

摘 要

数据链（Data Chain）是一个区块链技术综合应用平台,拥有树状分层的、立体的多链架构，同时添加区域链技术2.0为核心的智能合约平台、分布式应用底层协议等创新技术。DTC将侧重于对各行业的数据储存，分析与决策，同时与其他应用链进行合作，实现DTC在各类数据中的交易与流通，在今后的时代能够成为行业数据应用的“流通者”。

随着以比特币、莱特币等电子货币为核心的区域链1.0时代的开启和以瑞波(Ripple)、以太坊(Ethereum)等二代区块链技术，两代技术将区块链推向了应用研发阶段。从而越来越多的区域链应用开始在市上流通，导致在区域链的数据增长迅速。DTC可通过侧链链接一个应用，并提供多项数据分析，进行数据的分级处理。DTC因其侧链功能或者通过智能合约的手段，可并行处理多项应用。而区块链特有的不可修改的记录可显示企业级应用在运行过程中所有的数据轨迹，大大提高了产品在溯源定位上的优势。

跟几乎所有其他去中心化交易平台不同，该分布式网络在无需可信任的网关代币的前 提下，允许不同区块链间直接进行去中心化交易。此外，市场利差将显著下降， 并通过去中心化监管以及市场活动透明度的提高来鼓励市场保障。上述过程通过 使用智能合约以及协议代币保证委托交易账本配对的正确性。这是使用以太坊担 保清算活动以及通过使用以太坊智能合约来保证历史交易数据的新结构。

DTC的目标不仅是在对区域链应用的数据处理，在我们的发展宏图中，DTC将成为区域链中的流通媒介，即成为区域链中的“比特币”。为此，DTC研发与社区希望与各位志同道合的朋友一起携手，为DTC发展不断奋进。

目 录

[第一章 区域链发展 1](#_Toc466640616)

[第二章 DTC 2](#_Toc466640621)

[2.1 设计背景 2](#_Toc466640622)

[2.2 DTC技术 4](#_Toc466640626)

[2.1.1 混合挖矿 4](#_Toc466640622)

[2.1.2 代币模型 5](#_Toc466640622)

[2.1.3 侧链 5](#_Toc466640622)

[第三章 应用场景 6](#_Toc466640628)

[3.1 数据流通 6](#_Toc466640622)

[3.2 智能合约 6](#_Toc466640626)

[3.3 决策树应用 6](#_Toc466640626)

[第四章 ICO 7](#_Toc466640635)

[第五章 总结 7](#_Toc466640635)

第一章 区域链发展



区块链的概念继承于比特币，也就是我们现今常说的区域链技术1.0。比特币的概念最初由中本聪在2009年提出，根据中本聪的思路设计发布的开源软件，比特币是一种P2P形式的数字货币而其核心思想-点对点传输。则意味着比特币是一个去中心化的支付系统，有着主心的特点。

比特币之所以区别与大多数货币，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，其总数量非常有限，具有极强的稀缺性。比特币经济使用整个P2P网络中众多节点构成的[分布式数据库](http://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F%E6%95%B0%E6%8D%AE%E5%BA%93" \t "http://baike.baidu.com/_blank)来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节[安全性](http://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E6%80%A7" \t "http://baike.baidu.com/_blank)。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。

而如今由于社区与技术的推动，我们迎来了区域链技术2.0。其中的代表便是以太坊。以太坊是一款能够在区块链上实现智能合约、开源的底层系统，以太坊从诞生到2017年5月，短短3年半时间，全球已有200多个以太坊应用诞生。以太坊是不仅是一个平台，更是一种编程语言，使开发人员能够建立和发布下一代分布式应用。 以太坊可以用来编程，发布类以太坊应用，如可以投票，域名，知识产权，还能涉及到传统行业，如农业种植记录等。

第二章 DTC

2.1设计背景



以太坊是由创造数字资产而生，但是它的图灵完备虚拟机系统也提供了更多的想象空间，把人们从数字资产的领域，拉到了很多其他领域里面。区块链的概念火起来的原因，也是因为大家把数字资产的底层技术区块链和数字资产本身剥离开，开始讨论上层的应用才开始火起来的。我们知道区块链只是一个底层的操作系统，一个价值传输的链条。在这个基础之上，我们可以建立无数我们想要的商业应用，一切和“买”或者“卖”有关系的应用，都可以在这样的区块链上建立起来，以太坊其实就是这样的一个系统。它延伸了比特币的区块链概念：在全球范围的多个计算机上验证，存储，和复制交易数据。以太坊在这个概念上更进一步，使在全球范围的多个计算机上运行代码成为现实。以太坊里的代币叫做以太币（Ether），简称ETH。与BTC类似，这种加密货币可以用来与其它加密货币或其它法币进行交易。

简而言之，以太坊（Ethereum）是将比特币中的一些技术和概念运用于计算领域的一项创新。比特币被认为是一个系统，该系统维护了一个安全地记录了所有比特币账单的共享的账簿。以太坊利用了很多跟比特币类似的机制（比如区块链技术和 P2P 网络），来维护一个共享的计算平台，这个平台可以灵活且安全地运行用户想要的任何程序（当然也包括类似比特币的区块链程序）。区块链技术被认为是互联网发明以来最具颠覆性的技术创新，它依靠密码学和 Hash 函数，博弈论等应用数学基础理论，在无法建立信任关系的互联网上，无 需借助任何第三方中心的介入就可以使参与者达成共识，以极低的成本解决了信 任与价值的可靠传递难题。 自比特币之后，很多区块链项目如雨后春笋般涌现，其中很多项目都有突破性创 新，或者底层协议作创新，或在应用层面做创新，从整个行业来说，这些区块链 项目有具备实验性意义。

区块链的主要作用是解决网络参与者间的多边协议之间的协调问题。通过确 保透明度，保障以及执行，我们可以有效达成多方共识，而这在以前是不可能实 现的。当网络内参与各方发现业务不仅透明化，而且运行机制无法轻易改变，那 么它们会更愿意进行协调。参与者显然更能确保，任意一方很难通过改变业务流 程或利用信息不对称来强行收取暴利益租金。换句话说，任何单个参与者都更乐 意使用业务流程和机制本身不属于任何其他单个参与者所拥有的系统。 支付处理商，网关和金融机构之间存在着基本的协调问题。例如，银行的客 户希望在另一个网络上支付商家。过去，建设一个在支付网络和机构之间兼容的 支付系统是一项浩大的工程。 这个过程通常是通过建立一个管理交易的交换所，即使用与中央交易对手清算中 心或者银行往来帐户的通信网络，例如 FedWire，CHIPS，SWIFT，消费者银行 卡支付网络，NSCC / DTCC，OCC 和 ACH。这些网络服务于不同的角色和功能， 包括本地/国家支付，国际支付，信贷，股票/资产交割和衍生工具。这些中心化 网络允许控制实体随意更改机制，在信息成本，尽职调查和所有各方之间的合同 执行的过程中导致交易成本大幅度上升。

DTC正是在这样的背景下产生的，正如之前的互联网应用，当应用如雨后春笋般不断冒出时，我们认为最后的核心仍然是数据的获取与理解。只有赢的了数据，才能获取到用户，从而实现应用的价值。而DTC正是有这样的愿景，愿成为在区域链应用中的数据流通者，在这个技术浪潮中赢的自己的一席之地。

**2.2 DTC技术**

**混合挖矿**

大家已经非常清楚挖矿是由最开始的CPU挖矿，过度到GPU挖矿，最终演化到当前的ASIC挖矿时代。挖矿的演进是硬件的演进过程，同时也是软件的演进过程，尤其是软硬件对接协议的改进过程。DTC决定使用 POW+POS 混合共识机制，两者有等同权 重，区块链中 POW 与 POS 区块被设计为 1:1。之前存在过由于POW共识设计比重过大，导致后期矿区的POS区块基本没人去挖取。DTC团队觉得应把POS+POW共存，增加DTC矿区的生态稳定性。这两种机制的难度调整将相互制约，并且随着 连续同种类型区块的增加，难度会额外增加。 这种混合方式并没有削弱任何一种单独共识机制的安全性，区块链的安全充分结合了 POW 与 POS 优点，对区块链的攻击情况将变得更加复杂，一方面，由于存在 POW，击者还需要大量的币配合才能实现双重支付攻击。POW 耗费算力，耗费能源，但系统的安全性比较强，POS 不浪费能源，但其安 全性能还没得到公认，而且公平性也存在一些争议。

**代币模型**

一个资产发行实体，在比特币网络发送一个交易，附带一个“资产创始”的元数据，实际相当于创建了一个代币，用来代表某一项资产。这些代币的所有权在比特网络上，不需要资产发行人的授权，就可以自由交易流通。事实上，一个代币就是一项资产的数字化、不记名债券，只不过这种债券被资产发起人嵌入到比特币的区块链网络中。在代币模型中，主要存在两种，UTXO 模型和 Account 模型（账户模型），比特币及由其衍生 的区块链体系都是采用 UTXO 模型。但现今只能合约也越来越多的应用于代币中。 直观上，Account 模型更符合人们日常使用习惯，大多数情况下，人们只在乎账户收入多少， 支出多少，余额多少，而不关心具体消费哪一笔收入。 经过综合考虑，DTC采用 UTXO 模式，可以在一个固定的账户中一直存放DTC代币。

考虑到效率和安全问题，DTC 需要对以太坊公共链上进行全节点验证。我 们可以在以太坊区块链上创建一个合约，该合约锁定了由 DTC 链条件决定的资 金。这些资金现在已经被捆绑和锁定，其活动由 DTC 链执行。当订单执行时， 系统会提供一个证明来解锁以太坊那边的资金。 这种结构假设 Schnorr 或 BLS 签名未来可用于以太坊。交易跟踪DTC 链的 活动，并且在传递到以太坊链上付款之前满足达成一定程度的成熟度约束。资金 仍然可以在 DTC 上结算，并持续更新余额。只有在以太坊上进行支付时，才进 行最终的传输。DTC 链强制执行以太坊链上的支付行为。在非对抗环境中，我 们可以使用类似闪电的结构，用户可以直接提供付款而无需证明。如果付款在一 定的区块成熟度后没有争议，则不需要区块证明/计算。 如果支付行为与 DTC链中的状态不匹配，那么任何人都可以提供证明，发送方 的余额将被削减。通过这种方式，以太坊链的算力和带宽效率得到显著提高。 这个 DTC链上的结构适用于以太坊、类以太坊链以及使用担保智能合约的 满足 ERC-20 的以太坊发行代币的交易。

**侧链**

侧链是一种特殊的区块链。它使用一种叫做“SPV 楔入”的技术实现与其他区块链之间的资产转移，这使得用户能用已有的资产来使用新的加密货币系统。人们不必再担心比特币难于采纳创新和适应新需求，只要创造一个侧链，然后对接到比特币的区块链中即可，通过继承和复用比特币强大的区块链，还避免了新货币的流动性短缺和市场波动等问题。并且由于侧链是一个独立的、隔离的系统，侧链中出现的严重问题只会影响侧链本身，这极大地降低了创新的风险和成本。侧链的灵活性还表现在，所有的区块链参数是可以定制的，简单的比如区块间隔、区块奖励、交易费的去向等，高级用户还可以修改共识算法。 不过最重要的还是业务逻辑，侧链上可以轻易的开发出与你的业务相关的交易类型或者智能合约。 这一点是与侧链的发明者blockstreams不同，blockstreams的侧链，只是一个不同的货币系统而已，开发新型交易和智能合约很不容易。

这个网络是一个开放的网络，准确的交易活动要求去中心化交易中心的获取 最终公共，哪怕是盲承诺/盲投标。虽然现在可以通过 SNARKS 进行新的密码学 处理，但是对于大批量的交易网络来说，目前还是太慢，并且面临资源密集的问 题。我们目前正在对性能和速度进行优化。因为这是一个本地匿名网络（带有可 选的代币发行 AML / KYC 结构）。 其他链的 SPV 验证被认为是不安全的，没有因为它们的区块链没有阻止重 组。对于允许重组的链，要么需要对该链进行全节点验证，要么需要建立 HTLC 清算中心。它假定以太坊会为最终结果创造更高的可靠性和保障（当前的权益 证明研究）。 这些技术都是全新的且尚未经过测试。我们会尽全力建设，使其在对抗环境 中具有最大的安全性。我们正在搭建这些机制的安全模型，这些机制需要使用人 类行为的真实用例来正确理解。当链之间交互时，很难回滚错误。所以我们在进 行去中心化跨链活动时，如无必要，尽可能不要在该链产生交易。初始版本在对 抗性设置中可能不够稳健，我们建议降低风险值，因为随着软件的开发，攻击（ 尤其是拒绝服务攻击）会随着时间的推移而得到解决。设计的性能和其对现实世 界的影响还有待研究观察。

第三章 应用场景

2.1数据流通

DTC可用于企业级数据决策，为全球中小企业提供数据梳理，分析与决策。DTC可通过侧链链接一个应用，并提供多项数据分析，进行数据的分级处理。在数据分析过程中，通过对数据的深度挖掘分析，可以形成用户画像，将会给个人隐私带来威胁。而在流通环节，由于多方主体的介入，使得数据转移的控制力差，数据泄露的风险正在加剧。

2015年国务院印发的《促进大数据发展行动纲要》明确指出，要引导培育大数据交易市场，鼓励产业链各环节的市场主体进行数据交换和交易，促进数据资源流通。而区域链技术在数据发展上有着强大的优势，通过区域链的数据定位可以确定数据权属问题，同时由于加密技术的发展与应用，保证数据流通找那个双方的隐私互存。

2.2智能合约

在区域链上，所有人都可以看到智能合约，因为这些智能合约的代码和状态都在区块链上（假设区块链是主链且公开）。从用户角度来讲，智能合约通常被认为是一个自动担保账户，例如，当特定的条件满足时，程序就会释放和转移资金。简单来说，智能合约类似于网络服务器，但与网络服务器不同的是，智能合约不依赖某个特定的硬件设备，事实上，智能合约的代码由所有参与挖矿的设备来执行。正是由于这样的特性，即足够透明化，区域链应用可用于如证券登记和清算，银行等信用度较高的场景。

2.3决策树应用

DTC以储存的企业数据为基础，通过侧链的多级算法处理，可形成有利于决策者分析决策的决策树。在决策树的基础上，可发展有着以企业为核心的企业级应用,即在依靠于DTC的主链，通过侧链形成的基于企业场景为核心的应用，这些应用可以通过与主链的信息交互，从而获取到主链的相关算法，自上而下，形成一个具有强大拓展性的“神经网络体系”。

第四章 特点

上述机制需要大量的活动（和大量的状态数），而且在这个时候并不适合让 所有的活动都发生在以太坊主链上，但是，这个结构将把交易活动绑定在公共以 太坊链上，其中，合约执行的输入由 DTC 链提供。 我们正在建立一个挂钩到其他区块链来进行跨代币/资产类别的交易。这个 过程主要由以太币来支持。从任何单一链条的角度来看，我们正在建立一个可扩 展的区块链，其合约状态由 DTC 链本身的活动绑定。其他链条的活动可以通过 类似与 BTC 中继的形式以跨链提交证明的形式进行链间连接，这个过程可以 提交到以太坊处。DTC链验证了该活动所有参与者的行为（包括其他链条上的 活动）。换句话说，DTC代币的作用是提供计算和执行。代币本身作为其在该区 块链上的活动的保证金，不正确的活动将导致代币/保证金在 DTC链上销毁。 通过创建一个具有深度执行力的定制链，我们可以构建一个系统，在这个系统中， 其共识规则对于高性能活动是最优的。 该设计优化了快速执行和清算，但是结算速度会较慢。未来的迭代可能包括 OMG 链的分片技术，但是对于初始迭代，我们将假设具备高吞吐的区块传播量。 拥有OMG代币，实际上是依照协商一致的规则，购买验证此区块链的权利。 交易费用，包括（但不限于）用于支付，交换，清算和结算所的资金，将给予无 故障的验证节点执行保证金抵押的合约状态。 这些代币将根据从网络中导出的费用获取价值，也意味着承担向链上用户提 供验证的义务和成本。这些代币必须具有价值以防止低成本攻击，并且对于推动 网络的执行时非常必要的。 在我们的路线图上，我们可能允许将验证授权委托给第三方，而在需要重新 授权之前，每一次可以减少有限的数量（该安全模型的完整机制尚未确定）。 因为这将被设计为一个高性能的系统，因此我们需要一条证明连接区块链。 我们期望这个系统能够处理大量的交易，这样我们只要把最终的结果传输到以太 坊就可以了。清算和结算都在 DTC 区块链上发生。共识规则将通过股权证 明网络执行。作为网络共识规则的一部分，我们要求所有 DTC验 证节点也同时运行以太坊网络来并行验证，从而使以太坊成为区块链间验证的首 要保障。 我们同时假设存在如以太坊/ ERC-20 来进行担保或者退款的机制，BLS 签 名方案（或 Schnorr）将在不久的将来用于以太坊。对于加密数字货币，这些代 币是非监管的，而是锁定在智能合约中（不像其他交换平台，比如 Ripple，需要 可信的网关来代表底层）。它也不依赖于所谓的集中验证集合（例如Ripple）。DTC 区块链负责管理在以太坊上的执行顺序的匹配和管理执行。DTC 上 的活动确保验证节点的活动也可以通过本地以太坊智能合约在以太坊区块链 上执行。对于比特币和类比特币系统，我们允许通过闪电网络上的清算网络来进 行交易。区块链通过提交证明在该网络上执行活动。虽然不如以太坊网络那么强大， 但它允许在无需全节点验证的情况下协调DTC链上的几近即时的清算和结算活 动。为了安全性，我们期望在未来让不允许区块链重组的节点进行部分验证，支 持重组的区块链上的简单的 SPV 验证不允许在此网络中执行。DTC将在北京时间2017.06.26 晚上8时进行ICO，ICO的目标总额为2000BTC。DTC的代币总量恒定为2亿个，永不增发，本次ICO的分配方案如下。



ICO的时间表如下：



第五章 总结

数据链（Data Chain）是一个区块链技术综合应用平台,拥有树状分层的、立体的多链架构，同时添加区域链技术2.0为核心的智能合约平台、分布式应用底层协议等创新技术。DTC的目标不仅是在对区域链应用的数据处理，在我们的发展宏图中，DTC将成为区域链中的流通媒介，即成为区域链中的“比特币”。为此，DTC研发与社区希望与各位志同道合的朋友一起携手，为DTC发展不断奋进。