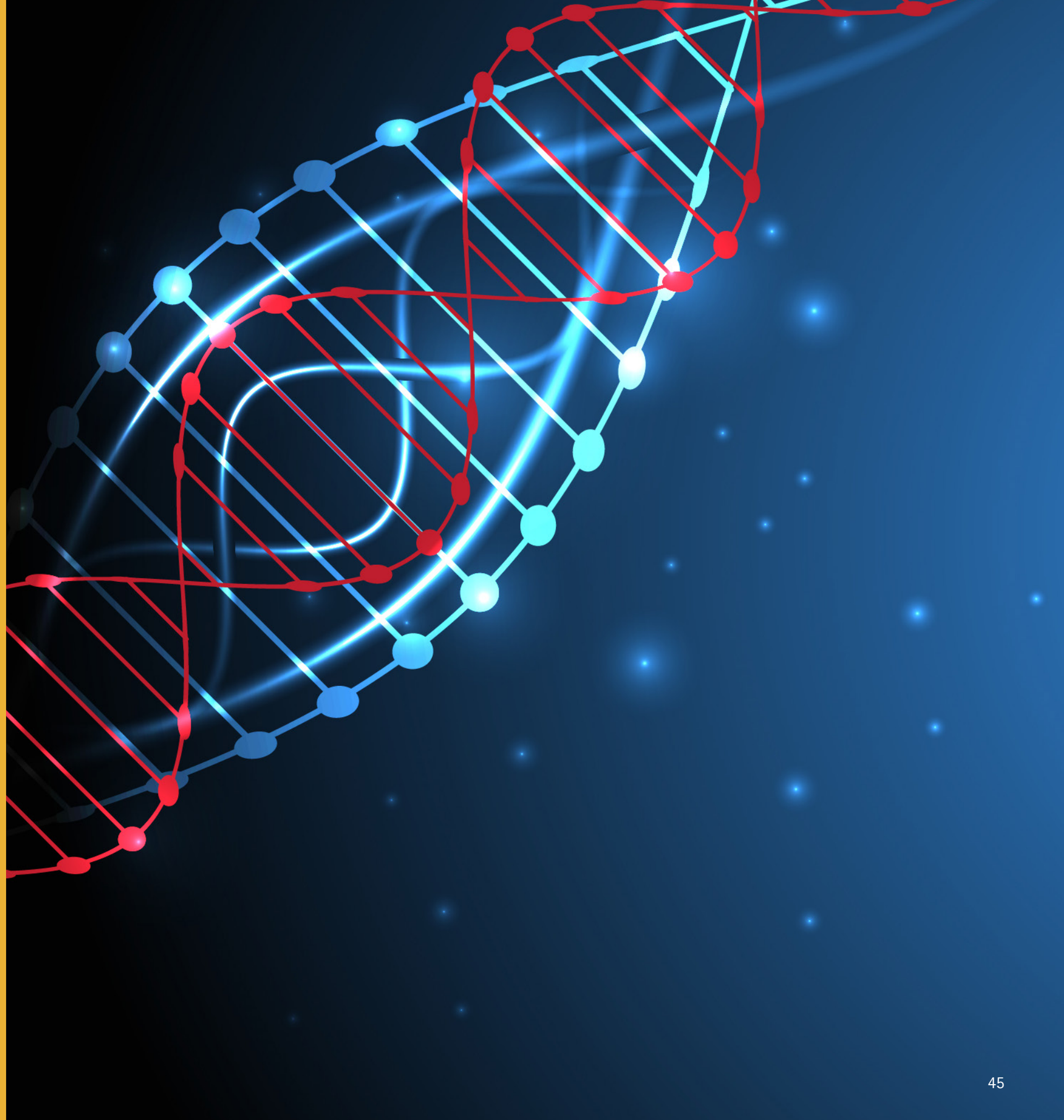
让区块链技术适应不完美的世界

林睿嘉（Richard Lumb）、大卫·垂特（David Treat）
欧文·杰尔夫（Owen Jelf） | 文

“理想主义固然可贵，但面对现实环境，成本就成了拦路石。”

——小威廉·F·巴克利（William F. Buckley, Jr.）



如今，商业互联网每年的经济估值已达1.5万亿美元。很难想象，曾几何时，几乎所有人都在反对互联网商务。早期的互联网先锋中不乏不折不扣的纯粹主义者，他们认为“商业的铜臭味”会侵蚀互联网这个“合作、共享、信息交换与互助的独特堡垒。”这些网络纯粹主义者直言不讳，不希望刚刚诞生的互联网被商业势力所左右。但他们未曾料想，到了2016年，每天有超过20亿人在积极主动地使用电子商务。

眼下，区块链就像当年的互联网，正处于获得广泛接纳和应用的临界点上。区块链技术能够像互联网一样改变世界，但前提是，需要解决技术圈内正在探讨的关键性问题，倾听实用主义者和现实型创新者的声音。

因此分布式账本技术在应用于企业和授权管理型网络时必须变革——这个世界并不完美，人为失误、法律缺陷和恶作剧都需要该技术更加灵活；同时，不可编辑让该技术的前景喜忧参半，欧洲出台的“被遗忘权”法律、近期高调的加密货币盗窃活动以及由来已久的“乌龙指”，均给金融服务业带来了日益严重的危害。

如果业界准备引入新技术，就应当允许修正人为失误。因此埃森哲与知名学者共同推出了“可编辑区块链”的概念。

区块链技术的不可更改性

目前而言，“不可更改”是区块链的核心问题之一。区块链是一种只允许追加信息的系统，数据只能添加，不能删减。这意味着，区块链上的所有信息都是永恒、不可改变的。例如，自比特币2009年推出以来，其区块链上已发生了约1.6亿笔交易，而只要该货币存在，所有交易记录都将永远完整地保留在账本中。

在围绕这个核心问题的辩论中，一方坚持，正是不可更改令此项创新如此重要。另一方则是实用主义者，他们越来越多地发现，面临人为失误、恶作剧和隐私法规，不可更改可能会限制该技术在企业环境中的广泛应用。

与此同时，区块链未来的应用路径尚待明晰，这也让该技术的开发群体压力日增。世界经济论坛日前指出，这方面的成功需要“老牌企业、创新机构和监管者之间深入合作”。

恶作剧和人为失误

2013年，比特币区块链元数据被发现嵌入了非法色情内容，且无法消除。三年后，它仍然在那里供人观览。同样不可抹去的还有另一项区块链顽皮之作：美联储前主席伯南克的点阵画像。

```
      ASCII BERNANKE
:'::.:::::.:::.::.:
: :.: ' ' ' ' : :':
:.:      _.__      '.:
:    _,^"   "^x,    :
'   x7'        `4,
 XX7            4XX
 XX              XX
 Xl ,xxx,   ,xxx,XX
( ' _,+o, | ,o+,"
 4   "-^' X "^-'" 7
 l,     ( ))     ,X
 :Xx,_ ,xXXXxx,_,XX
  4XXiX'-___-`XXXX'
   4XXi,_    _iXX7'
   , `4XXXXXXXXX^ _,
  Xx,  ""^^^XX7,xX
W,"4WWx,_ _,XxWWX7'
Xwi, "4WW7""4WW7',W
TXXWw, ^7 Xk 47 ,WH
:TXXXWw,_ "), ,wWT:
::TTXXWWW lXl WWT:
----END TRIBUTE----
```

更令国家安全管理者们头疼的是，2010年维基解密曾披露超过25万条外交密电，也以一份2.5兆字节文件的形式，嵌入在130笔单独的比特币交易中，永久记录在了区块链上。

这类无害、但可能已触犯法律的恶作剧，有多种解决方案。但对于监管严格的企业系统以及由指定人员管理的授权环境来说，区块链的不可更改，或将导致重大的实际损失。对于资本市场行业来说，尤为如此。合规和风险管理人员需要跨越各种信息渠道，监控并管理交易对手方的通信，并在必要时进行编辑甚至审查。

如果这些渠道和通信协议，如FIX、SWIFT等，都被计入账本且账本不能更改，那么企业就很难修改受限信息，或防止交易员恶意泄漏敏感信息，并且这些信息会被嵌入永久账本中。

此外，看错对手方、记错账本等无心之过也并不罕见，交易失手误记到错误的交易账户中，或填错符号、标记和到期时间。无论账本计对计错，银行都需确保交易信息的保密性。如果区块链系统中的错误不能修正，交易策略就有可能被他人破解。

智能合约

在近期一份报告中，世界经济论坛展示了智能合约的大量使用案例，同时指出：区块链技术“有潜力实现所宣传的效果并重塑金融服务业”。智能合约实际就是区块链上的一系列指令，当触及事先约定事件时，合约将自动执行指令。研究公司Autonomous Research认为，到2020年，这些合约能够为投资银行节约160亿美元的清算和结算成本。

但是，如果代码中存在故障或缺陷，会引发哪些后果？如果合同设计不清晰，代码难以执行，合同复杂导致执行失败，又将发生什么状况？

如果区块链不可编辑，可通过追加合约来解决未来所有类似交易问题。但漏洞依然存在于账本中，可能被滥用，即便交易各方达成了修改共识也无法避免这一风险。

此类担忧绝非空穴来风：初创基金“分布式自治组织”（DAO）在风头正盛之时，遭遇黑客攻击，致使价值6千多万美元的数字货币“以太币”（ether）被盗。而黑客之所以得手，很大程度上是由于很小的一个漏洞——DAO智能合约代码编程的人为失误。而在此次事件发生前，以太币正作为区块链智能合约应用的范例，颇受追捧。

即使最智能的合约也很容易受人为错误的影响。对于不可更改的区块链而言，对合约“打补丁”意味着在链上增加新合约。这很难规模化——特别是在合约变得更大、更复杂之后。如果我们能够编辑，而不是添加智能合约，就能节约时间和资源。

失败是成功之母？

DAO事件的律师辩驳称，其客户有权获取错误编码下的资产。令人吃惊的是，不少区块链纯粹主义者都同意其观点。一名DAO投资人、同时也是区块链的开发者对《华尔街日报》表示，他反对补救措施，因为技术“必须容许失败方能完善”。

智能合约将复杂的合同约定改写为

计算机程序，从而免受人为干预。与埃森哲合作创建可修改区块链架构的计算机科学家朱塞佩·阿特尼则博士（Giuseppe Ateniese）指出：“这种不可变更性不是好主意，特别是对于受监管的金融企业而言。这需要程序员一次性写出完美无缺的代码，并且次次如此。

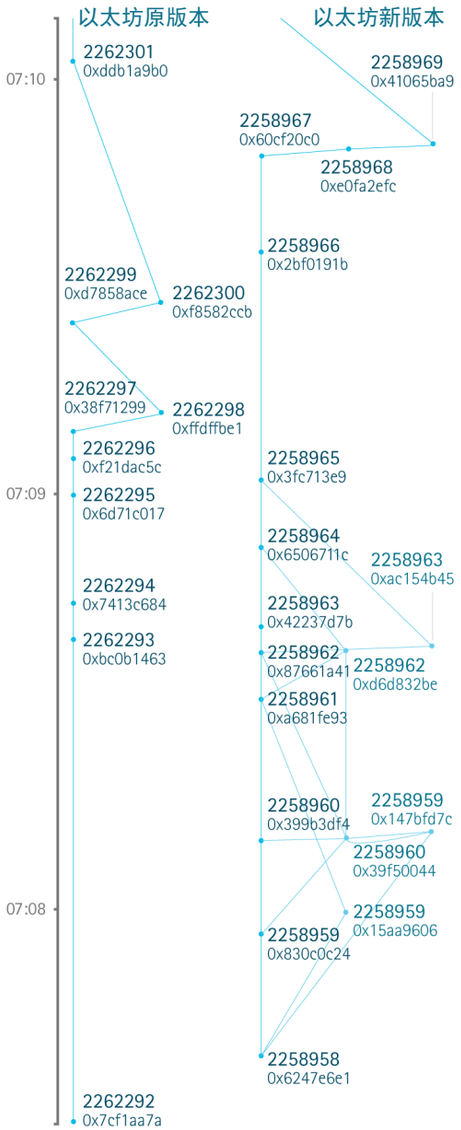
我们大多数人都看过《奇爱博士》（*Dr. Strangelove*）或《战争游戏》（*War Games*）两部影片，虽然它们是以好莱坞式的夸张手法描绘了智能合约一旦出现问题所引发的大规模危机，但却反映着非常现实的问题。人们并不希望电脑具有完全、无法干预的自主权，而是需要由人来作为最后一道防线。”

在 DAO 这场资产侵占中，其参与者们损失了三分之一的开发资金，好在他们在盗窃者得手前果断地在区块链上添加了“硬分叉”。其中一个分叉包含原始链，另一个则开了一个新链，避免了 6 千万美元损失，重建了迄今为止所有后续交易。虽然新链去掉了失窃的片段，但却没留下任何修改痕迹 / 版本。DAO 的用户和开发者可以选择新链，挽回损失，也可以拒绝接受，以维护其原本的“不可更改性”。不幸的是，硬分叉使 DAO 分裂成两大阵营。大批 DAO 参与者出于意识形态或财务得利考虑，继续使用原始区块链交易（见下图）。

同时必须指出的是，硬分叉仅对新挖出的区块有效。在 DAO 中创建硬分叉所需的“共识”，实际上也比较难达成。但由于失窃事件才刚过去一个月，重建后续区块相对简单。如果很久后才发现，届时 DAO 的区块链已经增长、智能合约不断交织，或者交易量已攀上了更高水平，那么加硬分叉就几乎不可能了。

以太坊原版本与新版本对比

以太币单价/美元	1. 30	12. 08
以太币单价/比特币	0. 00213119	0. 01981240
市值（美元）	109, 050, 675	1, 014, 265, 308
市值（比特币）	178, 907	1, 773, 992
散列率（10亿散列/秒）	652	4610
折价率（以太坊原版本/新版本）	14. 25%	
散列率（以太坊原版本/新版本）	14. 15%	



资料来源：http://www.etc-eth.com （截至 2016 年 9 月 15 日）以及 http://fork.ethstats.net

正如克林特·芬利（Klint Finley）在《连线》杂志上所言，DAO 黑客事件已成为区块链技术发展的分水岭。他写道，“机器总是难免受到人类世界混乱政治的影响。此次事件让人们产生了分歧，也暴露了人性难以避免的弱点。但同时，它也让人们走到一起，共同解决问题。这是人性，而不是数学的力量。”

诚然，DAO 黑客案降低了数字货币体系的可信度，也在敦促各方重新审视区块链的优缺点。但有一点非常明确：如果金融服务行业准备引入一项新技术，那么就必须允许修改人为失误，不能让犯罪者在意识形态的庇护下肆意妄为。

“被遗忘权”

2012 年，欧盟委员会根据新的数据法规，提出了“被遗忘权”保护。两年后，欧盟最高法院将之确定为一项基本权利。自那时起，单是谷歌就批准了超过 30 万项在线内容修改申请。

2016 年，《数据保护通用条例》（GDPR）被写入法律。按照该规定，企业须在 2018 年前达到合规要求，否则就会出局。公司在客户数据的使用和控制方面面临着比以往更为严格的要求和监督。严重违规将导致巨额罚款：公司年收入的 4% 或 2 千万欧元，取两者中较大金额。

或许更为重要的是，这些法规的影响将远远超出欧洲范围。任何在欧洲开展业务或拥有客户的企业，即所有在欧洲内外持有或使用欧洲个人数据的实体，都会受到新法的影响。

《数据保护通用条例》的基石之一是消费者有权从与其有交易来往的公司记录中抹去所有个人数据痕迹。隐私保护组织“国际隐私专业人员协会（IAPP）”CEO 特雷夫·休斯（Trevor Hughes）认为该条例具有“根本性的突破”。“个人现在能够用一只虚拟的黑色马克笔，真正涂掉自己的名字。”

该条例还要求“数据可迁移权”——如果客户提出请求，企业必须拷贝并向客户递交其个人数据。此类个案累加后，请求共享和撤销个人数据方面的职责，将给银行的后台部门造成巨大影响。

在很多方面，区块链技术和智能合约非常适合让这类新的工作实现自动化。它们能让个人数据更细致，并将授权、条件和使用限制进行编码；方便数据迁移，并能提供知情同意书，让审计更好操作。

但欧洲的隐私法规也让该技术遇到了麻烦。将个人信息的权利交给消费者的要求，让区块链在不可编辑的情况下，几乎不可能满足法律合规要求。

距离《数据保护通用条例》生效还有两年左右时间，但即便是现在，也有隐私法规可能与区块链的不可更改性产生冲突。如《格雷姆 - 里奇 - 比利雷法案》和美国证监会的《S-P 法规》都要求机构必须每年通知消费者他们的信息共享业务，并告知客户有权退出。如果某位客户今年选择加入，下一年选择退出，那么如何从区块链上删除这些数据？一年之内对数百万客户记录的处理如何管理？

再以《公平信用报告法》（FCRA）为例。根据该法案，消费者报告机构必须纠正或删除不准确、不完整或不可核实的信息——通常为 30 天以内。美国联邦贸易

委员会估计，在当前制度下，信用报告有误的美国人达 4 千万之多。但同时，一个问题浮出了水面：一边是“被遗忘权”的新规，一边是永远不会遗忘的区块链技术，金融机构如何合规？

业已取得的进展

世界是不完美的，不可更改的区块链技术面临着诸多问题。埃森哲相信，如果下一代的授权区块链应用要想从实验室走向现实部署，就必须重新思考其绝对不可更改的特性。

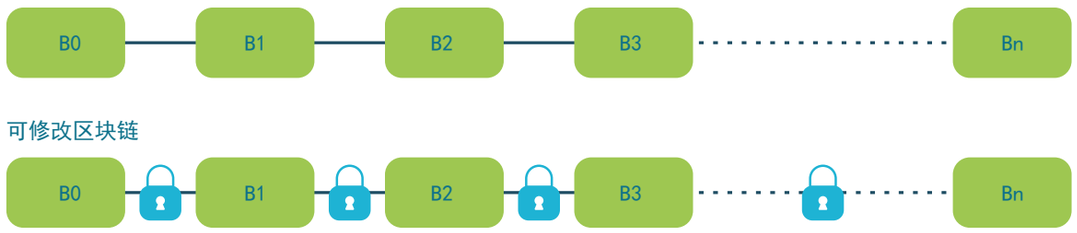
在这方面，不同形式的设想正不断涌现。近期，我们与朱塞佩·阿特尼则博士联合申请了可编辑区块链技术专利。该技术提供了一种新的应对策略，不仅可用于金融服务业，在各行各业都能发挥优势。这一发明改变了现有的区块链技术，指定授权方可以在不打断整个区块链的前提下编辑、重写或删除前面区块的信息。其主要特点之一，就是能与目前的区块链设计完全兼容，并且只需对现有应用软件做很小的修改，便可立即部署。

该技术是“变色龙”散列函数的一个新变种，可利用安全隐私密钥重新制作匹配算法。对区块做出变更之后，原始的区块链仍然保持完好，也不需要创建硬分叉并重建随后的区块。这意味着，有缺陷的智能合约可以在发布后进行更新，并且改动将适用于链中的后续智能合约。即使编辑一个区块会影响其后续区块，修正也要比添加硬分叉容易得多。

可编辑区块链的创新是在连接两个区块的链条上安装虚拟挂锁（如图）。修改区块链很简单：用变色龙散列密钥解开需要修改的区块与下一个区块之间的锁。该密钥可以在不打断整个区块链的情况下直接替代区块。

必要时，该发明也能保留区块链不可更改的特性。为了明确识别经过修改的区块，可以重新设计区块链，以便使任何修订都留下连授权方也无法删除的必然“痕迹”。我们通过两项要素来实现这一目标：沿着一条标准化、不可编辑的散列，用一个可编辑的变色龙散列来连接各区块。因此，尽管可编辑区块功能不会迫使一个节点从其档案中清除数据，但现在，用户拥有了遵从隐私法规所需的技术能力。

区块链



可修改区块链

通过修改使用最广的区块链技术——比特币的核心技术，我们得以成功地创造出该发明的原型。这种修改方法可适用于一系列的现行区块链技术，只需要对当前的区块链、区块或交易结构，以及本地参与软件的信息解读方法，做极小且低成本的改变。

可编辑区块链发明针对授权区块链系统而设计，这些系统会指定管理员来管理系统并对编辑区块链进行授权。与之相比，免授权区块链系统并没有统一的治理机构。已知各方必须事先约定好区块链编辑相关的治理模型和规则，才能使可编辑区块链有效。对于在什么情况下可以编辑区块链，相关规则必须基于清晰的原则和角色划分。让编辑“版本化”，对于保持链的完整性至关重要。

据世界经济论坛统计，过去三年间区块链企业已吸引了超过 14 亿美元投资。金融机构和技术企业有望在 2016 年为此投入 10 亿美元以上资金——而许多创意也将在这一年成为实际产品。此类应用包括存储文档，公正文件，管理健康记录，协调物联网设备以及管理资产。但如果这些记录有误，或涉敏感信息，或有违法律，

区块链在中国的光明前景

罗水权

区块链技术，中国基本上是和全球站在同一起跑线上，一开始就被大量的中国企业、机构和开发人员密切关注、研究和探索可能的行业应用。特别是各类金融行业机构，自上而下，都在密切关注区块链技术本身及其带来的冲击。许多公司都成立了区块链工作小组，研究和追踪行业应用，参与和建立各种区块链联盟（如：R3、Hyperledger 等）。从 2014 年以来，埃森哲也和我们的客户，就区块链技术及行业应用，进行了深入和广泛的交流研讨。

目前，大多数机构都停留在技术研究和原型论证阶段。虽然有些企业也开发出一些基于区块链的应用，但这些应用也是可以通过传统技术实现，并没有充分利用区块链的独特性实现业务场景的颠覆。一些区块链联盟及区块链技术公司（特别是一些创业公司）也在积极探索应用场景，整个市场呈现出活跃的态势。埃森哲认为，目前中国市场亟需一些典型成功案例来证明区块链技术在商业领域应用的可行性，以及能带来明显的经济效益。

可编辑区块链技术，作为埃森哲的独特创新，在全球及中国都引起了极大关注。可编辑区块链能够完成错误交易的纠正和非法交易的撤销，同时保证了整体账本的可靠性，满足这点将契合中国金融市场强监管的要求。另外中国目前没有类似“被遗忘权”的条例或规定，区块链在金融机构中的应用不会受到这方面的影响。然而，随着我国法律的进步，“被遗忘权”的出现几乎是必然，所以目前的应用方案仍有必要提前考虑用户个人隐私保护。

金融企业对于大规模应用区块链技术，还是保持谨慎态度。一方面需要识别只能利用区块链技术实现并能带来巨大收益的业务场景，而不是为了应用区块链技术而启动相关项目。另外一方面，区块链技术的不断完善，用于企业级的核心业务环节，也需要解决以下问题：

1. 建立高效、公平的共识机制（性能）；
2. 记载于区块链中业务数据的选择与安全保护（安全）；
3. 和上下游系统的集成以及配置业务流程的调整（集成）。

除此之外，由于金融市场本身的复杂性和敏感性，它需要一套完整、高效、安全的解决方案，制定这样的方案，需要确立标准，建立治理规则，多方合作，这些相比解决区块链本身的技术问题有着更为重要的意义。

当利用区块链技术能够实现的业务价值越来越大时，区块链技术才真正成熟。我们深信，区块链在中国的应用前景十分光明。

作者简介

罗水权

埃森哲大中华区金融服务业董事总经理，资本市场业主管，常驻上海
kelvin.luo@accenture.com

就需要抹去。

总而言之，我们正处在一场深远变革的前夕，授权区块链系统彻底革新了信息的处理、储存和分发方式。然而，在革命真正开始前，我们仍须观察这项技术可以得到多大力度的支持，进而快速发展并实现大规模的企业应用。

如果纯粹主义者和实用主义者能够认识到——区块链的确具有改变世界、令其更加美好的潜能，那么答案已不言自明，并且该技术的应用正逢其时。

作者简介

林睿嘉

埃森哲金融服务事业部全球总裁
常驻伦敦
richard.lumb@accenture.com

大卫・垂特

埃森哲资本市场服务董事总经理、区块链业务主管，常驻纽约
david.b.treat@accenture.com

欧文・杰尔夫

埃森哲资本市场服务全球董事总经理、业务主管，常驻伦敦
owen.jelf@accenture.com