



区块链之跨链技术介绍

文 | 高志豪 编辑 | 李佳琪

如果说共识机制是区块链的灵魂核心，那么对于区块链特别是联盟链及私链来说，跨链技术就是实现价值网络的关键，它是把联盟链从分散单独的孤岛中拯救出来的船舶，是区块链向外拓展和连接的桥梁。

在加密数字货币的区块链公网百花齐放发展的同时，出于交易性能、容量规模、隐私保护、合规监管的考虑，联盟链和私链技术被商业机构特别是金融机构广泛采用。相比公链来说，现在联盟链的发展势头要耀眼得多，但我们需要警惕的是，不要让联盟链变成纯粹的中心化或多中心化。相对于传统的区块链设计技术，现在大部分的联盟链显然没有提供太多的可实现不可逆交易或降低中心化风险的方式，这些中心化式的信任会使联盟链区块链因网络审查和简单故障点的失误，导致整个网络处于风险之中。

相比之下，在比特币等公网区块链的框架下，交易一旦完成传输确认无人能更改，无论是法院执行令还是少部分参与者的冲动都无权冻结资金或征收罚款。对于联盟链，无论是主观的团体作恶或因不可抗的审查或多节点故障等风险，都让他们的用户们对此却无法彻底信

任和放心。Elwin认为，联盟链和私链的方式从一定程度违背了区块链的去中心价值和信任体系，也让区块链里面的数字资产不能在不同的区块链间直接转移，主动或被动地导致了价值的孤岛，联盟链和私链的局限性令各种连接不同区块链的跨链技术开始应运而生，也开始受到人们进一步的关注和探索。

目前关于区块链的跨链技术还在研究和试行中，并没有被大规模使用，Elwin将于下文尝试为大家介绍目前较为人熟知的跨链技术的研究案例，当中包括侧链、M2、Poladot、Interledger等。

1.侧链

自比特币7年前诞生以来，数以百计的竞争币被开发出来，有着各种新的优势和特性，但比特币的霸主地位依然屹立不倒，而很多复制竞争币却湮灭在历史中。虽然比特币有不少

高志豪 (Elwin)

资深互联网技术专家，拥有超过18年的企业IT系统、互联网产品、移动应用、区块链等产品设计及多终端跨平台架构和系统开发经验，目前是广州两家软件公司及互联网公司的技术总监。

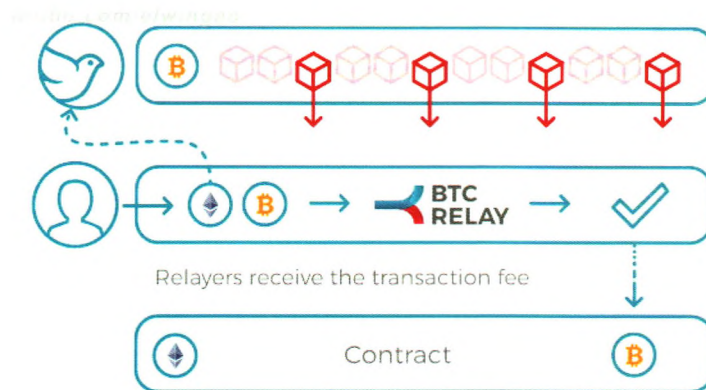


图1 BTCRelay示意图

缺点和限制，但比特币却又是最能去中心化、最多分布节点、最公平的区块链应用，从数字货币地位、节点数量、去中心的权威等方面来说比特币是很有优势的。另一方面，类似以太坊、比特股的区块链在技术和应用上后来居上，对比特币区块链产生相当大的威胁的同时也给了比特币开拓了新的思路。为了在创新的同时，又保留比特币网络的去中心化，侧链技术由此推出。

在广义上，侧链是以锚定原生数字资产为基础和其他帐本资产在多个区块链间的转移的新型区块链技术。其中比较狭义的侧链，是专门指比特币和其他数字资产在多个区块链间的转移，使用户能用他们已有的资产来使用新的和创新的加密货币系统，就像美金锚定到金条一样。侧链是以融合的方式实现加密货币金融生态的目标，而不是像其它加密货币一样排斥现有的系统。利用侧链，我们可以轻松的建立各种智能合约、股票、期货、金融衍生品等等。你可以有成千上万个锚定到比特币上的侧链，特性和目的各不相同，所有这些侧链依赖于比特币主区块链保障的弹性和稀缺性。在这基础上，侧链技术进一步扩展了区块链技术的应用范围和创新空间，使传统区块链可以支持多种资产类型，以及小微支付、智能合约、安全处理机制、真实世界财产注册等，并可以增强区块链的隐私保护。

比较著名的比特币侧链是ConsenSys的BTC-Relay、Rootstock和BlockStream推出的元素链，非比特币的侧链如Lisk和国内的Asch。因为篇幅有限，所以Elwin主要介绍BTC Relay、RootStock、元素链和Lisk。

BTC Relay是一种基于以太坊区块链的智能合约，把以太坊网络与比特币网络以一种安全去中心化的方式连接起来。BTC Relay通过使用以太坊的智能合约功能可以允许用户在以太坊区块链上验证比特币交易。BTC Relay使用区块头创建一种小型版本的比特币区块链，以太坊DApp开发者可以从智能合约向BTC Relay进行API调用来验证比特币网络活动。BTC Relay进行了跨区块链通信的有意义的尝试，打开了不同区块链交流的通道。（图1）

RootStock是一个建立在比特币区块链上的智能合约分布式平台。它的目标是，将复杂的智能合约实施为一个侧链，为核心比特币网络增加价值和功能。RootStock是以太坊虚拟机的一个改进版本，它将作为比特币的一个侧链，使用了一种可转换为比特币的代币作为智能合约的“燃料”。（图2）

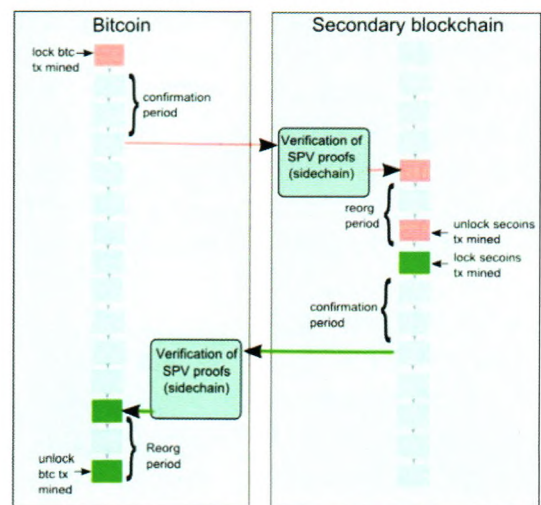


图2 Rootstock示意图

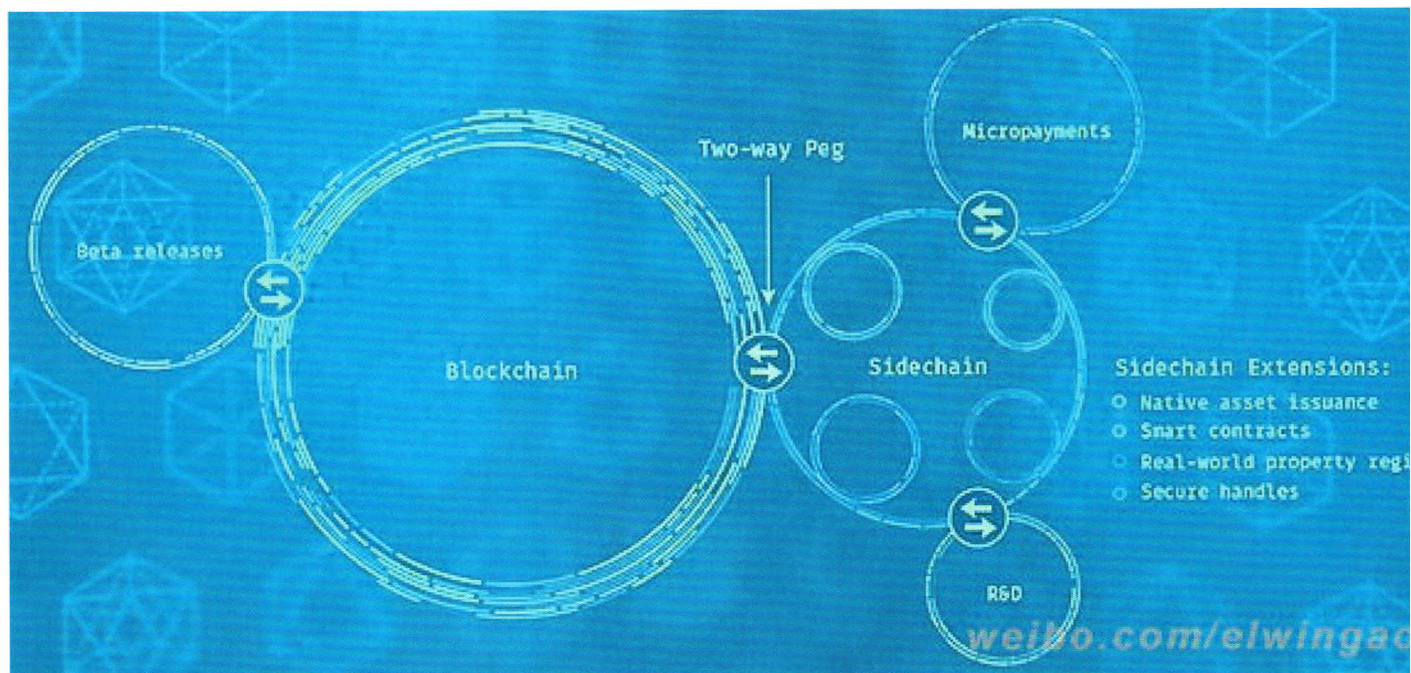


图3 元素链示意图

元素链是Blockstream的开源侧链项目，使用了比特币双向挂钩技术，侧链协议的目的是实现双向锚定（Two-way Peg），使得比特币可以在主链和侧链中互转。除了智能合约外，它还给比特币带来许多创新技术，包括私密交易、证据分离、相对锁定时间、新操作码、签名覆盖金额等特性。这些技术可以被任意组合应用到任意侧链中。（图3）

Lisk是新一代的区块链平台，它把每个应用加到Lisk的单独侧链上。用过比特币和以太坊的朋友都知道，由于比特币和以太坊只有一条主链，所有功能和数据都加入这条主链导致区块快速膨胀，超大的区块体积，超长的同步时间，这是个痛苦的经历。Lisk的侧链模式给在处理高交易量下如何解决网络拥堵的问题提供了一种方法，用户只有用到相关的应用时才需要下载对应的侧链，大大减小了无效的同步数据，保持了整个Lisk网络的高效运行，而且，Lisk网络的速度随着时间的推移会继续加快，显示出它的特别优势。

2.M2

M2是由公证通网络采用的同时锚定比特币和以太坊两种区块链的新技术。公证通（Factom）利用区块链技术来革新商业社会和政府部门的数据管理和数据记录方式，核心是在区块链上建立不可更

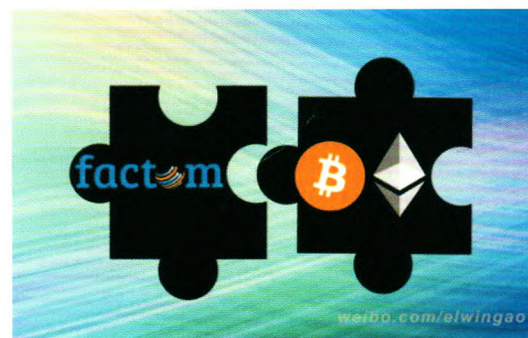


图4 M2示意图

改的审计公证业务流程。Factom原来是通过比特币网络进行数据存证，后来通过M2功能，同时整合比特币和以太坊区块链，以使得确保数据时时刻刻都是安全和可信的。（图4）

M2功能大概情况是，Factom将网络中所有数据整合成条目或者链。用户数据存储条目中，而链与条目之间形成互动协作。每个链拥有条目区块，这些区块又以每十分钟的速度生成新的。十分钟的结尾所有链的全部新的条目区块会整合到一个目录区块中，然后嵌入比特币和以太坊区块链。如果10分钟之内某个链没有新的条目，该链就不会增加新的条目区块。

Factom这样做的意义，可以使他们的数据存储不会仅仅依赖于比特币账本一个单一的区块链，

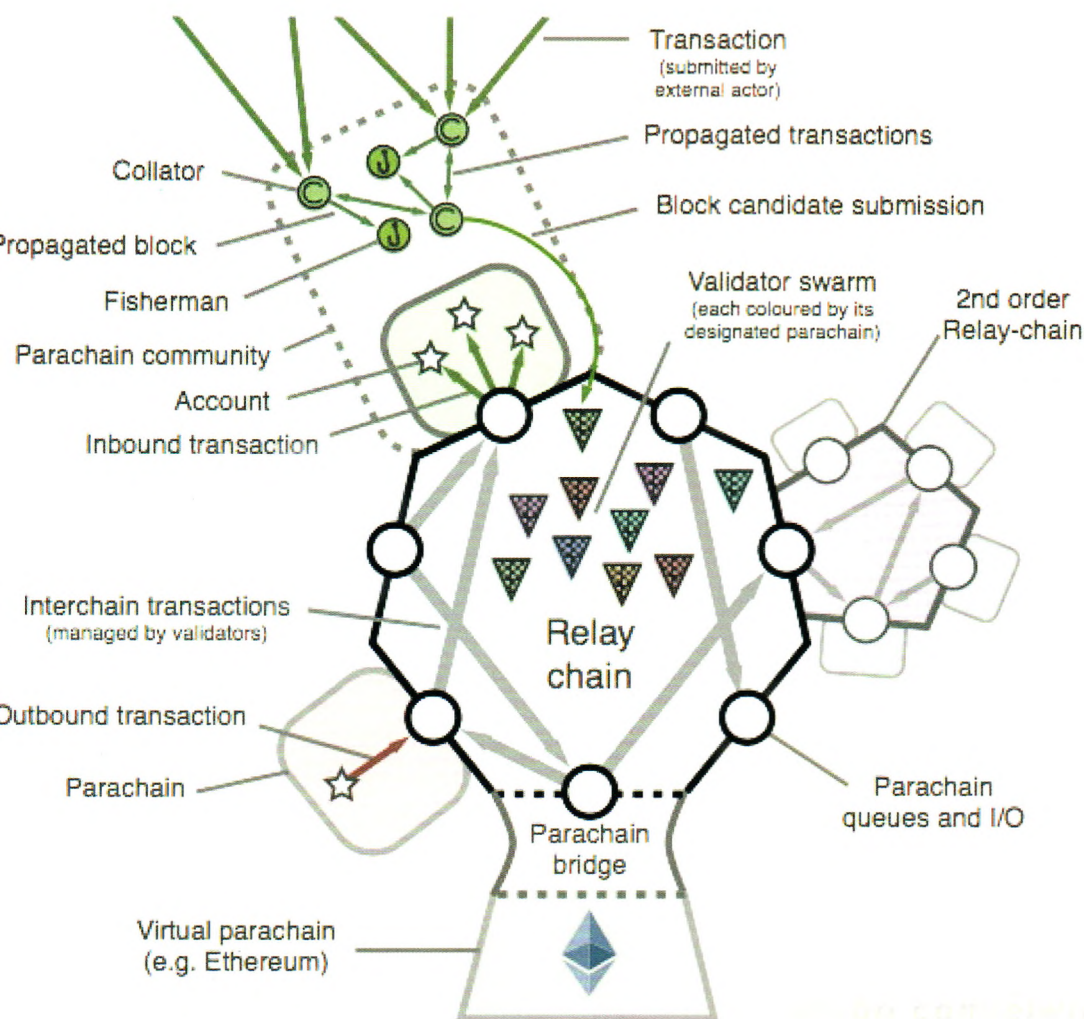


图5 Polkadot示意图

是作为链接多个公链的有意义的探索。

3. Polkadot

Polkadot技术是由以太坊Ethereum（Parity科技）推出的第三代公开无需授权的区块链科技，它的设计核心理念为即时拓展性和延伸性，解决了当今两大阻止区块链技术传播和接受的难题。

Polkadot计划将私有链/联盟链融入到公有链的共识网络中去，同时又能保有私有链/联盟链的隐私和许可的防护措施。它给予了我们一个全新的交易层，并有机会将数百个区块链互相连接。

Polkadot的核心思想是区分交易方发起和执行交易的方式以及交易方统一记录的方式。Polkadot提供基础的中继链（relay-chain），很多可验证的、全球动态同步的数据架构都建立在这个基础上，这些数据架构为平行链或者侧链。区块链应用可以将以太坊分叉，按照各自需求调整，通过

Polkadot与以太坊公有链连接，或者给不同的链设置不同的功能，实现更好的扩展性和效率。（图5）

Polkadot目前以以太坊为核心，实现其与私链的互连，并以其他公有链网络为升级目标，最终让以太坊直接与任何链进行通讯。

4. Interledger

在不同账本之间进行价值转移和交换，总会碰到各种问题。比如Elwin希望通过比特币作为媒介向海外同事Jam进行汇款，Elwin目前只有人民币，而Jam只接受美金。Elwin首先需把人民币换成比特币再把比特币换成美金给到Jam，但这里有个问题就是币价会不稳定，导致价值损耗。而Ripple、Stellar、Circle等区块链技术体系正是解决这些难题的利器，这几个的核心思想方向基本一致：账本提供的第三方会向发送者保证只有当账本收到证明，且收件人已经收到支付凭证时，他们

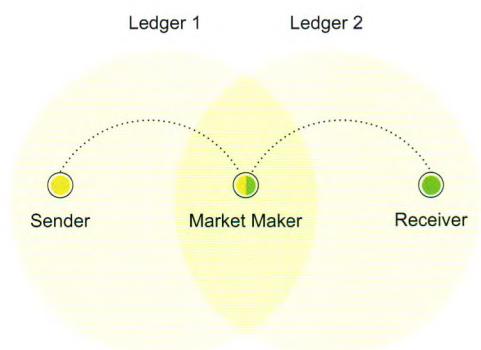


图6 Interledger示意图

才会将资金转移给连接者。第三方也会保证一旦他们完成了协议的最后部分，连接者就会收到发件人的资金。（图6）

Interledger Protocol, 简称ILP, 是由Ripple公司主导发起了互联账目协议, 它将实现不同账本之间的连接从而创造账本之间的协作。Interledger协议适用于所有记账系统、能够包容所有记账系统的差异性, ILP推出的目标就是打造全球统一支付标准, 创建统一的网络金融传输的协议。

金融机构基本上都是在自己的网络之中运行着各自的记账系统, 即使运用了区块链技术后, 也是在运行自己的私链或内部圈子的联盟链, 这个除了是应对监管合规性的原因外, 更重要是保护他们的内部数据避免泄密。ILP是为了解决Ripple原来推广业务时遇到的困难而产生的。银行宁愿用Ripple的源代码来搭建他们自己的私链, 也不愿意连接到Ripple上。既然建立一个每个人都支持的全球金融传输协议很困难, Ripple就开发一个协议, 能将所有我们目前正在使用记账系统连接在一起。

Interledger协议创建了一个这样的系统, 在这个系统中, 两个不同的记账系统可以通过第三方“连接器”或“验证器”机器来互相自由地传输货币。记账系统无需去信任“连接器”, 因为该协议采用密码算法为这两个记账系统和连接器创建资金托管, 当所有参与方对资金量达成共识时, 便可相互交易。ILP移除了交易参与者所需的信任, 连接器不会丢失或窃取资金, 这意味着, 这种交易无需得到法律合同的保护和过多的审核, 大大降低了门槛。同时, 只有参与其中的记账系统才可以跟踪交易, 交易的详情可隐藏起来, “验证器”是通过加密算法来运行, 因此不会直接看到交易的详情。理论上, interledger可以兼容任何在线记账系统,

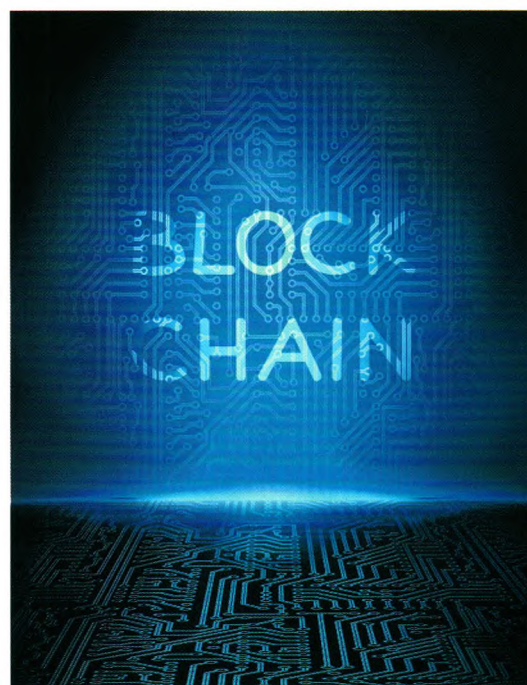
而银行现有的记账系统只需小小的改变就能使用该协议。

Ripple让世界各地的银行可以无需中央对手方或代理银行就可直接交易, 从而使得让世界上的不同货币(包括法定货币和虚拟货币)自由、近乎免费、零延时地进行汇兑; Circle则让用户可以在无需手续费的情况下, 以发送消息的形式发起即时的国内或跨境转账、收付款。目前Ripple和Circle正受到资本市场的热捧, Elwin觉得其中的原因, 与其说他们的崛起是由于跨境汇兑和P2P支付革新, 还不如说他们是对价值交换的革新, 它们将各种账本连接起来, 实现在互联网上交换资金能像交换信息一样轻松。

其他跨链项目一览

跨链的身份认证平台: 科技巨头微软与初创企业Blockstack Labs和ConsenSys达成合作, 共同搭建开源身份认证平台, 目的是整合比特币和以太坊区块链。他们用ConsenSys的uPort保证与以太坊区块链的互连, 然后用Blockstack的OneName整合该平台与比特币区块链。这种跨链的解决方案能够扩展到未来所有的区块链, 或者全新的分散化的分布式系统中。

Bletchley: 微软推出了区块链项目Bletchley, 它是一个区块链生态系统所用的体系结构和解决方案。



66

区块链是价值网络空间的核心基础设施，区块链应用不应该只局限于和止步于联盟链的应用，将价值圈在一个小范围中，我们需要跨链技术，对不同区块链进行连接和扩展，构建价值网络的高速公路。

99

案，旨在打造“开放、模块化的区块链框架”，它是“用微软自己的架构方式创建区块链企业生态联盟”。Bletchley包括了区块链中间件和加密书签Cryptlets，其中，Bletchley区块链中间件将提供的核心功能之一是区块链网关服务，它使用类似Interledger的服务为相互关联的分布式分类账提供相互通信的能力；而Cryptlets将支持互操作性，以及Azure及其他的公共/私有云、生态系统中间件及其他的客户技术的沟通。Bletchley支持多种协议，例如HyperLedger和Ethereum，无论使用哪个的底层区块链平台，都可顺利支持区块链中间件和Cryptlets的运行。

以太坊联盟区块链网络：微软即将正式发布基于以太坊技术为核心的以太坊联盟区块链网络，企业用户将可以快速部署私有、半私有，或共同体区块链（consortium blockchain）网络，也可以通过 Azure来部署公共的以太坊节点。微软希望该项目将会帮助整个行业联合起来共同打造更加复杂的联盟，以更好地利用不可变的共享账簿的网络效应，微软对于该服务的整体目标是帮助全球行业打造区块链联盟。


Multichain：MultiChain向后兼容比特币，因此用户能够把现存的比特币应用导入到MultiChain。它不是支持像比特币内核的单一链，MultiChain可被配置以同时支持同一网络的不同区块链。MultiChain能够支持很多第三方资产，能够使私有区块链和比特币区块链相互转换。

龙链：龙链是一个混合公有/私有区块链的区块链平台，它与其他公共和私人区块链的有很强的互操作性。龙链区块链拥有共五个层次各种类型的

节点，在任意一个层次的节点的验证处理中，可以选择与其他区块链进行连接和联系。比如第一层是商业节点，用于处理交易并且可以决定某笔交易是否被批准或者被拒绝，如果要提供更去中心化的实现，可以选择使用比特币网络或其他基于PoW共识机制的区块链去实现交易的共识处理。

太一区块链：太一区块链支持跨链交易和多链交互。太一跨链交易有两种模式，第一种模式是基于太一超导网络而设计的逻辑链之间的双向交易，这种模式是无第三方参与的一对一的跨链交易；第二种模式是基于太一区块链特有的逻辑链之间而发起的多重签名的智能合约来实现的无第三方参与的一对一的跨链交易。太一多链交互一方面包括行业内的价值转移链、信息记录链的交互，另一方面包括身份链、征信链、数据存证链、监管链等基础服务功能的区块链的交互，各种链互为关联，共同向用户提供可信安全、快捷高效的服务。

结语

区块链从技术上来看是去中心化数据库和分布式账本技术，从商业层面来看则是价值网络，在这个价值网络中，连接的有效节点越多和分布越广，可能产生的价值叠加会越大。区块链是价值网络空间的核心基础设施，区块链应用不应该只局限于和止步于联盟链的应用，将价值圈在一个小范围中，我们需要跨链技术，对不同区块链进行连接和扩展，构建价值网络的高速公路。

（作者微博：weibo.com/elwingao）

如对本文观点有任何讨论和补充，请发送至：
gkbi@ste.gd.cn。