区块链技术和智能合同在未来经济中企业联盟的应用

李智健
（以太坊中国基金，香港 852）

摘要：信息技术已经突破了行业和商业惯例(Jakšič & Marinč，2015)。互联网创造了许多新的经营方式，甚至创造了几年前甚至不存在的新兴行业。信息技术的真正吸引力在于它为企业和人们合作创造了全新的、更有效的方式，区块链技术(Blockchain Technology)正是引领商业社会的革命，这技术促使了企业联盟、金融领域使用区块链和产生新的经济组织，这些都成为本文的研究内容。

关键词：区块链技术；智能合同；以太坊企业联盟；超级账本

一、解构区块链技术

区块链技术是一个可公开、可分布和可信的分类帐，可供大家使用。它也是防篡改的，这意味着当一条信息被放入区块状时，它不能被篡改和被忽视。在技术上，任何一种有价值的无形信息都可以放在分类账中。区块链技术不需要其用户之间的任何信任，这允许在没有第三方的情况下进行交易。目前，这技术最被人注意的正是称为虚拟加密币位的比特币和以币，但是本论文目的专注于区块链技术运用金融领域和它促使于企业联盟。

“经济学人”(2016b)指出，虚拟货币比特币背后的具体技术与区块链的一般思想是不同的。Buterin(2015)突出了私人和公共区块链之间的区别，它是封锁又是公开的，因为所有参与者都可以使用该区块。该技术其重要性，正面对挑战。尽管区块研究技术的应用已经在多项研究中得到成果，目前和未来仍将能推进的。Malinova 和 Park(2016)解释了基于区块链应用在土地登记册，它如何能够抵制腐败现象、证券交易和市场设计如何重塑和加信任度。Pinna 和 Ruttenberg(2016)在研究中声称，这项技术应用是智能合同，其取代目前传统贸易机构的功能。根据统计预测，这项技术将与二十年前的互联网一样革命化。

本文在几个不同的领域进行了应用，特别关注企业联盟和金融部门如何利用嵌入式技术，如“经济学人”(2016b)所述，该技术有机会特别影响依靠人与人信任的行业。Murray(2016年)，区块链技术将真正彻底改革金融机构，甚至让一些职业，如证券经纪人消失。相反，这项技术同时会产生新的就业机会(Murray，2016)。最极端的假设是区块链技术逼使不再需要银行的可能性，金融机构更有可能积极利用区块链技术，正因为它能消失传统金融机构。

区块链技术提供的许多应用需要金融部门的行为者之间的共同标准和合作，回顾过去几年，金融技术初创企业与世界各地约50家金融机构之间的合作。这种合作的目的是发展区块链技术，并将其适应各金融机构。他们图提出如何使用这项技术的共同标准，这在竞争激烈的金融世界中肯定是一个挑战（“经济学人”，2016a)。根据 Trautman(2016)的说法，尽管面临诸多挑战，但是区块链技术有可能破坏而且又重塑银行业的世界。

区块链技术将比特币进一步发展，提出的智能合同。它突破当前的金融体系，且具有很大的潜力。它让中介机构，例如国际支付或证券交易，金融机构能降低成本，提高了效率。基于区块的流程减少资本，风险降低(“经济学人”，2016a)。区块链的透明度和可靠性造成了金融体系的信心。同样，每一区块有价值的信息都投入到区块中，因为一些服务可能比其他服务更适合区块链。尽管如此，金融机构将受益于应用区块链技术。区块链技术以假名 Satoshi Nakamoto(The Economist，2015)诞生，Nakamoto 正是比特币的隐藏发明者，2008年出版了《比特币：对等电子现金系统》。这项研究被认为是一个黑客或一群黑客制造(Trautman，2016)。可以肯定，比特币是世界上第一个分散的公共分类帐，它今天在全球获得了全球的地位。然而，比特币的成功来自于其基础的加密技术，即区块链技术(Pilkington，2015)。这项技术最近也成为研究人员的热门话题，被认为是比比特币更为重要的现象。该区块是分布式分类帐的一个特征，这意味着它不受任何单一演员的控制，而是由几位参与者维护。这使得不了解或甚至相互信任的人形成一个可信赖的分类帐，其中记录了信息。任何一种非物质信息，如财产权和虚拟货币交易都可以存储在这些块链中。三个基本特征是它是一个共享的，值得信赖的和公开的分类账(“经济学人”，2016b)。区块链技术的核心思想是所有人都可以参与，但仍然由用户单独控制或拥有。正是按照现在的时间保持分类账的网络参与者的帮助和合作。再者，细数区块链五个的基本功能：

第一，去中心化结构，成为交易媒介：纯数学方法建

立信任关系，区块链技术的信任机制建立在数学（非对称密码学）原理基础上，借助开源算法，使系统运作规则公开透明。在这种模式下，各个节点之间进行数据交换时可以自动达成交易共识和自动信任，在保证信息安全的同时有效提升系统的运营效率和降低成本。

第二，数据信息不可篡改，具储存价值：配合“时间戳”等技术，区块链将系统成立以来的所有交易全部记录在数据区块中，所有的交易活动都可以被追踪和查询，并且形成的数据记录不可篡改。这便于对交易活动进行追踪，可以有效解决交易验证和交易后续纠纷等问题。

第三，分布式记账与存储，记帐单位：区块链的记账和存储功能分配给了每一个参与的节点，因此区块链系统不会出现集中存储模式下的服务器崩溃等问题。分布式记账与存储使区块链系统在运转的过程中具有非常强大的容错能力，即使数据库中的一个或几个节点出错，也不会影响整个数据库的继续运转，更不会影响现有数据的存储与更新。同时，基于区块链技术建立起来的数据库是一个所有节点共同组成的超级大数据库，系统发生的所有交易活动（包括开户、登记、交易、支付、清算等）的信息，都可以存储在这个超级大数据库中，使业务模式具有极高的包容性。

第四，智能合约可灵活编程，契约执行：区块链技术基于可编程原理内嵌了“脚本”的概念，这使得后续基于区块链技术的价值交换活动可变成一种灵活智能的可编程模式。例如，房产交易通过“智能合约”进行，“智能合约”处理协议和任何指定条件的区块链中的数字规则。购买和销售仍然可以通过代理进行，或者由智能合约体现销售规则并自动作出此决定。每处房产的区块链会随着账本中交易的增加而增长。没有代理人、减少产权律师和土地所有权机构的中介服务，保证了区块链技术在未来的发展能形成一种可持续进化的模式。

第五，透明信息背后的匿名保护，电子公证：区块链的信任基础是通过纯数学方式背书而建立起来的。区块链技术利用公钥地址代替用户的身份信息，从而能够有效实现匿名性，使人们在互联网世界里实现信息透明共享的同时，不会暴露自己的真实身份信息。区块链上的数据都是公开透明的，但数据并没有绑定，人们无法知晓交易背后的参与者是谁。透明交易背后的匿名性特点，极大地保护了参与者的个人隐私。

- 交易媒介
- 記帳單位
- 儲存價值
- 電子公證
- 契約執行

图1 区块链的基本功能

二、区块链之共识机制

（经济学人，2016b）这个协议被称为“共识机制”，该技术通过基于数千个“节点”的对等网络进行功能，节点可以随时随地来到网络（Nakamoto，2008）。新的区块通过一个称为采矿的过程由专门的节点出生，换句话说就是矿工（mining）。这些矿工通过合作进行匿名操作，并尝试解决数学难题，从而为区块链创建新的块。在货币交易中，多名矿工验证交易并监督所有事项的顺序，并且进行交易的人实际上拥有他想要支付的钱；如果是有效的交易，矿工确认变更。此后，类似的交易按照同一个方块中捆绑的时间顺序排列，从长远来看，它们形成了一连串的区块链。

（“经济学人”，2015年）该区块链包含自区块状物出生以来发生的所有接受的交易（Peters & Panayi，2015），所有信息在任何给定时间都可用。Peters和Panayi（2015）已?将区块链称为按时间顺序分类帐，或者由计算机组成的网络记录事务的数据库。区块链技术的安全性即使这些块是公开的，它们是安全可靠的。根据“经济学人”（2015年）的观点，至少有两个因素可以增加封锁的安全性。首先，可靠性与机会有关。没有人可以预测哪个矿工会在任何时候更新和解决数学谜题。第二，由于时间历史，可靠性得到提高。篡改交易历史的尝试将会显示出来，篡改块的哈希值变得不同，不再符合以下区块。此外，矿工们不断关注交易，拒绝接受不一致的交易。

事实上，如果有人试图重写历史，这个人就需要知道如何解决一个非常困难的数学难题来创建一个新的区块。如果作弊者能够比非作弊矿工更快地建立链条，其他人将开始在假冒链上工作，因为矿工们始终致力于最长的链条。因此，这几乎是不可能的，欺骗者不太可能从修改的区块开始创建一个新的区块，同时延长新链，比矿工延长原始链的速度更快。（“经济学人”，2015年）、Nakamoto（2008）在研究中强调，要在一个方面改变历史，需要重新制定所有的区块。因此，历史和机会使作弊非常困难。

本论文承认的区块链不仅限于比特币，各种非物质资产也可以记录和转移到区块状（“经济学人”，2016b）。对这

表1 分布式分类账基础设施的杠杆来源：资本市场中的Celent blockchain

1、资本，资本效率提高
2、不变性，记录的耐久性，无法检查数据或更改数据
3、不可侵犯性，没有机会多个版本的真相
4、控制，控制分配给分布式分类帐的所有成员
5、分发，交易与网络的所有成员联播 - 每个网络节点的数据和资产成本，寻找摩擦成本的指数下降
7、合规性，合规性是隐含在分类帐中，审计和监管访问也是如此
8、澄清，本地智能合同或智能合约叠加的潜力来绑定事务数据

项技术能够实现的人才依然很稀少，但是转型中经济如何发挥作用，特别是破坏靠信任的行业具有很大的潜力。该区块是不断更新的，它给系统中交易的公共分类帐，并在资本市场中运用（表1）。它记录对等网络中的任何事务，使其不能被更改或篡改，亦是透明的，允许以分散的方式处理交易，并消除中央机构验证信任和价值转移，例如货币的需要。

三、以太坊的智能合同是一个新的突破

智能合同（或简称合同）是存储在该块中的“自主代理”，被编码为将契约引入区块链的“创建”事务的一部分。一旦成功创建，智能合同就被识别出来，合同地址每个合约都有一些虚拟硬币（以太币），拥有自己的私有存储，并与其预定义的可执行代码相关联。合同状态由两个主要部分组成：私人存储和它所拥有的虚拟硬币（以太网）的数量（称为馀额）。合同代码可以像传统的命令式程序一样操纵变量。以太坊（Ethereum）合同的代码是一种低级的，基于堆栈的字节码语言，被称为以太坊（Ethereum）虚拟机（EVM）代码。用户使用高级编程语言（例如Solidity（类似JavaScript的语言））来定义组合，然后将其组合成EVM代码。要在地址上调用合同，用户将一个交易发送到合同地址。交易通常包括：用于执行在以太网中的付款（对于合同）和/或用于调用的输入数据。

（Loi Luu elc，2015）智能合同是一个聪明的合同是一个程序，运行在区块上，并由协商一致协议执行正确的执行（Nick Szabo，1997）。合同可以编码以其编程语言表示的任何一组规则－例如，当某些事件发生时（例如，托管系统中的安全存款的支付），合同可以执行转移。因此，智能合同可以实施广泛的应用，包括金融工具（例如子货币，金融衍生工具，储蓄钱包，遗产）和自我执行或自主治理应用，例如外包计算分布式赌博（资料：EtherDice smart contract is down for maintenance. https://www.reddit.com/r/ethereum/comments/47f028/ etherdice is down for maintenance we are having/）。

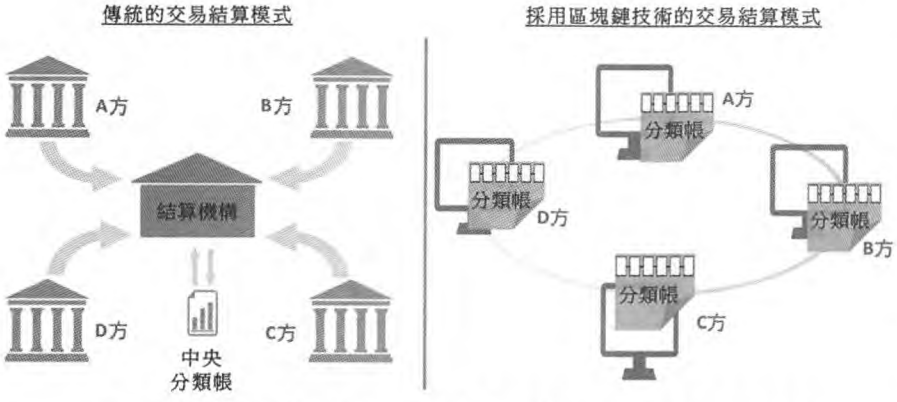

图2 传统模式与采用区块链技术模式在交易结算安排的不同之处

Oliver Wyman（2015）及IBM Corporation（2016）。

智能契约由地址（具有160位标识符）标识，其代码位于区块链上。用户通过将交易发送到合同地址来调用当前加密货币中的智能合同。具体来说，如果一个新的事务被该块接受并且具有一个合同地址作为接收者，那么采矿网络上的所有参与者都将以块状态和事务有效载荷的当前状态作为输入来执行合同代码。网络通过参与协商一致的协议来同意合同的输出和下一个状态，其中以太坊（Ethereum）是一个更新的隐藏式，它是一个有前途的图完整智能合同平台，它与比特币不同，以太坊支持有状态合约，其中值可以在块链上持续以在多个调用中使用。仅在过去六个月里，以太坊网络已经部署了约15,000个智能合同，这表明该平台的使用量稳步增长，更多的公开展示和其他类似的项目，如RSK Labs，2015 and Counter Party（资料：Counterparty platform. http://counterparty.io/，2015），以太坊出现在比特币块之上，我们预计智能合约数量将会增长。智能合同的关键在于条款和信息可否放在合同之中，如果条款和合同自动执行（“经济学人”，2016a）如果条款未达成，合同不生效。将信息嵌入到区块链中的可能性使得能够在不需要第三方确认的个人之间建立安全合同。双方都不能违反智能合同中的协议条款（Pinna & Ruttenberg，2016）。

智能合约在实际操作上，区块链系统可分定为公开或私人系统。公开的区块链系统开放予所有使用者，可自由读取或核实分类帐数据，这与虚拟货币交易系统相类似。私人区块链网络只限于一羣预先选定的参与者使用，而这些参与者拥有权限更新分类帐。参与者可来自同一机构，或某一行业的不同机构，他们签订非正式协议、正式合约或保密协议厘定彼此之间的权责。

图2显示了传统模式与采用区块链技术模式在交易结算安排的不同之处。在区块链网络中，每台电脑系统均备存一个相同的区块链复本，此复本会自动更新每项交易，而电脑利用精密的运算程序就交易作出核实，从而确定交易金额及其他资料，令区块链成为一个记载了所有交易活动的分类帐。处理交易的电脑系统一般分布于不同位置，并且不由任何一个机构/参与者单独拥有或控制。由于区块链是分布于网络而非备存在中央服务器，故此区块链有时亦被称为分布分类帐（distributed ledger）。

举例，中国香港特别行政区政府展开区块链的金融服务开展探讨，资料来自ISE15/15-16研究主题：财经事务、金融科技、Fintech、分布分类帐、共享分类帐：

四、区块链技术在金融领域的应用

区块链技术被认为有潜力革新传统金融交易的运作，因此备受金融机构的重视。来自一份业界报告，资本市场在2015年投资于区块链技术的金额达7,500万美元(5亿8,400万港元)，并预期在2019年，有关投资额将会大幅增加至4亿美元（31亿1,000万港元）Aite Group (2015)。区块链技术在金融领域可使用的方向：

1、数字货币

比特币是目前区块链技术最广泛、最成功的运用。而在比特币基础上，又衍生出了大量其他种类的去中心化数字货币，统称为“竞争币”或“山寨币”。比较着名的竞争币有IXCoin、莱特币、狗狗币、蝴蝶币、瑞波币等。其中，IXCoin为第一款竞争币，通过更改比特币的一些参数，从而增加了货币的发行量；莱特币通过改善比特币技术的一些算法（主要改善了区块链“挖矿”工作量证明算法），将新数据区块产生的时间从比特币的10分钟缩短为2分半钟。狗狗币(Dogecoin)是一种基于Scrypt算法的小额数字货币，是目前国际上用户数仅次于比特币的第二大虚拟数字货币。

2、支付清算，现阶段商业贸易的交易支付、清算都要借助银行体系

这种传统的通过银行方式进行的交易要经过开户行、对手行、清算组织、境外银行（代理行或本行境外分支机构）等多个组织及较为繁冗的处理流程。在此过程中每一个机构都有自己的账务系统，彼此之间需要建立代理关系；每笔交易需要在本银行记录，与交易对手进行清算和对账等，导致整个过程花费时间较长、使用成本较高。与传统支付体系相比，区块链支付可以为交易双方直接进行端到端支付，不涉及中间机构，在提高速度和降低成本方面能得到大幅的改善。尤其是跨境支付方面，基于区块链技术构建一套通用的分布式银行间金融交易系统，可为用户提供全球范围的跨境、任意币种的实时支付清算服务，跨境支付将会变得便捷和低廉。

3、银行征信管理，商业银行信贷业务的开展，无论是针对企业还是个人，最基础的考虑因素都是借款主体本身所具备的金融信用

商业银行将每个借款主体的信用信息及还款情况上传至央行的征信中心，需要查询时，在客户授权的前提下，再从央行征信中心下载信息以供参考。这其中存在信息不完整、数据更新不及时、效率较低、使用成本高等问题。商业银行可以用加密的形式存储并共享客户在本机构的信用信息，客户申请贷款时，贷款机构在获得授权后可通过直接调取区块链的相应信息数据直接完成征信，而不必再到央行申请征信信息查询。

4、权益证明和交易所证券交易，在区块链系统中，交易信息具有不可篡改性和不可抵赖性

该属性可充分应用于对权益的所有者进行确权。对于需要永久性存储的交易记录，区块链是理想的解决方案，可适用于房产所有权、车辆所有权、股权交易等场景。其中，股权证明是目前尝试应用最多的领域：股权所有者凭借私钥，可证明对该股权的所有权，股权转让时通过区块链系统转让给下家，产权明晰、记录明确、整个过程也无需第三方的参与。以区块链为蓝本打造下一代金融资产交易平台，在所有交易所中，纳斯达克证券交易所表现最为激进。其目前已正式上线了Linq区块链私募证券交易平台，可以为使用者提供管理估值的仪表盘、权益变化时间轴示意图、投资者个人股权证明等功能，使发行公司和投资者能更好地跟踪和管理证券信息。此外，纽交所、澳洲交易所、韩国交易所也在积极推进区块链技术的探索与实践。

5、保险管理

随着区块链技术的发展，未来关于个人的健康状况、发生事故记录等信息可能会上传至区块链中，使保险公司在客户投保时可以更加及时、准确地获得风险信息，从而降低核保成本、提升效率。区块链的共享透明特点降低了信息不对称，还可降低逆向选择风险；而其历史可追踪的特点，则有利于减少道德风险，进而降低保险的管理难度和管理成本。目前，英国的区块链初创公司Edgelogic正与Aviva保险公司进行合作，共同探索对珍贵宝石提供基于区块链技术的保险服务。中国国内的阳光保险于2016年3月8日采用区块链技术作为底层技术架构，推出了“阳光贝”积分，为国内第一家开展区块链技术应用的金融企业。

6、金融审计

区块链技术能够保证所有数据的完整性、永久性和不可更改性，因而可有效解决审计行业在交易取证、追踪、关联、回溯等方面的难点和痛点。德勤公司从2014年起成立了专门的团队对区块链技术在审计方面的应用进行研究，目前已与部分商业银行、企业合作，成功创建了区块链应用实验性解决方案。其开发的Rubix平台，允许客户基于区块链的基础设施创建各种审计应用。普华永道自2016年宣布大举进军区块链领域研究后，已经招募了15个技术专家探索和研究区块链技术，并与专门研发区块链应用的Blockstream、Eris科技公司合作，寻求为全球企业提供区块链技术的公共服务。此外，区块链技术在P2P借贷平台、去中心化的众筹平台等方面，也有巨大的应用潜力和应用场景，吸引了资金投入和应用探索。

五、区块链使各行业充满新发展气象

我们再细看智慧合同在应用方面的发展情况，根据数位商会(Chamber of Digital Commerce)区块链行业主要

表2 智能合约:12种商业及其他使用案例的益处和挑战

使用案例	益处	挑战
1、数码身份	个人数据控制；企业不在需要保存数据。	单点失败就会成为黑客攻击目标;第三方机构可能成为数据泄露源。
2、记录	降低法律费用;自动贷款跟踪;自动记录清理。	摆脱纸质备案;UCC和政府备案/归档仍需人工处理,容易出错。
3、证券	数字化的端到端证券工作流程;自动股息支付;股票分割。	更替人工和纸质流程;中介增加成本和风险。
4、贸易融资	更快的付款批准;更有效的贸易、运输和合同协议。	实体文件管理;文件欺诈;重复融资。
5、衍生产品	自动结算和外部交易处理；实时位置评估。	多余的OTC资产服务流程；纸质交易协议。
6、金融资料记录	交易数据的完整性和透明度,降低会计数据管理成本。	会计制度存在错误与舞弊;资本密集型过程。
7、房产抵押贷款	自动解除留释权；降低误差和成本;提升财产数据可见性;验证。	各缔约方之间的摩擦(合约,借款方,房地产的产权记录);数据隐私。
8、地契记录	抵押贷款欺诈。	多方共同拥有同一财产；人工延迟;身份验证。
9、供应链	简化复杂的多重机构系统；跟踪库存;降低欺诈和盗窃风险。	数据不兼容和供应链盲点。
10、汽车保险	使用传感器为车辆带来一种'自我意识'和损失估计;提供一种保单数据存储库。	主观性的损失诊断;重复的形式和保险商验证。
11、临床试验	增加试验可视性;数据共享;自动征求患者同意;病人隐私。	申报不足;不一致的同意管理;机构延迟。
12、癌症研究	数据共享;病人隐私。	跨机构的繁琐的研究共享过程。

的贸易协会，联同智慧合约联盟（Smart Contracts Alliance)和德勤今年初发布了一份智能合约白皮书,标题为《智能合约:12种商业及其他使用案例》(Smart Contracts:12 Use Cases for Business&Beyond:A Technology,Legal &Regulatory Introduction,December 2016)这份白皮书涵盖12种智能合约能够重新定义自动化的不同领域(谭嘉恩,2015),内容包括:

第一,数码身份(Digital Identity),个人对自己数身份的资料，如信誉和拥有的数资产等能够作出管控。在「以用户为中心的个人互联网」(User Centered Internet)中，智慧合约可以指定那些个人资料可以或不可以与企业共享。

第二,记录(Records),智慧合约可以把各种规条进行自动化的合规性,降低法律的交易费用,也可轻易自动进行记录清理。

第三,证券(Securities),可协助私人企业自动股息支付,股票分析和负债管理流程。

第四,贸易融资(Trade Finance),可把信用证和贸易支付的流程进行自动化,这样一来,可以在买家、供应商和金融机构之间,创建一种更高效,风险更低的贸易平台。

第五,衍生产品(Derivatives),智慧合约可以为衍生工具提供执行标准和确立交易规则,简化场外交易(OTC)金融协议。

第六,金融资料记录(Financial Data Recording)，可以用作一种企业级会计帐本,去精确与透明地记录财务资料。

第七,房产抵押贷款(Mortgages),智慧合约可以自动执行房产交易的各个环节，包括支付处理,房产抵押权

第八,地契记录(Land Title Recording),智慧合约可以以提高交易的完整性,效率和透明度,提升财产转让流程,从而减少讹诈的糾纷。

第九,供应链(Supply Chain),智慧合约可以为供应链的每一个环节,提供更高度的可见性和透明性,并与物联网设备协调,从工厂到销售点,有效追踪货物在供应链内任何一个环节的情况。

第十,汽车保险(Auto Insurance),在汽车行业智慧合约可以实现保险索赔流程自动化，提供近乎即时的处理、验证和付款流程。

第十一,临床试验(Clinical Trials),在医学研究领域,临床试验或者药物研究,往往涉及参与者的个人资料隐私，都是一些敏感协议，智能合约可成为一种用于跨机构可见性的机制,并创建基于隐私的规定,以改善机构间的资料共享。

第十二,癌症研究(Cancer Research),类似临床试验,在癌症研究方面,智慧合约可以实现患者资料管理自动化，在保护患者隐私时,资料得到更多的参详与研究,发挥合众之力,更有效推动癌症研究。

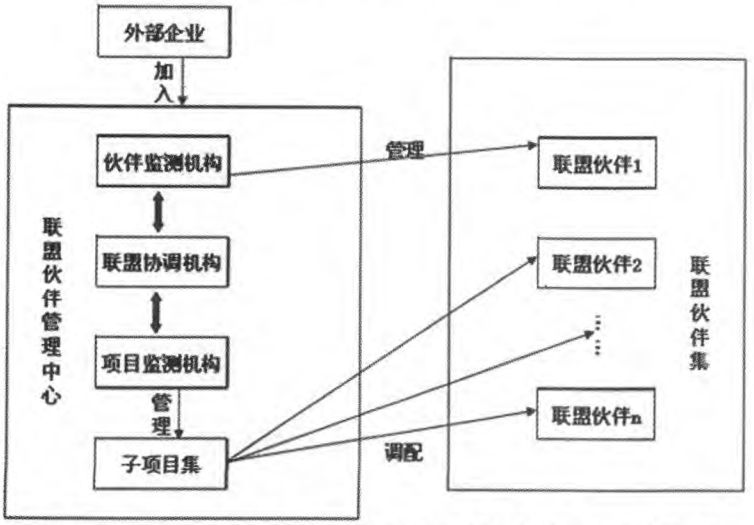

图3 引用战略伙伴联盟模型了解以太坊促使企业联盟(EEA)

六、以太坊促使企业联盟(EEA)

全球企业对区块链技术的需求迅速升温,微软以开放且强大的 Microsoft Azure 为基础的「区块链即服务(BaaS)」,提供快速、低成本、低风险的云端平台,并于今(2017)年二月底结盟国际区块链技术应用组织以太坊(Ethereum)及多个国内外尖端金融、科技及新创企业,共同组成企业以太坊联盟(Ethereum Enterprise Alliance, EEA),期以透过跨产业交流场域并共创产业区块链应用,拓展全球发展区块链应用所需要的技术及生态体系。

EEA 的成立,目的在于推动以太坊企业版基础架构持续进步,并赋予其足以服务企业级需求之技术。国际区块链技术应用组织以太坊创办人 Vitalik Buterin:「以太坊为世界上独一无二,同时与有充满活性的公共开发者社群,以及专为企业需求而提出的区块链基础建设,并从两个社群的互动中获得许多经验和价值,这个社群代表了成千上万来自世界各地的开发者,将让区块链技术更上层楼。」

引用战略伙伴联盟模型,每个联盟伙伴都与本企业有基于某项目、某业务、某职能的合作关系;联盟"伙伴集'行动态增减;项目监测机构主要负责管理联盟"子项目集",对联盟"子项目集"实施动态管理并为相关项目调配合适的联盟伙伴;联盟协调机构则是一个支持中心,主要支持伙伴监测机构和项目监测机构的顺利运作,通过控制机制协调可能产生的冲突,通过信任机制建立彼此间的信赖,通过学习机制培育企业的创新能力。从理论层面管理联盟"子项目集"就是使用区块链技术和共同确认使用以太坊的货币,在战略上扩大了产业范围,又增加了交易的效益,见图 3。

台湾微软云端及企业平台事业部副总经理李玉秀表示:「微软区块链即服务(BaaS)及 Microsoft Azure 相较其他平台具备更多关键优势,让企业更快速部署区块链,例如:Microsoft Azure 上的 Market Place 已提供多种分布式帐本节点及开发工具,企业只要 one click 即可完成简单的部署,让企业可更专注在情境应用的设计。而企业最在乎的资安问题,我们亦提供中介软体服务(Azure middleware services),包括 Crypt lets 技术、Azure Active Directory(Azure AD)身份识别管理,以及金钥保存库提供身份验证与金钥管理等。过去,大家习惯将区块链与金融科技(FinTech)划上等号,随着生态系的越发丰富,我们预期很快就可以看到更多非金融产业的创新应用惊艳问市。」

区块链技术新创 AMIS 帐联网执行长刘世伟表示:「以太坊为目前业界最为多元的区块链基础架构,拥有最活跃和凝聚力的开发者社群,无论是台湾本土还是全球市场,AMIS 认为以太坊平台具备革命性潜力,能符合当地企业及法规的需求。AMIS 帐联网公司将持续积极投入以太坊社群及以企业太坊联盟的开源社群。」。

富邦金控创新科技办公室副总经理李相臣表示:「富邦金控不断朝向国际化及数位化迈进,区块链技术被视为关键技术,在区块链应用实作 – BraveLog 诞生后,我们期望借助企业以太坊联盟,更进一步与全球各地的顶尖企业合作,跨越产业与地理疆界共同为区块链应用商业化。」

企业联盟 2017 年 3 月宣布的 86 名新加入成员当中包括:德勤、三星 SDS、加拿大国家银行、丰田、DTCC(The Depository Trust & Clearing Corporation)、三菱日联金融集团、华尔街区块链联盟(WSBA)、台新金控以及台湾金融科技协会等。(完整成员名单详见:entethalliance.org)另外,由近 30 家强大企业组成的团队成员还包括埃森哲,西班牙桑坦德银行,英国石油公司(BP),瑞信、瑞银、西班牙对外银行,纽约梅隆银行,汤森路透和创业公司 ConsenSys 和 BlockApps。

七、企业以太坊联盟(EEA)愿景白皮书

与此同时,这个新成立的 EEA 已经发布了一份愿景白皮书(Vision Paper):企业以太坊愿景(Enterprise Ethereum Vision)。在这份白皮书中,EEA 讨论了很多有关可插入共识(Pluggable Consensus),治理,互操作性,以太坊协议更新,安全代码执行,存储和性能优化有关的话题。EEA 已经确定了 2017 年的 5 大目标:第一,开发一种充分的模组以太坊实施来分离和定义网络与存储层之间的清晰的接口,这是一种可插入共识的原型,可以最大限度地减少共识算法切换所需要进行的代码更改;第二,测试可能的共识算法,以及数据隐私和许可框架;第三,开发出一套明确的能力与性能特点,要能满足企业的需要;第四,开发出 EEA 的愿景的参数;第五,利用一种稳健的治理流程来确保方法的一致性。

(信息来源:https://www.infoq.com/news/2017/03/Enterprise-Ethereum-Vision)

八、企业以太坊联盟(EEA)使用超级账本项目

EEA 与超级账本项目都正在研究开源区块链项目,并且两个项目在成员方面也存在交集,让我们看看 EEA 与超级账本项目的相同点和不同点。首先,超级账本项目正在从零开始开发自己的区块链,原来由 IBM 领导。另一方面,EEA 正在合作修订一种现有的以太坊区块链来满足企业需求。第二,超级账本项目是一个社区,旨在防止项目被某一方或团体所控制。尽管 IBM 是超级账本项目的创始成员之一,但是超级账本的核心是通过成员合作的方式来进行的,没有单一方能够进行决策。正在现有以太坊平上创建和添加新服务,旨在尝试将以太坊带到与企业对企业需求和模式相同的水平,而不是一个必须从零开始创建这些能力的组织。第三,超级账本 Fabric,它是使用最广泛的超级账本项目,从基础开始创建企业级(私有)区块链。注意超级账本本身是一个项目集合(与 Apache 相似),将最

终变得可以被整合和重复使用(Iroha,Sawtooth Lake,Cello,Composer,和 Dashboard)。相反,EEA是围绕着以太坊平台成立的,而以太坊平台是作为一种公有无需许可区块链创建的。

2017年8月31日,以太坊区块链的以太坊基金会(Ethereum Foundation)与俄罗斯国有开发银行(Vneshe-conombank)签定合作协议,共同发展与推动俄罗斯国内区块链研究。根据他们的联合声明指出,以太坊基金会将与俄罗斯国有开发银行一同成立一个区块链研究中心,提供专业训练和技术支持,培训人才专注研究分布式账本和以太坊平台开发。合作计划的最终目标是希望在俄罗斯国内凝聚更多区块链人才,促进以太坊和其他区块链应用发展。俄罗斯的区块链活动「区块链:俄罗斯的新石油(Blockchain:The New Oil of Russia)」中进行,合约由俄罗斯国有开发银行的高层与 Vitalik Buterin 共同签署。2017年6月,就有传 Vitalik 与俄罗斯总统普丁私下会面,俄罗斯对区块链发展的态度逐渐开放,8月初更有数个俄罗斯银行组成联盟,测试利用以太坊区块链进行支付和结算超级账本项目,区块链跨越了国际领域,被受政府认周,并且交易商品时使用,虚拟数码资产渐渐有实业挂勾。

九、总结

金融科技产业中的区块链技术,提出了去中介化(Disintermediation)的交易机制,具有一致性(Consensus)、来源可追溯(Provenance)、不可更改(Immutability)与决定性(Finality)等关键特性,成为一种受信赖的金融科技技术。现今许多先进国家已投入大量资源于区块链的技术研发中,区块链联盟以及以区块链技术为基础所发展的金融科技市场平台(Market Platforms)等,值得深入予以探讨,包括相关政策法规制定、金融服务推动目标、交易资讯流之资料应用,为本研究的原因。

本研究基于「个案研究」及「文献分析」所搜集到的资料撰写内容,研究以区块链技术应用为主线,提出关键成功因素如下:一、区块链技术内容,提出各国的应用例子。二、区块链技术应用就是智能合同,开始使用在各行业之中。三、区块链技术应用平台政策法规与增进企业的利益层面,促成了企业以太联盟,这正是共享经济的延申、打破资讯不对称的传统经济学理。

区块链技术还处于成长期,若区块链技术要成为真正成熟的技术至少需要五到十年的时间。目前,区块链发展速度已经非常明显,因此,区块链技术使用在金融领域和促使企业联盟,背后正代表这技术的认受性和公信度。无疑,区块链技术一定是未来经济的新宠儿。

参考文献

[1] Buterin,V.(2015).On Public and Private Blockchains. Etherum Blog.https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

[2] Christopher Allen & Shannon Appel cline(2016),Smarter Signatures:Experiments in Verifications,A White Paper from Rebooting the Web of Trust II:ID2020 Design Workshop, Smarter Signatures v1.0,9/7/16.

[3] Jakšič,M.,&Marinč,M.(2015).The Future of Banking: The Role of Information Technology. Bančni vestnik,68.

[4] Japan Exchange Group.(2016)News Release:Commencement of Proof of Concept Testing for Blockchain Technology.

[5] Loi Luu,Jason Teutsch,Raghav Kulkarni,and Prateek Saxena (2015):Demystifying incentives in the consensus computer. In Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security,CCS 15,pages 706-719.ACM,2015.

[6] Long Finance.(2014)Chain Of A Lifetime:How Blockchain Technology Might Transform Personal Insurance.

[7] Morrison&Foerster LLP.(2016)Demystifying Blockchain and Distributed Ledger Technology-Hype or Hero? 5 April.

[8] Mckinsey&Company (2015)'Beyond the hype:Blockchains in capital markets',availableat:www.the-blockchain.com/docs/McKinsey%20Blockchains%20in%20Capital%20Markets_2015.pdf (accessed 9th August,2016).

[9] Pinna,A.,&Ruttenberg,W.(2016).Distributed Ledger Technologies in Securities Post-Trading Revolution or Evolution? ECB Occasional Paper,(172).

[10] Sutardja Centre for Entrepreneurship&Technology of the University of California Berkeley.(2015)?Blockchain technology beyond Bitcoin.

[11] The Financial Times(2015)Technology:Banks seek the key to blockchain. 2 November.

[12] White&Case.(2016)Beyond Bitcoin:The blockchain revolution in financial services.

[13] 陈怡之(2017):区块链应用于金融交易关键成功因素之研究[D].台湾:中兴大学,2017.

[14] 程华、杨云志:区块链发展趋势与商业银行应对策略研究[J].中国金融监管研院 2016(6).

[15] 谭嘉恩:(2017) 区块链应用商机不容错过香港科大资讯《解牛集》[J].信报,2017 .

[16] 袁勇、王飞跃:区块链技术发展现状与展望[J].自动化学报,2016.

[17] 蒋润祥、魏长江:区块链的应用进展与价值探讨[J].甘肃金融,2016.

(责任编辑:周瑞华)