井通中国

井通技术白皮书

V0.3

版本控制

版本号	时间	执笔	修改主要内容
V0.1	20161125	陈小虎	初稿
V0.2	20161128	陈小虎	增加井通系统介绍
V0.3	20170208	陈小虎	更新智能合约

井通中国
Jingtum China

目　次

井通中国
Jingtum China

井通白皮书

1. 区块链技术

这一节主要介绍区块链技术的几个重要因素，以及当前主流的区块链技术解决方案。

1.1【背景】

计算机系统的技术发展几乎都集中在中心化的解决上，包括互联网，大数据，云计算，移动通信，等等。因为中心化的架构可以很好的模拟大部分的用户需求，更由于中心化的思想一直贯穿着计算机技术的发展过程，所以选择中心化的架构是非常自然的结果。

去中心化的尝试一直存在，从最开始的Napster到后来的BitTorrent，去中心化作为一个非主流的解决方案，并没有登上主流的应用场景。直到2008年的比特币【1】的诞生，及由此带来的颠覆性的力量，才引起了广泛的关注。

比特币第一次成功的提供了去中心化的信任的解决方案。比特币利用密码学原理和挖矿（proof of work）机制很好的解决了不信任网络中电子资产双重使用的问题（double spending）。比特币的成功来源于两个方面。一个方面是美国次贷危机引发的广泛的对中心化的不信任，另一方面是比特币利用密码学技术，提供了一个划时代的区块链技术。这两者相结合，率先在金融领域提供了一个去中心化的实用方案。而且技术上的实现简单可靠，使得比特币得以广泛流行。相比传统金融技术，比特币的应用发展迅猛。从比特诞生到现在，派生了多种数字加密货币（比如Ethereum，Ripple【2】【3】）。每种新货币的出现，都是想更好的解决某一方面的实际问题。但是，各种山寨币的出现，包括比特币本身，仍然有有各种局限。相反，支撑比特币的底层区块链技术，却蕴藏着巨大的力量。主流社会包括政府，银行刚开始对比特币存在着敌视。但是比特币的巨大成功也促使这些银行机构认识并学习比特币尤其是区块链技术。各大银行机构都在这方面投入了很多技术力量，力争使自己不脱离最新的技术发展。同时，利用区块链技术对传统金融行业的改造，也越来越成为热门的话题。最新的进展包括花旗银行的CitiCoin【4】，英国央行的RSCoin【5】，以及中国中央银行行长周小川关于数字货币的构想【6】。

1.2【区块与数据】

区块链技术是电子加密货币的底层技术。同时区块链也是一个交易数据库，其中存储的是在系统中由所有节点共享的信息，称为分布式加密总账本。通过这个总账本，区块链实现了其不需要一个中央权力机构或受信任的第三方来协调互动、验证交易或监管行为的特征。 一个区块链上的完整副本包含了每一个曾经执行的交易，使得历史上的任何信息都可以被任何一个参加的节点所访问。简单来讲，区块链包括三个要素：（共享状态；更新规则；历史相关模型）。这三个要素解决了分布式加密总账本的三个主要问题： 1. 数据保存功能。2. 实用于所有节点的更新规则，解决了数据安全性的问题。3. 使用历史相关使得数据保存实现一致性。这样区块链技术使得数据通过协议在多个独立计算机组成的网络间实现一致性。由于采用了数字加密技术数据的安全性也得以保证。

1.3【共识】

数据的一致性具体通过共识来实现。共识给所有的计算机节点指定了统一的规则。但是各个节点的拜占庭行为，对这个规则的执行比率决定了整个系统是否能够达到数据的一致性。根据CAP定理，一个分布式系统中，Consistency（一致性）、Availability（可用性）、Partition tolerance（分区容错性），三者不可得兼。 因此，如何根据所需解决的应用，选择合适的共识方式，对整个系统是非常重要的一个因素。 通常的共识方式包括PoW，PBFT，PoS等。

Proof Of Work（挖矿）

比特币和类比特币都是用挖矿的办法来保证各个节点选取同一个区块链。具体做法是让每个区块的生成都很昂贵，同时协议保证所有节点同意选取最长链，即使由于各种原因区块链有分叉的情况下，系统仍然能够很快收敛到最长的分支，短的分叉很快就背抛弃掉。长期来看，总的区块链还是唯一的。

Proof Of Stake （股权认证）

针对POW的高耗能等其他确定，Proof of stake作为一个替代的解决方案受到越来越多的关注。Peercoin是最早采用POS的加密货币。 原理就是每个节点通过持有的系统股份的比例进行对系

统中的交易进行验证。因为 每个人都是利益相关方，理性的参与者都会维护系统的正常工正的运行。具体的实现方面各个方案有许多细节上的不同。

PBFT

采用多个节点共识的方法保证每个区块都是大家投票表决过的。数学上是解决拜占庭将军的问题。理论上能保证系统中1/3的容错率。

1.4【智能合约】

区块链技术本身是一个面向交易的数据的分布式存储方案。但是具体在应用中，以交易基础可以衍生出非常广泛的应用。在这些应用的实现方式，可以通过一系列的程序运行来实现。这样的程序，称为智能合约。由于智能合约的实现是与加密货币一起提出的，所以通常算作区块链技术的一部分，但是其作为区块链的应用层更加合适。

智能合约其实应该称为傻瓜合约，因为它的执行是通过代码定义，然后程序一行一行代码执行实现的。所以并不是合约本身有智能，而是指合约的编写可以通过代码的形式预先编写。一旦代码运行，执行无法干预。

为了实现智能合约的功能，加密货币通常需要在共识机制里面添加支持。一般实现的方式可以是脚本语言或者是图灵完备的程序语言。后者通常需要单独的虚拟机执行来隔绝与其他模块的相关性。

1.5【比特币】

比特币是第一个被广泛关注的使用区块链技术的加密货币。比特币可以称为加密货币的黄金。但是比特币的主要作用在于作为一种去中心化信任的电子货币。基于比特币的应用受到本身的功能限制。这方面的不足不要包括：

a) 执行速度慢。每次区块生成时间为10分钟，确认时间就更长
b) 交易的容量受限。由于区块的大小受限，所以每个区块能包含的交易数有限。同时比特币的决策机制很难有效的提高限额。
c) POW的共识方式消耗能源巨大，但是比特币的价值必须以这种持续增长的算力维持，是条不归路。

d) 比特币通过脚本语言来实现一些简单的合约功能。合约不支持图灵完备。

e) 比特币本身的交易已经很拥挤，基于比特币的应用范围受限。

1.6【侧链】

鉴于比特币区块链不能完整的提供图灵完整合约的功能,所以一个比较可行的解决方案是用侧链。侧链是指在比特币区块链之外单独运行一个区块链系统。这个系统可以采用与比特币完全相同或者不同的实现方法。用户可以在比特币系统和侧链系统中灵活切换。侧链的好处是侧链的实现方式灵活多样，可以采用支持图灵完备的实现，从而弥补比特币系统的弱点。

一般来讲，从比特币进入到侧链时，用户把比特币发送到某个系统地址锁定。然后在相应的侧链系统，相对数量的侧链货币会发送到用户的钱包。这个过程相对很简单，实现也比较容易。当用户需要把侧链货币兑现时，通过某种方式的验证（SPV验证），在比特币系统中得到相应的比特币。

但是因为比特币本身的特点，任何涉及到比特币协议的改变都将需要经历冗长的讨论。所以基本上任何功能的增加只能采用软分叉的方式。任何硬分叉的实现都不存在现实的可行性。所以这个极大的限制了侧链实现的方式，也就是怎么样解决从侧链系统回到比特币系统的问题。

想通过对比特币系统的改造以实现合约（图灵完备）是非常困难的。而且由于侧链系统针对比特币系统的不成比例的对比，只要侧链发展到有利可图的某种程度，对黑客来讲，他们必将发起攻击以获得额外收益。而且，复杂的协议中的漏洞也很明显。这种方式基本在现实中很难生存下去。

1.7【以太坊】

以太坊是对比特币有明显意义的更新。它的主要特色是支持图灵完备的智能合约。它采用了POW的共识方式，加快了区块生成的速度，并通过vm来执行合约，使得合约的执行也能修改共识的输出。它的主要不足包括：

a) POW的方式对资源的浪费，以及未来的POS的方式的不确定性

b) 每个节点都需要对所有合约进行验证，整个系统的执行效率不能大于单个计算机的执行效率
c) 跨合约的交互非常困难
d) 由于合约与交易的共识互相捆绑，合约的bug直接影响系统的稳定
e) 可能的硬分叉对整个系统的伤害会继续

1.8【中心化与去中心化】

去中心化是区块链的最本质特性。在实现区块链系统的过程中，由于系统的实际部署等因素，会导致各种因素的去中心化修正，包括部分的中心化，部分的算力集中，部分的结构化网络等情况。

比特币系统是最公开、最开放、去中心化最彻底的系统，但是由于POW的设计原则以及挖矿的自然演化，比特币系统中的运算能力逐渐向矿池集中。单个矿池拥有巨大的算力，成为比特币系统中的一个虚拟的中心，此中心在比特币系统中的重要性也随着算力的增长而扩大。 另外一些区块链系统的设计，在其设计之初就有部分的中心，例如Ripple、超级账本等在系统的设计中就有记账节点这个角色，系统中只有被认可的节点才能作为记账节点，系统实现的是部分去中心化。

完全去中心化的目标是绝对的自由、绝对的隐私。但从现实来看，这只是一个理想、一个目标。纯粹的自由不一定好，全民的选择也不一定是最优。而是应该在适当时候，适当的应用采用相应的方式。

2. 井通技术

本节介绍井通技术的实现细节以及对现有系统的改进和优化。

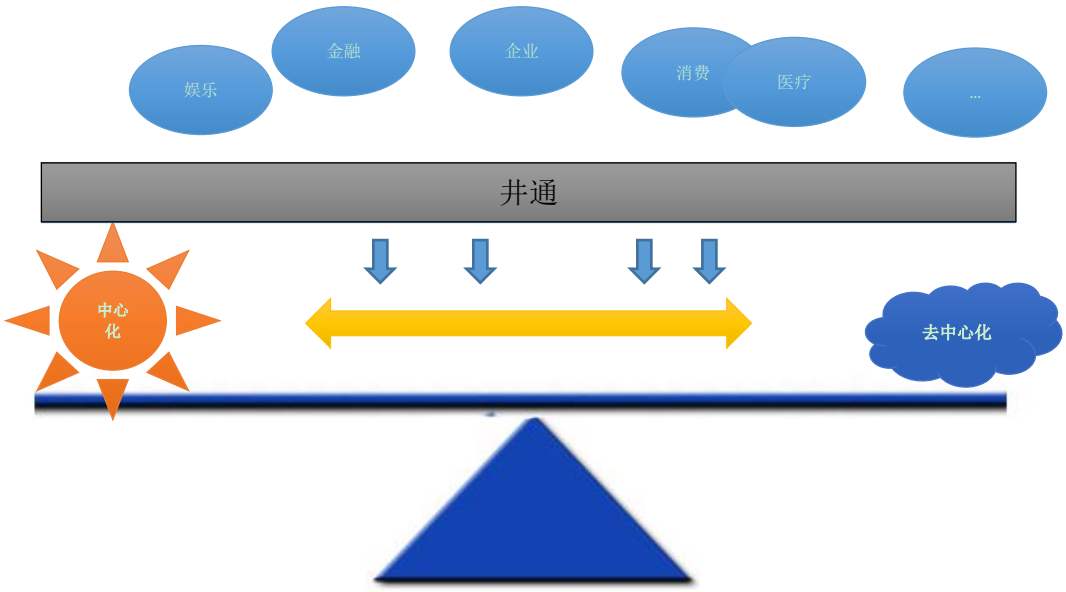
井通系统的设计目标

井通技术的重心是面向应用的通用平台。我们希望提供一个稳定，方便使用的平台，企业用户可以很方便的接入，使用区块链带来的好处，同时不需要了解区块链实现的细节。而且，企业有灵活的选择是否共享他们自己的用户，这样使得每一个新的应用都带来新的客户，同时新的应用也能获得平台的巨大的存量用户。这样构建的生态系统实现我为人人，人人为我的良性循环。

2.1 【有效去中心化】

针对现有的区块链技术的不足，井通技术提出了有效去中心化的解决方案。其核心就是如何在保持去中心化带来可靠性的同时，避免其在效率方面的不足。对此，我们的解决办法是选择一个有效的优化区间，而非一个优化点。一方面，从绝对的中心化到彻底的去中心化，中间有很大的一个区间，我们完全没有必要画地为牢，自我限定只能选择两个极端，而要因势利导、对症下药；另外可以根据不同应用的场景，结合不同行业的实践，来找到最符合使用者需求、成本最经济、使用最便捷的那个平衡点，即选择一个有效去中心化的节点。在这个节点，既能够享受去中心化的安全和成本优势，又不至于过度的去中心化而降低效率。

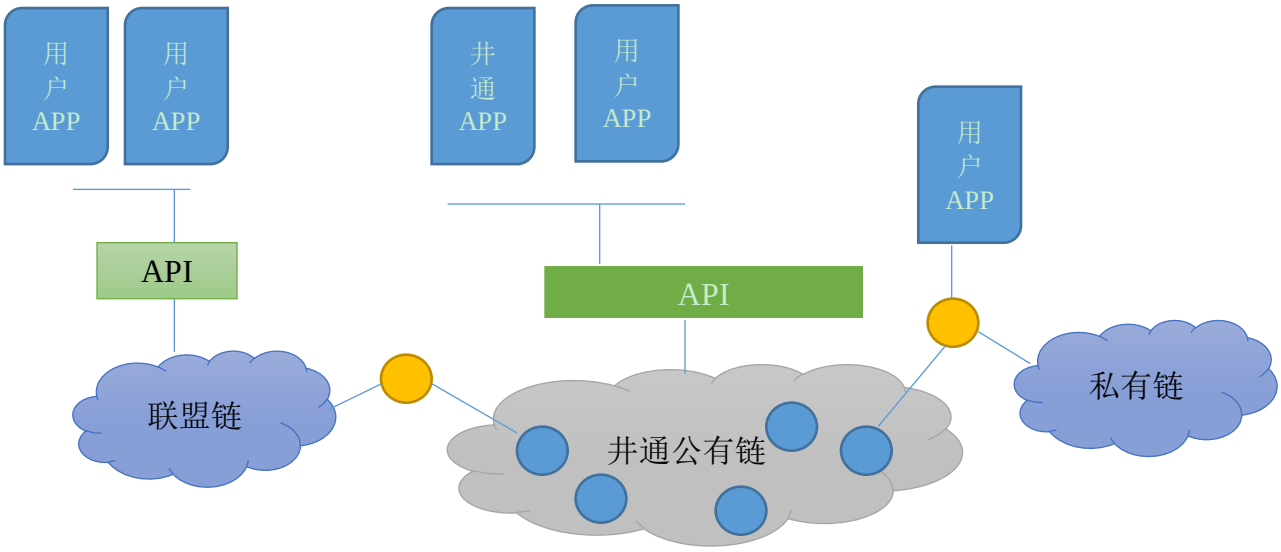
井通的做法，就是使得选择这个最有效的平衡点变得可以自动调节，根据用户的场景和需求自动优化到最佳的那个位置。在用户的接入方式上，用户也可以根据自己的需求选择接入井通的公链或者利用井通技术架设私钥以及联盟链。这些私链和联盟链都可以选择是否与井通公链互联。



井通的共识采用randomized BFT的方式。但是在选择验证节点的方式上，井通采用POA（proof of Application）的方式。井通的核心有若干个验证节点维持系统的基本验证网络。井通的验证网络对每一个接入井通的应用开放。接入井通的应用是指以井通为平台的针对某些用户的应用程序。这些应用可以通过井通提供的API直接接入井通的公有区块链，也可以使用井通的平台技术，部署私有的区块链。这些应用可以维持一个验证节点。这样的节点可以实现两个功能：

a) 参与井通网络的公共节点验证
b) 实现应用接入井通网络。如果应用本身采用一个私链的话，这个节点同时起到了从用户私有货币到井通的转化功能。

当然，如果应用只是仅仅使用API访问所需的区块链功能，则并不需要部署一个单独的验证节点。



在用户私有链和井通相连的情况下，通常还需要银关来实现用户通的发行和兑换。

2.2【井通系统架构】

井通系统的一个设计目标是避免当前区块链技术的缺点。与比特币不同，井通一开始设计的时候就加入了合约功能。与以太坊不同，井通采用更加合理的分层方法，使得合约的执行和交易分开，避免了合约的问题影响到整个系统，同时也使得合约的实现更加灵活。

井通系统的具体结构如下：

a) 井通不使用POW这种浪费资源的方式，而是采用RBFT来进行对TX的共识；另外，我们已经通过各种方法实现高速的并行处理能力和对海量用户的支持

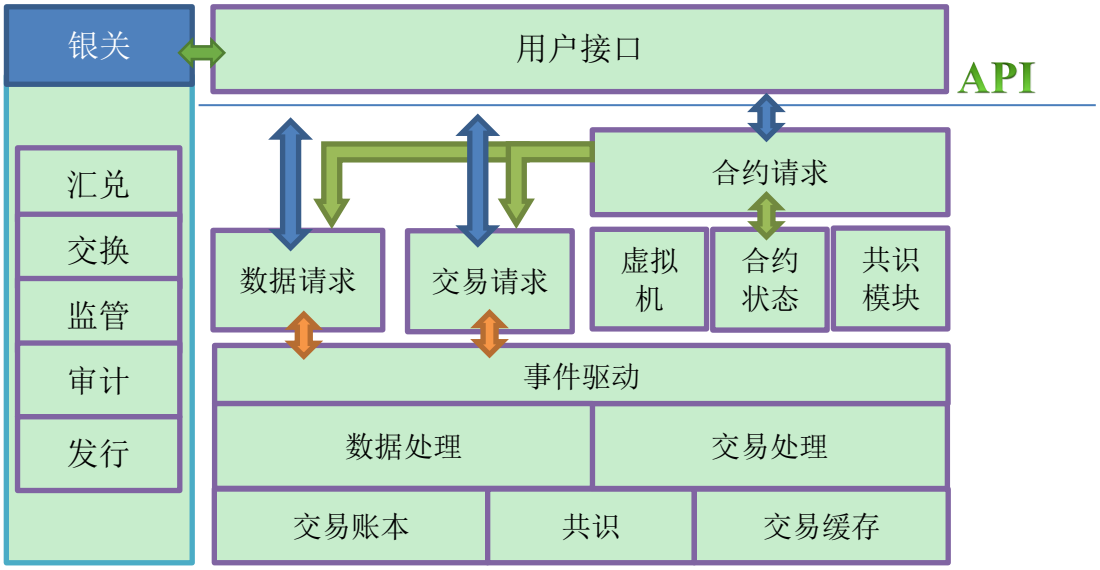
b) 我们将井通进行分层，底层系统称为TX层，负责处理最基本的TX，在此之上增加一个合约层，负责处理合约。我们将合约的要素（code，state, storage，transaction）分开，transaction的执行下传到井通的TX层，其他部分的执行在合约层实现。这样使得合约的执行与产生的交易分开，使得合约和交易从各自的特点来匹配相应的协议，以达到最高的效率和最大的安全。

c) 针对日益广泛的区块链应用对数据支持的要求，我们提供了BLHR（block level hash record）数据支持，使得用户很方便的将数据的签名保存到区块链中。

d) 为了提高整个系统的处理能力，我们在共识节点中引入分片的办法，使得不需要所有的节点都做完全一样的事情。而是对每个交易自动随机选择处理此交易的节点。这样一方面有效利用了众多节点的处理能力，同时维持足够的容错能力；另外一方面也大大降低了网络间信息流量，提高了网络的效率。

e) 创建合约时，用户可以标识需要的合约节点个数和共识达成的条件，一方面用户可以灵活控制付出的花费和可靠性之间的平衡，另一方面使得合约层能够更加高效的处理更多的合约。通过这样的抽样，合约系统的安全性并不会很大的降低。

f) 合约的执行速度和TX层的ledger close的速度去耦合。合约的状态变化可以以合约节点的共识速度完成。



2.3【区块链数据】

区块链的一个重要特性是不可篡改性。由于各个区块通过历史相关性串联在一起形成一个单一链，使得数据一旦记录，就不能被篡改。对数据的直接修改都将导致之后的区块无效化。所以这个特性被广泛的应用在数据的防伪，标识等方面。

对这个特性的应用的通常做法是将一些信息保存在交易的 metadata 部分，这样当交易被执行并计入区块链后，所包含的 metadata 也永久的记录在区块链中。但是这样做有几个缺点：

a) 执行需要交易来实现，一方面需要发送一定的交易数额，另一方面需要对交易进行签名，这样使得对数据的记录必须对应于某个用户账户或者钱包，并且需要访问相应的私钥信息。
b) 保存的宏信息分散在当个交易当中，对该信息的查询必须遍历每个交易。
c) 数据的保存必须通过交易的确认来实现正确写入。

针对于此，井通系统提供了BLHR（block level hash record）支持。用户可以直接递交需要保存的信息到区块中。每个区块有单独的位置来保存所受到的信息请求。如果用户的信息具有历史相关性，用户需要自己提供这个相关性的描述，区块不需要理解用户的应用逻辑，只是忠实地记录用户的发出的存储请求。每次区块关闭的时候，系统自动将所有的BLHR信息记录到区块中。

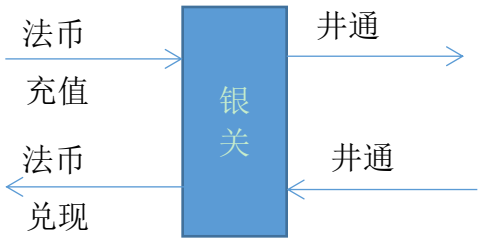
2.4 【银关和用户通】

井通支持除原生的基础货币井通外，还有用户通。用户通可以看成是一种自定义的数字资产的表征符号。用户通的发行由有资格的第三方发起，但是必须通过井通的合规性和风险评估。之后才能获得在井通上面发行用户通的资格。用户通的发行通过银关实现。发行方对用户通的承兑负责。一旦用户通发行完成，其可以象井通一样，在系统里面进行自由支付，流通，交易，不需要发行方的干预。但是用户通的兑换必须由银关实现。

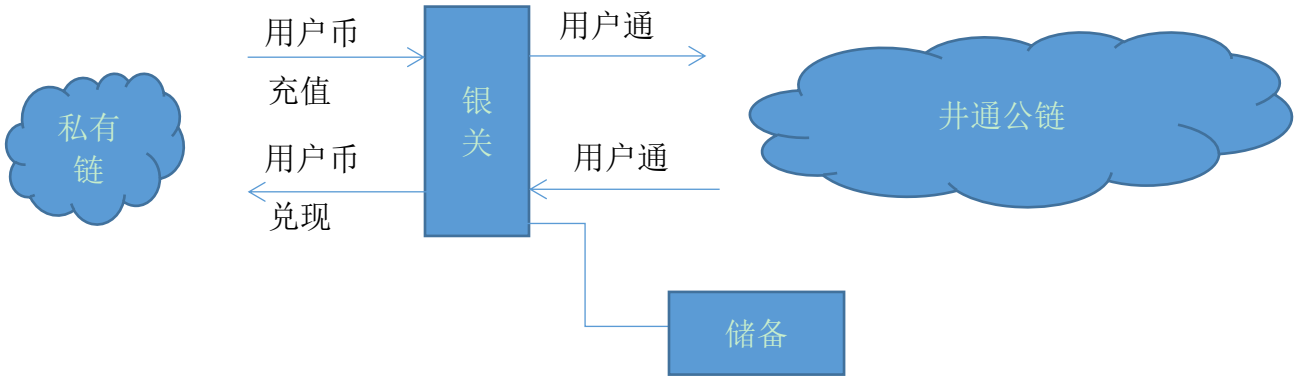
井通银关实现第三方的资产在井通网络中的接口。第三方的资产通过银关进入井通网络，并发行相应的用户通。如果用户通需要兑现，则也必须通过银关来获得资产。

在井通网络中以 CNY 标记的用户通是一个很好的例子。

应用场景一



应用场景二



2.5【分层与智能合约】

井通合约系统实现过程：

a) 我们采用TX驱动的做法，合约的创建，合约功能的调用，都由TX发起，如果执行的过程中需要修改用户的余额，则会发起交易并发到下层的TX，所有这些交易都将在TX执行验证并记录在底层的区块链中
b) TX层的交易不受合约的影响
c) TX层的跟合约相关的交易以单独的TX的方式保存合约的代码 和状态，合约的具体状态对应于对合约相关功能的调用及参数，TX层的状态 hash保证信息的一致性。
d) 合约层的执行由多个合约节点contract validator执行，以确定性的方式分别执行并进行共识
e) 每个合约节点采用VM执行代码
f) 合约节点保存合约执行的storage

在这样的分层设计下，我们进一步优化了井通系统，使得合约的调用采用异步的方式，在此基础上，实现合约的快速调用和返回，同时支持用户选择分片的方式来执行智能合约，不需要所有的节点都做同样的事情，提高了整个系统的处理能力。

2.6【智能合约的异步调用】

现有的智能合约的执行采用同步方式，利用交易触发或者自动触发合约调用，合约在具体执行的时候，区块链的共识机制必须等待合约执行完，返回结果后才能继续操作，从而完成对当前区块的共识。

这样的智能合约执行方式具有以下缺陷：

（1）合约执行的速度严重影响区块生成的时间：

因为区块共识依赖于合约执行的结果，每个节点必须对合约的结果的一致性达成共识，因此，合约的执行速度的快慢，直接影响区块后续操作，导致区块生成时间的延迟。

（2）合约执行的速度严重影响区块链能够支持的合约执行并发量：

在区块链生成的频率通常大致固定的情况下，在同样的时间段内，一个合约执行的快慢，将直接影响到同区块其他合约的执行，极端情况下，一个恶意的合约可能导致系统无法处理其他的合约，导致处理合约的并发量大大降低。

（3）合约执行过程中的容错能力受限：

由于采用同步执行的方式，合约执行时针对各种错误情况的处理需要全面考虑，并且实现对各种时间敏感的操作的快速处理，比如需要对各种操作的超时情况作相应的处理。

一些现有的解决方案，如以太坊，采用 gas 的方式， 对每个合约进行运算量的估算，并且利用一个系统总 gas 量来控制当前区块能支持的总运算量，来保证共识的按时完成。但是系统能支持的合约总数受到这个总量 gas 的限制，如果合约的代码越来越复杂，整个系统能支持的合约数就越来越少；另外，以太坊共识时间有限，gas 的最高值并不能大幅增加。

针对现有智能合约执行技术存在的问题，井通提供一种跨区块异步调用合约系统，该系统的区块共识不依赖于合约执行结果，可提高合约执行的并发量以及区块能支持的合约数量，提高系统容错能力。

井通的异步调用合约系统，包括以下单元：

1. 分布式系统验证单元：包括一个或多个服务节点以及若干个验证节点，用于接收用户递交的交易请求集合{TX}，包括合约调用请求 TX 和支付请求 TX；
2. 分布式合约执行单元：位于本地或远端的分布式系统验证单元，与分布式系统验证单元之间通过预定义协议进行通讯，用以获取合约执行所需信息，并在合约执行完毕后，将结果返回至验证节点；
3. 合约执行缓存单元：包括用于接收来自验证节点的合约调用请求，发送合约调用请求至分布式合约执行单元，接收合约执行结果，返回当前合约执行状态至验证节点，以实现合约的异步调用；

该系统实现方法如下：

1. 服务节点接收用户递交的交易请求 TX，每个验证节点收集上述 TX 并汇集成交易请求集合{TX}i；

2. {TX}i 中包含的合约调用请求发送至合约执行缓存单元，合约执行缓存单元在收到上述请求后立即返回当前合约执行状态；
3. 在所有验证节点收到{TX}i 后，{TX}i 在所有验证节点完成共识，区块 i 生成，验证节点对共识后的{TX}i 进行验证，验证后的状态写入区块 i；同时每个验证节点创建一个查询合约 TXq，并将其加入到区块（i+k）的交易请求集合{TX}（i+k）中；
4. 在进行 1~2 时，合约执行缓存单元采用异步调用的方式将合约调用请求发送至分布式合约执行单元，于后台执行合约，执行完毕后，合约执行缓存单元获得合约执行的最后结果，等待处理；
5. 区块（i+k）处理周期开始，{TX}（i+k）中包含的合约调用请求发送至合约执行缓存单元，合约执行缓存单元立即返回当前合约执行状态，同时，验证节点从查询合约 TXq 中提取出合约相关信息，并向合约执行缓存单元发出查询请求，合约执行缓存单元向验证节点返回区块 i 的合约调用请求的执行结果，并更新查询合约 TXq；
6. 在所有验证节点收到{TX}（i+k）后，更新后的查询合约 TXq 和{TX}（i+k）合在一起形成一个新的集合，在所有验证节点完成共识，区块（i+k）生成，验证节点对共识过的 TX 进行验证，验证后的状态写入区块（i+k）。

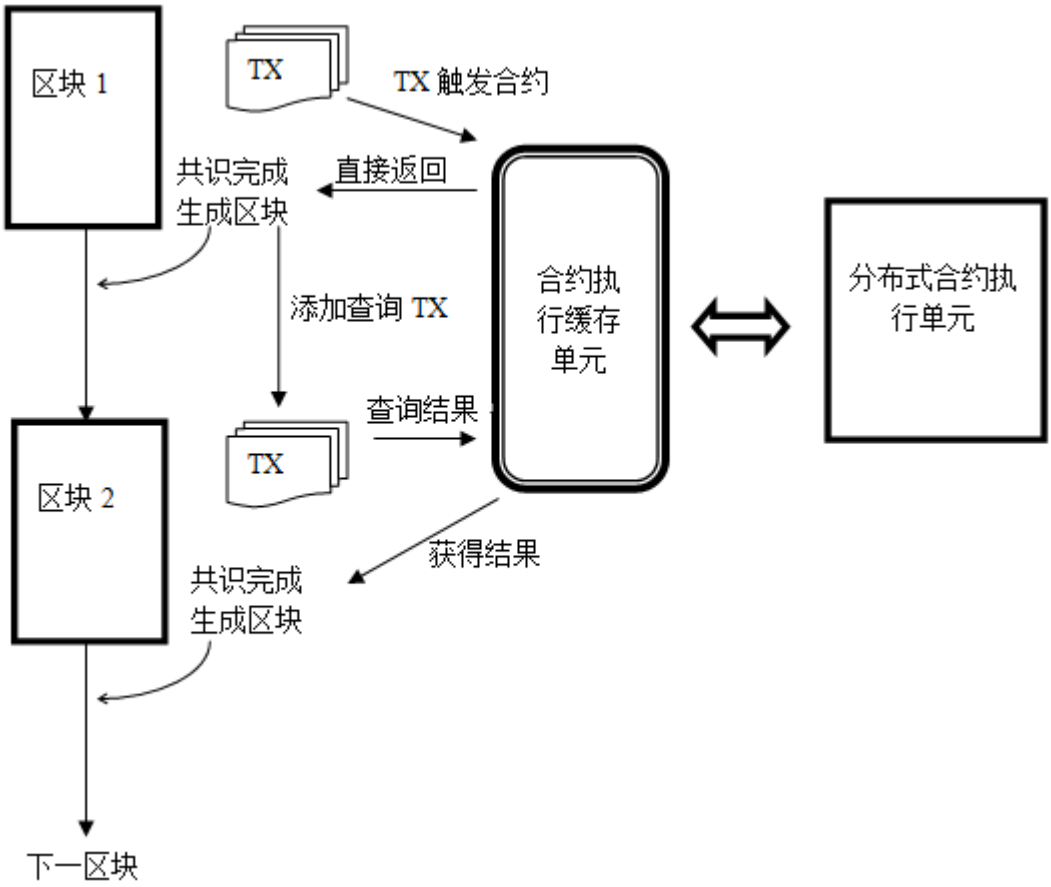
井通的区块链系统以异步调用作为后台核心技术，与现有智能合约执行技术相比具有以下优势：

（1）隔绝了合约执行和系统共识单元，合约的执行可以在远端，使得合约的执行不再占有系统共识的资源；

（2）合约执行单元和系统共识单元的去耦合，使得合约执行模块和共识模块相对独立，支持热插拔；

（3）在共识验证单元和合约执行单元之间设立合约执行缓存单元，在整个合约执行过程中创造性地采用了异步调用执行方式，使得合约的调用和执行结果在跨区（区块 i 和区块（i+k））之间分别实现， 同时又能保证各个验证节点之间完成共识；该种合约异步调用执行模式提高了合约执行的并发量，共识的过程无需要等待合约的执行结果，大大提高了区块能支持的合约数量。

（4）提高了整个系统的容错能力，一方面系统可以设置合适的超时处理机制来处理合约延时的情况，另一方面，用户可以在合约调用中配置合适的 k 值来保证长时执行的合约得到正确处理。



2.7【基于智能合约的快速交易】

现有基于区块链的分布式交易方式因区块链共识方式、区块链生成时间、区块的生成时间、区块的大小而受到很大的限制。基于区块链的交易速度一般都在秒级、甚至分钟级以上，此外，还存在如下缺陷：

1. 交易请求在分布式系统中的传播过程存在延迟，从某个发起节点到信息传播至其他所有节点之间存在信息延迟；

2. 共识过程存在时间延迟：数据的更新必须在共识完成后才能写入账本中，这种写入是间歇性的，每个验证周期更新一次，用户对数据更新的请求必须在更新周期之后才能得到响应并返回；

3. 现有的基于智能合约不仅受到以上两点的影响，还受到合约执行延迟的影响。

一些现有的解决方案，如闪电网络、比特币网络采用通道的办法来加快对交易请求的处理，但上述方案的协议或者比较复杂，或者采用了非拜占庭容错的方式，限制了其更广泛的应用。

井通实现了一种基于区块链合约的快速交易系统。在异步调用合约的基础上，对合约节点分成两种：普通合约节点和快速交易合约节点。普通交易合约节点与验证节点之间通过预定义协议进行通讯，获取合约执行所需信息，合约执行完毕后，将结果返回至验证节点；快速交易合约节点执行快速交易请求并将执行结果返回至合约接入服务器。

快速调用的具体实现方法如下：

（1）快速交易初始化：两个或多个需实现快速交易的用户之间达成一致并创建一个合约，发起一个快速交易初始化请求 tx，合约接入服务器经服务节点将该 tx 发送至验证节点形成交易集，验证节点对该交易集进行共识；完成共识后，验证节点将该交易集发送所有合约节点，依据预定义协议通过分布式随机算法在其中随机且确定性地选取一个快速交易合约节点；

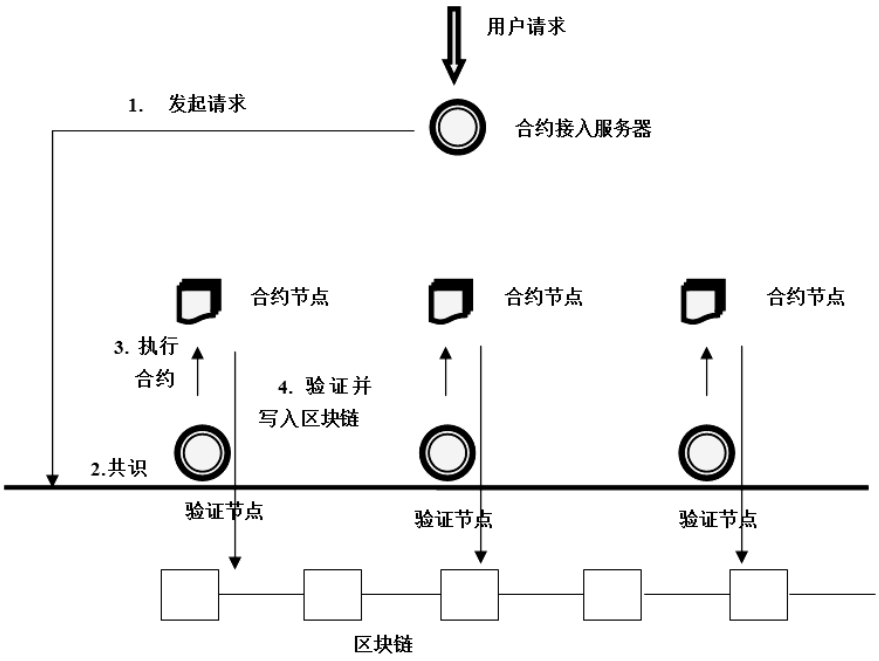
（2）快速交易实现：用户发起快速交易执行请求，合约接入服务器经服务节点将该请求发送至快速交易合约节点，于该节点执行交易请求，直接返回快速交易结果至合约接入服务器，同时该服务器记录交易状态，并保存自上一次确认后的所有快速交易历史；该快速交易合约节点的交易执行方式可以通过非对称加密方式或者其他方式（例如对称加密方式）运行，使得合约/交易的执行是保密的，仅对用户和当前合约节点可见。用户可通过合约接入服务器查询交易的历史记录；

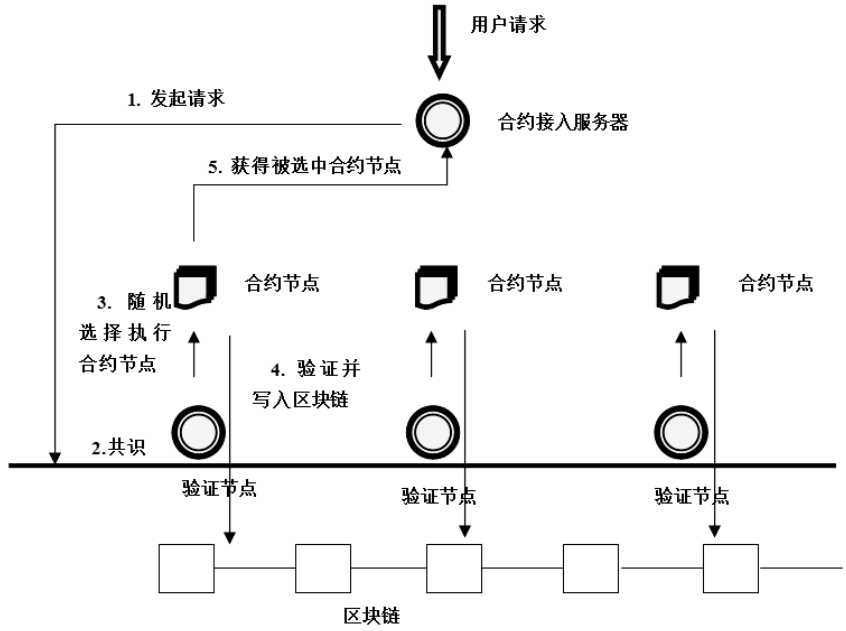
（3）快速交易历史的分布式确认：用户可在各方签名验证的情况下，对可未确认的交易主动周期（比如 10 分钟、1 天、1 周）或非周期性发起确认交易请求 tx，也可以根据实现定

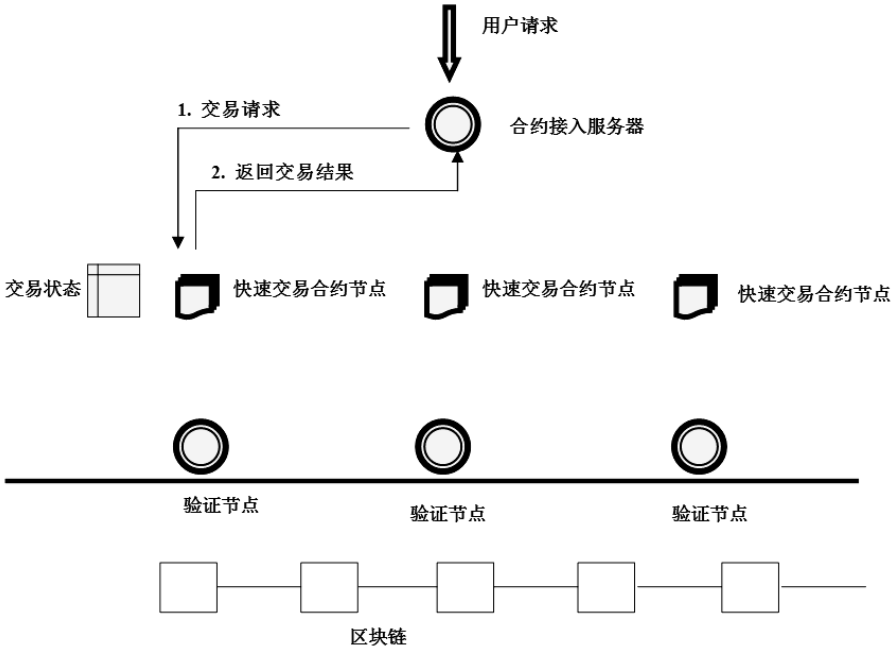
义的合约定时对发起确认交易请求 tx；发起的确认交易请求 tx 与上述未确认的交易历史合并，产生一个自上次确认后到当前状态的变换交易；合约接入服务器经服务节点将该变换交易发送至验证节点，验证节点对交易集进行共识，再将其发送至所有合约节点进行合约执行，合约执行结果经验证节点验证并确认，与其他交易信息（普通交易或普通合约执行信息）一起写入区块链，同时该合约执行结果返回给客户，通过共识节点对历史交易记录进行确认，从而实现交易确认的拜占庭容错。

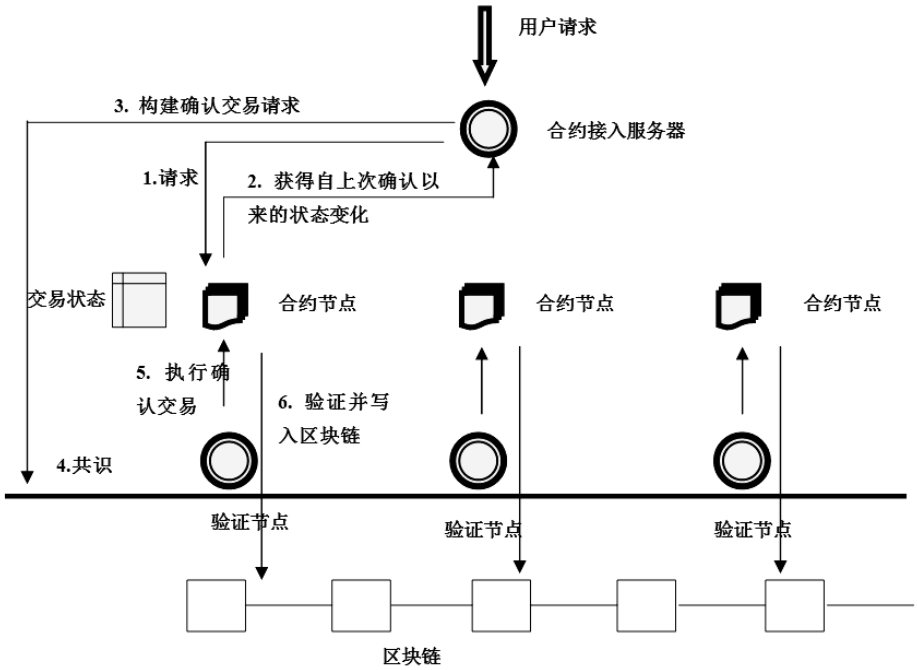
当用户重复步骤（2），选取下一个快速交易合约节点后，原来的快速交易合约节点的交易历史将被清空。

这样，井通系统分为独立的合约层和底层共识层，快速交易对合约层发起调用，在合约层实现快速交易，其快速执行结果周期性或非周期性返回底层共识层进行验证确认并写入区块链，使得交易的执行不受区块关闭的时间和区块大小的影响，也不受分布式网络传递的影响，同时具备分布式区块链固有的优点，克服了现有区块链交易方式在交易传播、共识过程以及和合约执行过程中存在的延迟现象，以接近实时的方式实现对交易的快速支持，维持了交易系统的拜占庭容错性，可实现对交易细节的隐藏和加密，同时保持了分布式系统的数据的一致性和完整性。




用户请求
1. 发起请求
合约接入服务器
5. 获得被选中合约节点
合约节点
合约节点
合约节点
3. 随机选择执行合约节点
4. 验证并写入区块链
2.共识
验证节点
验证节点
验证节点
区块链


用户请求
1. 交易请求
合约接入服务器
2. 返回交易结果
交易状态
快速交易合约节点
快速交易合约节点
快速交易合约节点
验证节点
验证节点
验证节点
区块链



2.8【分片调用技术】

基于智能合约的快速交易可以看成是一个分片技术的特例。从更通用的概念讲，对智能合约执行节点的选择性执行，就是一个分片技术的实现。

除以上所描述的快速交易外，如果多个智能合约节点之间通过预定义的协议（BFT）来实现之间的信息同步，那么他们之间就实现了一个 BFT 的共识。当然，采用这样的公识之后，对智能合约的处理效率会降低，但是比通常的全部节点同时处理一个合约的情况，仍然大大提高了。

3. 展望

井通系统采用了多货币的支持以及优化的智能合约，使得整个系统以一个多层次的，逻辑分开的快速系统为之上的各种应用提供可靠的保证。但是区块链技术还是在一个相对早期的技术发展阶段，我们预计在接下来的几年，区块链技术将得到更加迅猛的发展，同时各种应用也将层出不穷。井通将继续努力和保持对区块链技术的创新，为整个区块链社区的发展作出贡献。