表区块链技术的确还不成熟。这两个项目都有大量基金和著名公司支持，许多人还认为它们是两项“不可能失败”的项目，但是初期的实验还是没有成功。这代表什么？这是我们关切的问题。如果问题是基础性的，表示我们应该放弃区块链；但如果是其他原因，包括技术不够成熟，我们就不该放弃，并且应研究这次POC项目失败的原因，以后再不犯同样的错误。

Hyperledger并不像有人认为的那样是IBM公司的项目。这项目的确是由IBM牵头启动的，但很快它就捐给了Linux Foundation社区， Hyperledger也因此成为社区项目。为了区别起见，IBM又开发了IBM Blockchain Platform （IBM区块链平台），并且后来又采用其他区块链协议，例如Stellar（卫星）区块链，Stellar用在IBM2018年推出的World Wire项目，也是IBM公司推出的最重要的区块链项目， 就是数字美元项目，

也是美国政府支持的。请注意World Wire项目没有用Hyperledger的区块链协议。除了Stellar 协议，IBM公司表示他们还在物色其他区块链协议。

SWIFT原文报告中用DLT（分布式账本），而极少用区块链（Blockchain）。本文还是根据中文传统使用区块链这名词，除非在引用报告原文的时候，为忠于原文使用DLT[2]。

2. SWIFT POC的设计

SWIFT是现在金融中心的中心，一举一动都受到金融公司关注。2016年SWIFT表示重视区块链发展，并发布白皮书。这很合逻辑，因为那时许多人都认为区块链将会使SWIFT在几年后消失。当时还有许多人认为清结算公司、金融资产（例如股票）注册公司、证券公司都会因为区块链的出现而消失。多家清结算公司、银行、注册公司都发表白皮书，对此表示怀疑（就是表示即使区块链时代来临，他们以后还会有价值！），虽然他们也是最积极从事区块链研究的单位。

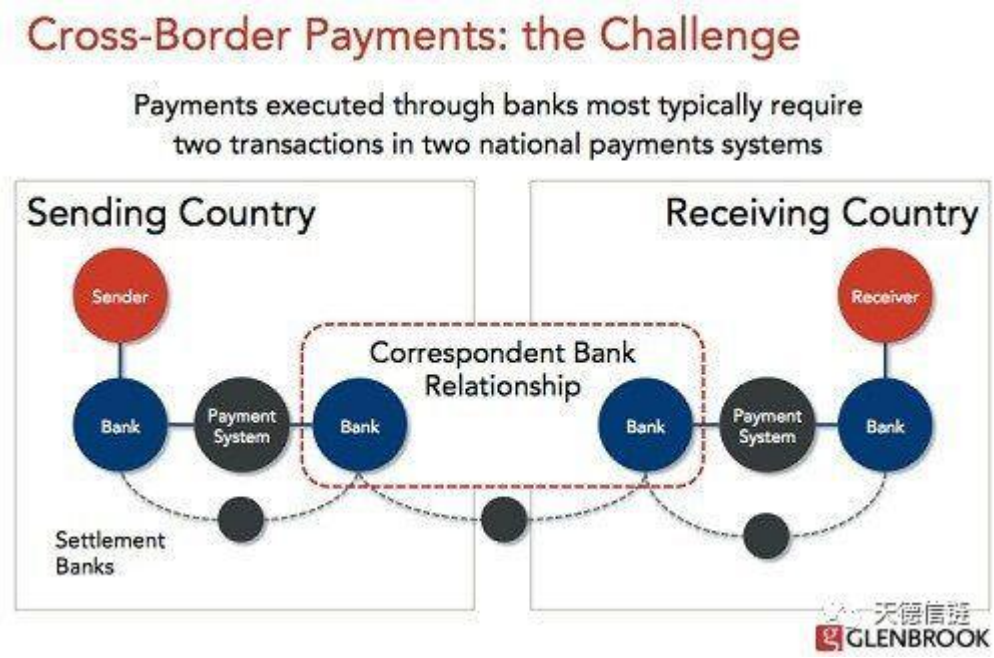
非常可惜的是，因为可能会影响机构自身的生存，许多相关研究报告都未做公开。例如欧洲一些大的清算公司做了一些实验，却没有出任何实验报告或是新闻发布，但是没有从事这些实验的第三方却放出消息说区块链不适合清算作业（可能大家不知道，几个月前，同一位专家还发文表示清算是区块链最好的应用场景！），因此估计实验没有成功。这次SWIFT的报告也是如此。他们大声宣告实验成功（却停止了项目），却没有发布实验细节，连基本架构都不发表，很明显就是不要其他人知道细节。

虽说如此，我们还是可以从各种报告包括第三方的报告中得到许多信息。例如在2016年，SWIFT已经提出区块链在银行系统使用的基本条件：1） 强管理性； 2） 数据控制； 3） 符合监管； 4） 标准化； 5） 身份证识别； 6） 安全和网络安全； 7）可靠性； 8） 扩展性。这些原则和加拿大、欧洲和日本央行使用的PFMI原则非常相似 [4]。这和其他公开信息提供了许多线索。

2017年，SWIFT联合34家金融机构进行区块链的实验，包括来自中国的机构，如中国银行，其中28家机构参与测试。2018年3月，SWIFT发布其POC项目报告，并表示这是迄今为止世界上规模最大的区块链POC项目。

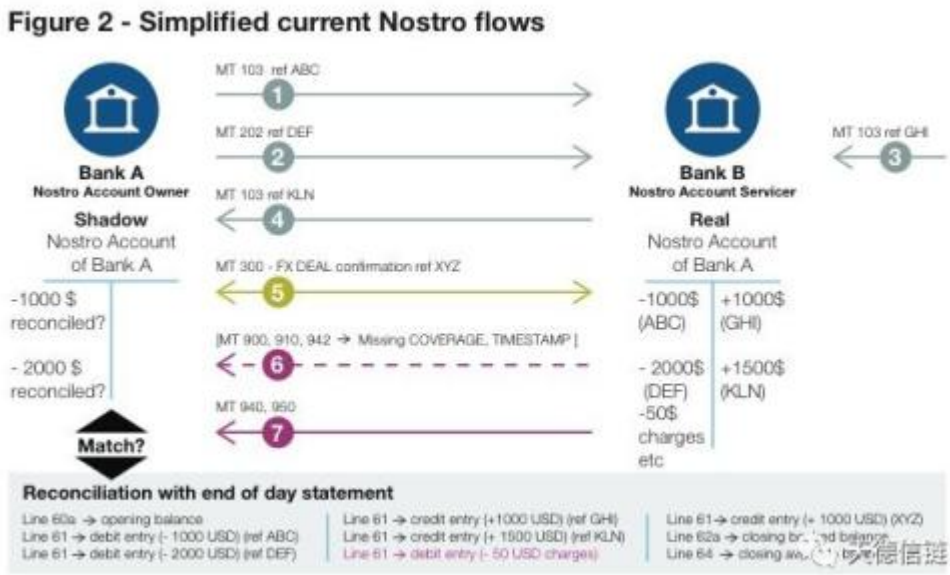
该POC项目是在国际往来账户上使用区块链。下图描述了SWIFT项目中的跨境交易流程。国内银行与国外银行都有专门的代理银行处理跨境交易，国内银行想要向国外其他银行发送交易，首先要将交易发送给国内代理银行，再由国内代理银行发送给国外代理银行，国外代理银行再将交易传给其他银行，由此完成跨境交易。国内银行与

国外银行的账户称为往来账户（Nostro Account）。对于一家大型银行而言，每天可能会有数十亿美元的交易流入流出往来账户。

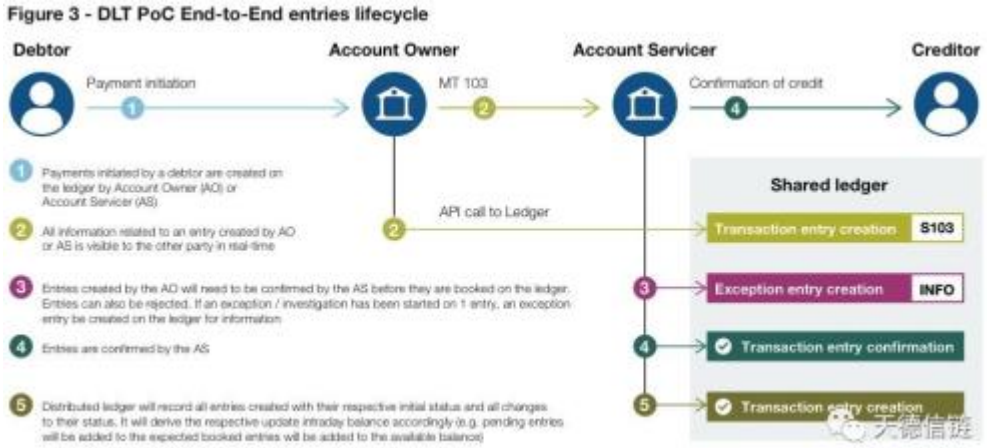


下图是SWIFT从2016到2018年的年日交易数统计表，从中可以发现交易数逐年增长。截至2018年7月，SWIFT每日交易数达到3千万笔，差不多是一秒347笔交易。

SWIFT目前的流程可用下图表示：



SWIFT的区块链POC实验中流程发生了改变，新流程如下。



这次POC建立在SWIFT已有的基础设施GPI和流程之上。流程有3个特性：

1）所有事件都是交易，通过往来账户进行收付款。

2）在理想情况下，所有交易都是实时完成，并立即确认交易完成。

3）没有中央权威机构，因为所有交易是点对点的。在一般情况下（除非出现错误），交易是不可撤销的。

上述场景和现在数字代币（例如比特币）交易非常像，因此SWIFT认为这是最合宜的应用场景。但是，该场景使用了现有的SWIFT技术和标准，例如使用ISO 20022数据标准，通过“模拟后台办公工具”生成各个点对点账本之间的流量。并且也使用SWIFT的管理模式， 例如基于SWIFT的“日内流动性标准规则手册”以及为SWIFT新的全球支付创新（GPI）基础设施开发的独特端到端交易参考（UETR）的概念。又

使用基于标准的业务标识符代码（BIC）识别各方，和SWIFT控制的证书颁发机构（CA）来颁发证书，为各方完成身份认证。

3. POC的结果

POC的官方结果当然是正面的， 而且极为成功（原文“Extremely Well”）：交易通过SWIFT网络实时传输，结果太好了（原文“Fantastic”）。对Hyperledger也是赞誉有加，非常满意。

但细读报告，从字里行间却得到不同信息。SWIFT对该项目不满意，因为SWIFT每天都有这样的交易，而且数量大的多，也没有使用区块链。SWIFT自己列出4个疑问：

1）今天只有44％的跨境支付需要实时确认，而且这数量不会增加很快。为了这44％交易，SWIFT需要对系统进行大幅更改吗？

2）虽然POC 成功，但是所有参与银行都需投入大量资金来改变后台支持软件。但现在这不是一个刚需（第一个观点），大部分银行不会愿意做这样的投资。

3）每个参与银行都有自己的应用场景，没有公认的共同解决方案。这是因为主要参与银行已在现有系统上投入了大量资金，而且功能强大。他们不认为在这上面投资是值得的。小公司由于不需要实时交易而且负担不起，也不会投资。

4）系统不能单独作业，为了涵盖所有往来账户的交易，如果系统要上线，必须大大扩大现在POC的范围，如需更改外汇系统和证券交易系统。换句话说，现在的POC只是一个小型实验，离实际系统还有很长距离。

除功能之外，最终报告还指出了一些严重问题，即区块链技术还不够成熟。报告特别提到Hyperledger的通道（Channel）的问题。通道是Hyperledger扩展性和保护隐私性的一个重要技术，但SWIFT报告对此技术采取保留态度。

通道是Hyperledger Fabric中的概念，它实质是由排序节点划分和管理的私有原子广播通道，目的是对通道信息进行隔离，使通道外的实体无法访问通道内的信息，从而实现交易的隐私性。网络上每个交易都在一个指定的通道中执行，且需要通过锚节点的认证和授权。要加入一个通道的每个节点都必须有身份标识，用于鉴定其节点和服务类型。虽然任意一个锚节点都可以属于多个通道，维护了多个账本，但不会有任何账本数据会从一个通道传到另一个通道[3]。

如果链上有n个参与者，如果所有参与者都会彼此交易，出于隐私考虑，交易双方必须有一个专用通道，所以需要（n-1）*（n-2）/ 2个通道。通道数随着参与方的增加而快速增长，这一增长速度虽然不是指数型的，也是非常快的。如34家银行，需要528（=33x32/2）个通道。根据SWIFT的计算，如果“系统”上线，则需要超过100,000个通道（这代表SWIFT参与金融机构超过470家）。SWIFT 认为这470家金融机构对于所需花费的代价还没有做好准备。报告轻描淡写地指出这些问题将带来“重大的运营挑战”。该解决方案在POC时就已无法负荷，随着规模扩大，问题会愈发严重。

总之，SWIFT认为区块链在往来账户的实际应用上，无论是功能、成本效益、技术还是操作，都是一条死胡同（dead end）！这批评真是非常严厉，与2017年加拿大央行的评语相比有过之而无不及。加拿大央行报告主题就是负面的信息，而SWIFT报告主题是正面的信息，但字里行间却充满令人窒息的批评。

而且，SWIFT认为该项目应该是区块链最理想的应用案例，如果连这么匹配的应用场景，使用现在最好的区块链技术，都会遇上困难。那么对于其他更复杂的金融应用如股票交易和结算而言，区块链技术更加不切实际。

IBM也有回应[12]，承认收到SWIFT公开的批评，并且开始改进通道和相关技术。

4. 讨论

SWIFT对区块链的批评的确严厉，对该POC项目至少有以下两点值得讨论：

1）为了保护隐私权和扩展性，该POC采取通道的解决方案，这种设计明显不能满足实际需求，另外还有可能造成严重的中心化。有其他方法解决这问题吗？

2）该POC设计很明显不是“改变世界的革命”，只是对现有系统的改进。就算这改进系统成功部署，仍然会面对来自其他系统的挑战，例如IBM在2018年提出的数字法币系统[6]。

4.1.采用通道来维持隐私性和扩展性

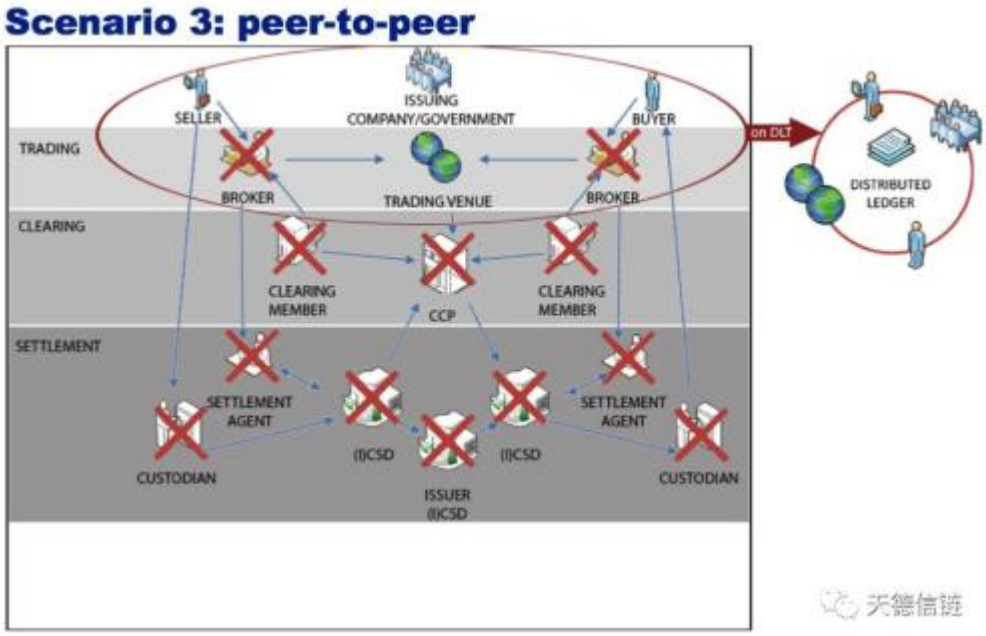
很明显，SWIFT希望使用这种方法解决数据的隐私性问题。目前解决隐私性问题的方法有三种架构上的方案：

1）2016年欧洲央行提出的一链通天下的模型 [7]；

2）2018年SWIFT使用的通道模型；

3）2016年我们提出的熊猫模型，并可使用大数据版区块链 [8]。

欧洲央行的一链通天下的模型

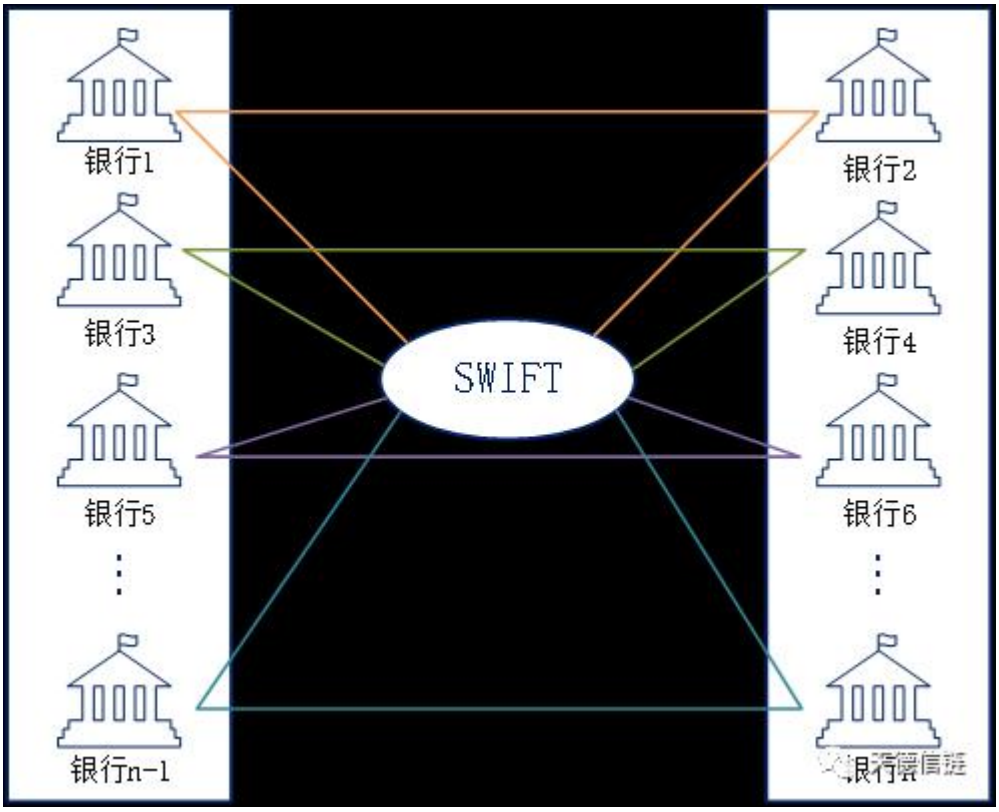


上图是欧洲央行在2016年提出的设计，在该模型里面，所有金融机构都在同一区块链上而且有节点，都在链上交易。这种的模型，代表所有金融结构都可看到其他机构的交易，都参与验证每一笔交易，甚至每一金融机构都可看到其他机构的所有账号信息。

这种设计是“不隔离”，因此隐私性极差，且因每个机构都要存储其他银行的账号信息，存储需求大增；由于每一笔交易都要被所有金融机构验证，共识成本增大，每个节点需要大量算力才能完成。

2016年的时候我们就估计每个节点需要超算所才能解决计算力问题。注意一下，不是一个超算所可以解决所有节点计算力，是每个节点需要自己的超算所。这样的设计是不可能投入实践的，因为代价太大。所以2018年，欧洲央行放弃了这一设计。

SWIFT 的通道模型



在SWIFT项目中，因为每个银行都不想和其他银行分享数据，所以每个银行都和另一个银行及SWIFT组成一个通道，如上图，不同颜色的线代表不同通道。在POC系统，因为有34家银行参加，需要支持528个通道。如果SWIFT原来系统上线，则需要10万个通道。

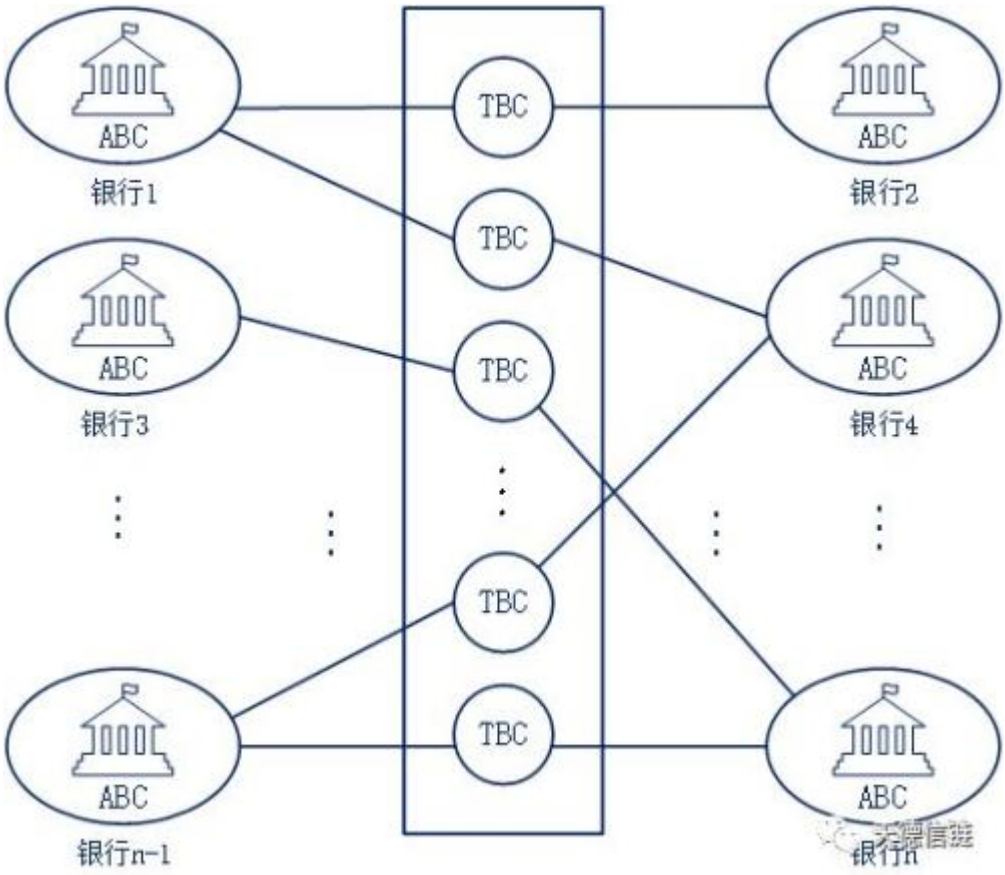
这种设计实际是“软隔离”，保护了隐私性，但其完全由软件技术来维持，共享硬件资源，与硬隔离相比，隐私性要差。同时这种设计也意味着系统有一个大中心——SWIFT， 就是SWIFT有其他所有银行的所有数据。这违背了非中心化的设计理念。中心化系统的可靠性可能是个问题。

这种设计有一定扩展性，但有限度，不能无限扩展。每个通道只需要完成两个金融机构之间的交易，计算力不需要太大。

该系统中存在一个中心SWIFT包含了所有机构的信息，可靠性好。加拿大央行2017年的报告里面一个重要批评就是在数据可靠性上。不要认为使用区块链，数据就可靠，这是加拿大央行的批评。

但是软件开发成本太高，这是SWIFT批评Hyperledger的一个重要观点，每个通道都不同，每个银行需要建立469个通道，需要和469家银行分别合作完成。

中国熊猫模型



第三种设计如上图，这是我们在2016年提出的熊猫模型解决方案，使用了ABC-TBC架构，将账户信息和交易信息分开，保证了隐私性。其中每个银行使用一个ABC用于存放账户信息，每两个银行间的交易使用一个或是多个TBC。每一个ABC都不和其他ABC通话，保护每个银行客户的隐私。TBC上只有交易数据，没有余额信息，还可采用其他加密方法保护交易隐私。不同TBC可以并行处理交易，增加速度。

熊猫模型可以有4 - D的架构：1）多链，不是像前面两个设计使用单链； 2）每条链上可以有多节点； 3）每个节点可以有多服务器； 4）每个服务器上多存储。这种4-D架构保证系统数据的可靠性。

这种设计是“硬隔离”，由不同服务器来维持链，对隐私性的保护最好。它既可是非中心化的设计，也可让SWIFT（中心节点）继续存在。如果SWIFT存在，则可设计只能看到TBC的数据，看不到其他银行ABC的数据。

4.2.SWIFT可能还会面对其他系统的严重挑战

SWIFT的实验结果证实了区块链系统不够效率且需要大量投资的说法是正确的。这次实验即使成功，而且还上线，也不是“改变世界的革命”

2016年英国首席科学家是用“改变世界的革命”来形容区块链带来的变革，因为区块链会带来流程革命 [10, 11]， 不只是技术革命。但是可以清楚看到，SWIFT实验的目的就是在现今系统里使用区块链，采用现在的基础设施和协议，例如ISO 20022和GPI。在旧流程上使用区块链，这不是革命，这是改进或是升级。这就好比火车发明之后，仍然让马在蒸汽机前跑一样！

这代表什么？SWIFT代表的是旧金融市场，旧流程，旧技术，他们使用区块链在现在系统里面，就是用旧思想和旧流程来思考区块链应用。这次POC就是新酒放在旧瓶里面。就如圣经里所说，新酒应该放新瓶里面，如果新酒放在旧瓶里就会造成新旧技术不合，会遇到许多困难。

SWIFT是现在金融市场的中心。这传统的金融市场经过70年来不断投资和优化，系统已经非常成熟而有效率，这是区块链系统所无法比拟的。

最近以IBM为首的新金融科技公司的出现挑战这一金融体系。IBM和Stronghold在2018年7月宣布发布数字美元稳定币，由美国政府背书，实际上就是美元数字法币。令人惊讶的是这数字法币会和12个国家做法币交易。这样跨境交易根本不需要经过SWIFT的基础设施，这场实验如果成功，以后可能真的取代SWIFT。这是直接挑战SWIFT在这方面霸主的地位。

自从2018年7月以后， 金融市场分为两个金融市场：

一是传统的金融市场，以SWIFT、央行、商业银行为代表；

二是新金融市场，主要是数字货币，但是最重要的是“数字美元”。跨境交易不用经过SWIFT，国和国之间可以直接点对点交易。数字美元由美国政府一个单位（FDIC）担保系统上资金，也受政府监管。这数字美元项目是由IBM主导。数字代币因其特性存在局限性，不能主导新金融市场，但是数字美元可以。

这意味着两套正规金融系统同时出现。新金融设施需要二三十甚至是四五十年才能成熟，达到现在金融系统的效率。

这个项目IBM也不使用Hyperledger，而是使用Stellar的区块链。为什么在他们最重要的区块链应用系统里，IBM自己都不用Hyperledger？这值得我们深思。

新金融系统如同小婴儿一样，才刚出现，还没有长大成熟，缺乏基础设施，使用者非常少，交易量异常小，却是一个新市场、新流程，即分布式市场和流程。

旧金融系统好像罗马军队一样，成熟、强大，拥有众多单位和从业人员，占据了大部分金融市场，但是使用旧技术，而且中心化。

这是一场新旧金融之间的大战！究竟结果如何，让我们拭目以待！

更多精彩资讯，请来金融界网站(www.jrj.com.cn)