2019年3月28日

Coin of Things：一种点对点物联网电子现金系统

—岂克文 2019.4

1. 概述

当前Blockchain技术实际上是基于多节点共识的强同步全局一致账本系统，所有的交易都需要此全局账本进行确认，因而导致交易TPS（Transaction Per Second）出现中心瓶颈，难以提升。而物联网系统中设备间的交易量将是异常庞大的，Blockchain的架构难于满足物联网系统交易规模的需求。针对物联网设备之间的价值流动需求，本文提出了一种分布式异步账本系统，实现设备间微支付CoT（Coin of Things），基于分布式异步账本系统，系统可以实现分布式异步交易确认，解决交易确认瓶颈，支持大规模的并发交易。

2. B-Tangle

2.1 交易结构

本文提出了一种新型的交易数据组织结构及其对应的共识机制和激励机制，如下图所示，基于DAG数据结构组织交易，采用tangle技术实现分布式的异步并发交易验证，并通过一条POW主链来完成交易顺序和一致性确认。此技术结合了BlockChain和Tangle的技术架构，简称B-Tangle。

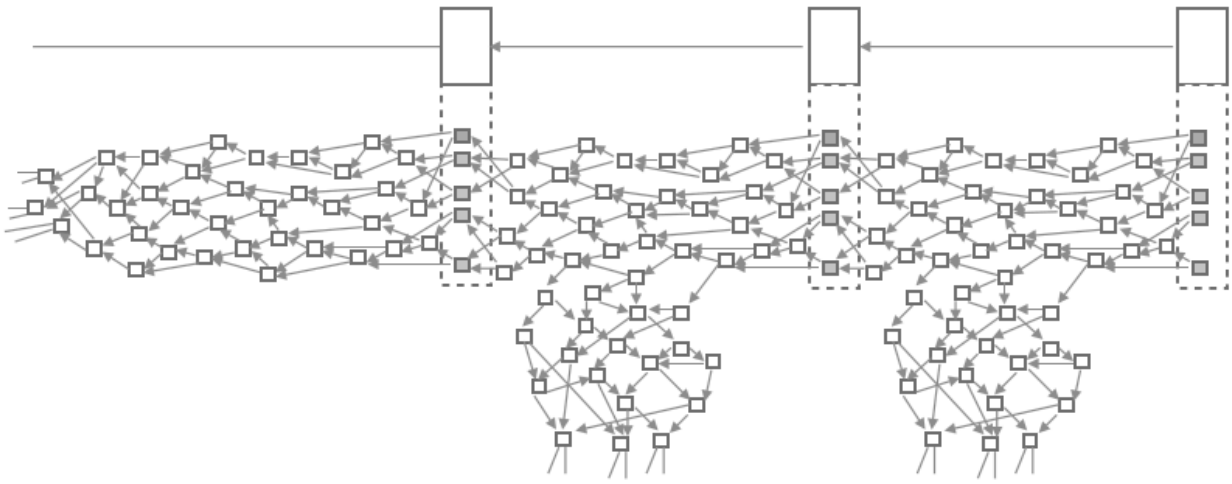

图1. Block-Tangle架构框图

B-Tangle中，每一笔交易都要验证前两笔交易，同时采用一条POW主链对端点交易Tips进行确认。其中，被POW主链的矿工选中并打包进主链区块的交易被认为是确认的交易Anchor

transactions简称ATips，这些交易可以作为整个交易网络的锚点，所有直接或间接被ATips验证的交易都被确认。

2.2 主链挖矿

B-Tangle的微支付是需要支付少量手续费的，一方面用于鼓励矿工对Tips交易进行验证，另一方面，可以防止攻击者制造大量垃圾交易对系统进行DDos攻击，保护系统安全。如图中所示，由于采用主链末端交易确认方式，未确认交易位于两个主链的区块之间的数量变的比较固定，不至于太长，所以新交易对于前两笔交易的确认也变的缩短很多，将会对交易速度有较大的提升。由于矿工总是偏向于寻找手续费较多的Tips交易进行确认，所以，对于越长的DAG交易链越会优先被确认，从而使得多数的交易确认时间控制在一定范围内。

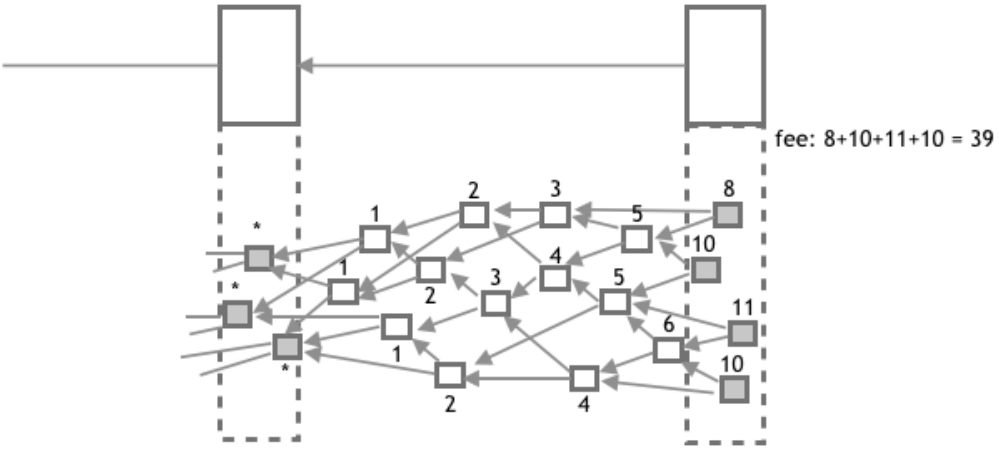

图2. Block-Tangle矿工手续费机制

被上到主链的Tips交易验证引用的交易，是做了确认的交易，每笔交易有一个手续费积分，手续费积分大小为本笔交易距离上个主链Tip交易中多条路径里最长路径的长度（间隔的交易数量），而矿工验证一笔交易将会获取Tips交易积分数量的手续费。

2.3 防双花交易

B-Tangle的防双花技术原理如下图所示，假设交易1和交易2是两笔双花交易，根据交易1和交易2被后续交易确认的情况可以分为以下A、B、C三种类型：

如下图A型，交易1和交易2在后续交易中刚好在上链Tip交易处产生交集，此Tip交易可以发现交易1和交易2的双花现象，所以在矿工验证交易的时候会被发现而被无效掉其中一笔交易。

如图中B型双花，1和2交易的后续交易延续到两个上链的Tips交易，矿工通过两个Tips对交易验证链条进行前向溯源，最终也会发现1和2两笔冲突交易。

图中C型，1、2两笔双花交易由于2交易的后续交易与1交易未有交集，其格子最终的最终Tips交易也未同时上链，因而暂时未被发现，但是由于2的Tip交易未上主链，所以，实际上交易2并未被确认，所以实际上也未能形成双花。

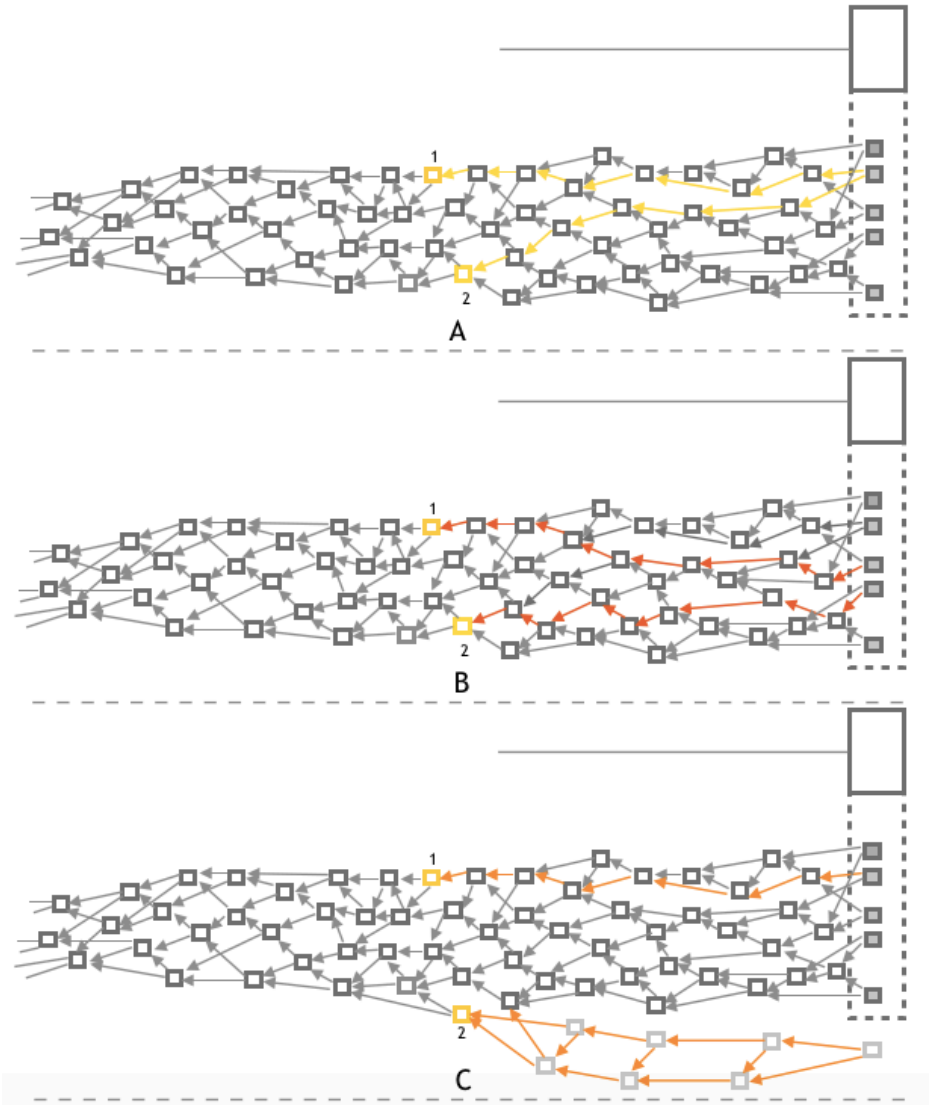

图3. B-Tangle 防双花原理

2.4 分布式交易

两个Block以内的微支付交易采用Tangle技术，每一笔交易验证前两笔交易，只有Tips交易需要发布到主链上进行确认，全网需要传输的交易数据大幅缩减，整个网络可以分区实现分布式的异步并发。

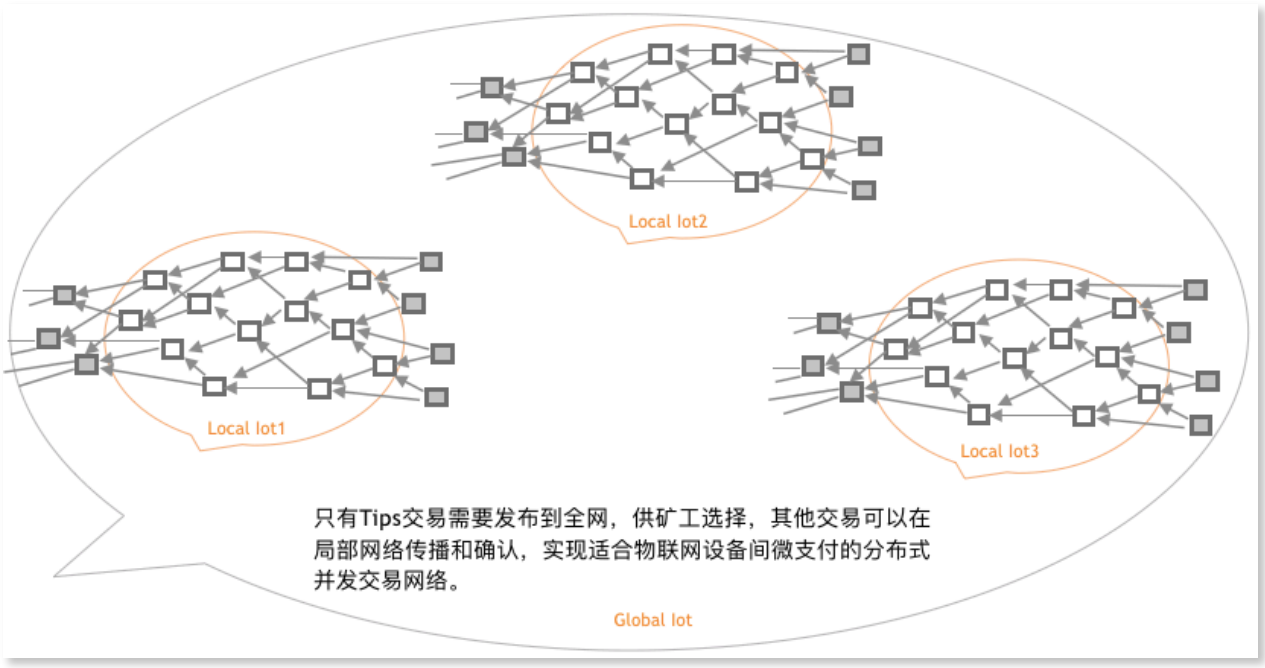

图4. CoT 分布式交易网络

2.5 LPOW共识

本文介绍了一种基于轻量级的权益证明的共识机制—LPOW（light proof of work）。延续工作量证明实现共识的设计理念，LPOW证明过程中，代币的投注消耗相当于工作量证明中矿工算力支出的经济等价物。区块打包权的选择上，POW中采取的是各个节点比赛随机散列（hash）计算的方式，实现了与经济投入（算力投入）成正比的概率随机选中每个区块打包的矿工节点，对应的LPOW中利用比特币网络生产的随机数Nonce，设计了一种新型的共识算法达到与POW相同的效果。通过对经济投注和挖矿节点选举机制的设计，LPOW实现了一种安全性与POW相当，而在能耗、效率上远忧于POW的新型轻量级共识算法。

2.5.1 共识模型

比特币的POW共识算法的关键部分是“工作量证明”概念：对每个区块进行SHA256哈希处理，得到的哈希值为长度为256比特的数值，该数值必须小于不断动态调整的目标数值，本文写作时目标数值大约是2^180。POW的工作量证明的设计非常巧妙，它正好实现了一个基于经济奖惩机制的共识模型。

对POW进一步分析，我们可以抽象出一个通用的共识模型。

我们来设计一个博彩的游戏：每一轮游戏开始前，参与博彩游戏的各个节点，每个节点需要投入一定的赌注参与博彩的活动。假设有M1，M2，M3...Mn, N 个节点参与博彩，每个节点的投入分别是C1，C2，C3...Cn代币量。

游戏规则一：提供N副纸牌，每个人（节点）一副牌，每个人Mi将他们投入的Ci代币用于购买纸牌抽看机，抽看速度与花费价格Ci成正比，谁最快抽出来大于某个数比如K（数字13），谁就能获得CP数额的代币奖励，CP比任何Ci都大得多。这里的潜在假设是洗牌够彻底，每副牌的分布都足够随机。

游戏规则二：如下圆形转盘，每个人将他们的投入Ci用于购买权益角度，这里为了简化，假设每个人的权益角度不可以重叠，设置好N张牌，每张牌上面分别写上“M1”、“M2”、“M3”…“Mn”放置于每个人自己的权益区。有个中间人拨动一下那个转盘，转盘开始转动，规则是那根白色指针落到谁的区域，谁就挖到矿获得CP数额的代币奖励。这里的潜在假设是转盘转动力度是足够随机的，指针停下来的位置不可预测。

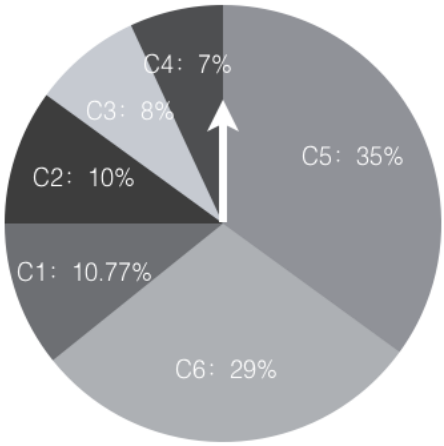

图1 转盘游戏图

对比POW的工作量证明与以上两个游戏，我们可以发现，它们的本质是一样的：其一、每一次游戏都需要一定的经济投入Ci用于获得与之成正比的概率赢得赌局奖励，只是Ci的具体投入形式不一样：POW是用于购买算力，游戏一是用于购买纸牌抽看机，游戏二是用于购买权益区域。其二、不管何总形式，最终需要达到一个目标：节点获得区块奖励的概率与其投入Ci代币量成正比，但每次谁赢得奖励是完全随机的。符合以上两点的设计选择每次胜出的节点来进行打包出块，便可以得到去中介化的共识。

对此我们再来看POW共识算法和游戏一，可以看到：这两种算法中采用节点的投注Ci用于购买算力进行计算，现实中矿工需要购买矿机和消耗电力，这是个不太好的实现，它浪费大量能源；另外，系统需要一段时间的运算来挑选出胜出节点，效率也变得很低。对比之下，游戏二的设计就环保和高效很多，它采用空间换时间的方式：节点的投注Ci用于购买其权益角度空间，通过转盘的随机旋转来挑选出最终胜出的节点，无须消耗能源，消耗时间，却能做到和POW及游戏1一样的效果。

基于经济投注的共识模型：每个节点对每次挖矿进行经济投注，以获取相应与经济投入成比例的资源；设计一个随机选择系统，此系统需要做到能随机选中挖矿节点，并且节点被选中的

概率与其事先投资购买的资源成正比；最后，对于每个区块成功挖矿并记账的节点进行经济激励。

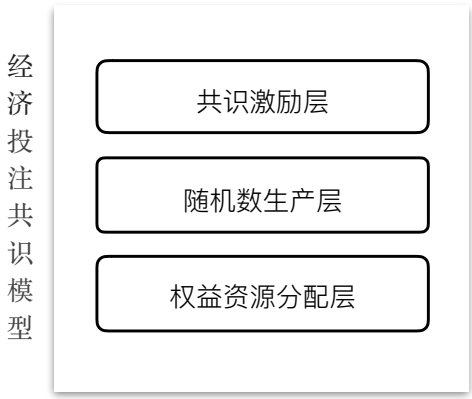

图2 基于经济投注通用共识模型

2.5.2 LPOW

投资共识模型的实现需要设计节点随机选举系统，节点被选中的概率与其投资代币量成正比。这个模型里的关键在于实现一个全网共识并且可验证的随机数，如上游戏二里是用一个物理的游戏转盘来实现。现设计如下挖矿资源分布图：

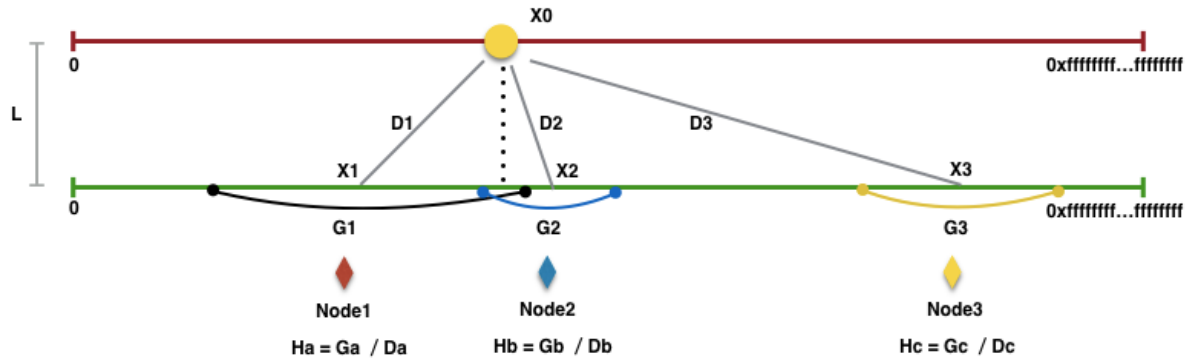

图2 代币量证明技术架构图

如图1所示，LPOW共识架构由三个层面构成：用于选择挖矿节点的随机数生成算法、节点挖矿的具体算法（即依据投注的代币量进行权益资源分配的算法）、共识激励的设计。挖矿节点的选取应当足够随机，并按照节点提供的用于挖矿投注的代币量来做证明，我们将其称为 “轻量级权益证明（Light Proof of Work）”。LPOW与POW本质上是同一种实现架构，不同在于每个层面的实现方案有所区别：POW下工作量证明对应LPOW下的代币量投注证明；POW下挖矿节点的选取依靠的是节点间哈希计算比赛实现，对应LPOW下采用的是共识随机数的生产算法实现。下面具体描述LPOW的实现方案，如上图4所示，设定两条坐标线段，取值范围在0～0xffffffffffffffffffffffffffffffff, 两个线段之间距离为1，其中：

X_n：矿工预先在时间点T_0时，在挖矿资源线段上选取一个点Xn作为挖矿的 “哈希碰撞点”；

X_0: 当前区块往前倒推32个区块的比特币网络的Nonce值，随机数X_0 = Nonce;

G_n：为节点投资共识挖矿的代币量，用于代币量证明；

D_n：为X_0所在横轴位置与A节点所申请权益空间的中点之间的距离；

H_n：为挖矿权重，取$H_n = G_n / D_n = G_n / (\sqrt{(X_n - X_0)^2 + L^2})$；

节点挖矿算法如下，每个挖矿节点进入挖矿时，先提交G_n用于做Gas量证明，并设定X_n，矿工设定X_n超过32个比特币区块以后才能开始挖矿，对于每个区块的随机数X_0，挖矿节点满足以下条件则挖到本次区块：

所有节点计算权重$H_n = G_n / D_n$，区块链系统设定H_0为难度值，$H_n > H_0$的节点挖矿成功，获得区块打包记账权，同时获得相应挖矿代币及手续费奖励，所有抵押上来挖矿的Gas进入黑洞地址销毁。每个区块的挖矿奖励为固定值 V，矿工依据V和当时手续费情况投入合理数量的Gas进行挖矿。系统可能有多个分叉，权重总和最大的分叉为合法链。H_0设定一定周期可以进行调整，以减少分叉数量。

2.5.3 安全性分析

基于已经被确认的比特币区块的Nonce值来选中每个区块的生产者生产区块，因而具备即时确认性，只有当比特币网络被攻击的情况下，链的安全性才会受到影响。

注：这里提出的是一种最基本的挖矿算法，后续会根据实际测试情况作进一步的性能和安全性方面的优化。

3. 性能对比

IOTA的Tangle、Blcokchain、B-Tangle三种技术的扩展性能对比，如下图5所示：随着用户规模的增长，IOTA的缠结网络具有良好的扩展性，交易量越大，系统越活跃，确认越快，系统效率越高，但是由于没有手续费，可能存在大量垃圾交易形成DDos攻击。而区块链系统包括XDAG、Confulx等Block DAG的技术，由于需要全网同步随着交易量的增加则越来越拥堵，可用性越来越差。而B-Tangle网络采用POW主链+Tangle的架构，随着交易数量的增长需要主链交易确认的交易数在稳定状态，所以处于稳定的高性能状态。

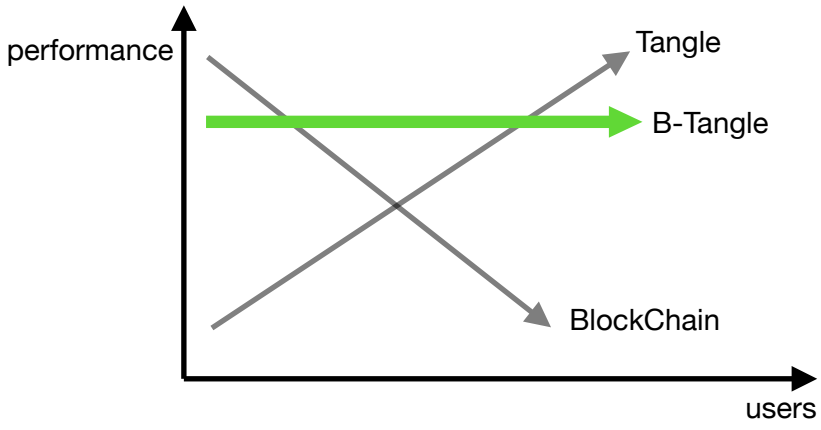

图5. 三种网络系统的扩展性对比

IOTA Tangle属于全网异步并发、Blcokchain(包括XDAG)需要全网同步、B-Tangle需要部分同步(如图8中所示，仅每个Block处上链的Tips交易需要同步)。

4. B-Check

B-Tangle技术里，虽然网络可以实现异步并发，但是对于单笔交易的确认速度还是不够迅速，需要一定时间的等待，每一笔需要等到后续间接引用它的Tips交易被主链引用，并且主链有几个确认之后才算交易得到安全的确认。以以太坊 12S出块速度为例，这里的交易至少也需要几十秒才能被确认。而这个速度在一些交易实时性需求比较高的场景下是比较难以接受的，比如用户拿着手机在自动售货机上付款买货，又比如拿着手机扫码支付进地铁等等类似的交易场景，其交易是必须得到立即确认的。基于此类交易需求和实际场景的分析，本文提出了一种类似支票的快速支付技术解决方案：B-Check技术，以此方案进行交易支付，可以得到立即的确认，其原理如下：

1、在主链上创建B-Check支付节点组，现实中，支付节点(特别是物联网节点)一般是比较固定的，比如我们生活中可能大部分的支付情况发生在以下几个点：楼下的便利店、附近的某几个超市、商场、地铁口等，而家里的智能电表也许只与供电局节点有交易，跟其他节点都不会发生交易，情况更加简单。因此可以创建如图中所示的交易组列表，交易组节点地址列表Addr_i存储在链上，同时每个节点需要抵押一定的数量的币Mount_i，用于后续的花费。规则是：列表以内的任何节点都能且只能与列表以内的任意其他节点进行交易。如此可知，列表以内的交易，其“双花”交易，只能被限定在列表以内的这些节点，另外，每个节点的最大花费是Mount_i。

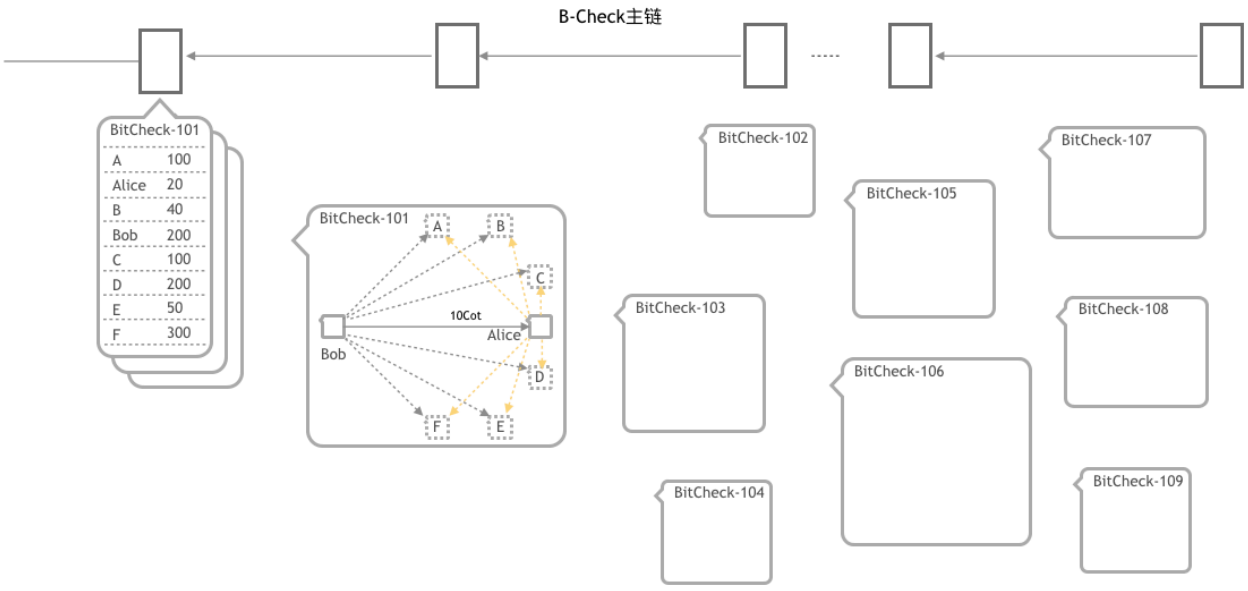

图6. B-Check技术原理框图

2、假设Bob想给Alice发一笔交易10Cot，那么，Bob将此笔交易组装并签名好之后发送给Alice。首先，Alice需要用Bob的公钥验证这笔交易是从Bob合法签名发出的；其次，Alice要依次询问Alice、Bob共同所在的交易组列表内的所有其他成员，确认Bob的最新余额是够本次这一笔

交易的，同时确认其他成员是否也同时收到了Bob的交易，即验证Bob是否花费了超过其余额的交易，进行“双花”。如果验证发现，Bob的支付交易超出了其余额，则拒绝接受本次交易，如果没有，则认为这笔交易没问题，并把交易信息保存起来。

这其中，可能存在的一点情况是：其他成员比如C，也跟Alice收到了Bob的支付交易，但是C不给Alice提供交易真实情况，假装没收到，那么，Bob就可能花费超出其余额的资金，形成“双花”。最终对交易进行主链合并的时候会发现因为C不诚实导致Bob抵押的资金不足于兑现给Alice和C两方，这种情况下如何处理？我们需要定一个惩罚规则，并设定一个系统没收的双花手续费(比如5%)：我们规定时间戳更新的交易是合法的，那么Bob账户上的资金扣除系统双花检测手续费之后，会先被转给Alice，剩余部分的资金再转给C，C不诚实，只能自己受损。而Alice如果不去查询其他成员的交易而导致的双花，那么，Alice会损失部分手续费。最终的结果是：Alice会积极地通过其他成员查询的Bob的交易记录，否则她可能损失部分手续费；C会需要积极配合Alice的查询，否则，他可能会损失被Bob双花的那个交易数额的币。

3、Alice随时可以将收到的交易发送到主链上，进行兑现。可能会收到很多单之后一起发送到链上进行兑现，矿工节点会将多笔相同收发方的交易合并成一笔进行打包上链（主链需要支持合并交易）。Bob花完的钱，后续可以继续抵押一定数量的币上去，继续后续的花费。

5. 代币循环

建立一个分布式加密网络的初衷是让物联网变得健壮、可靠、安全、自治，这个网络没有中心化的服务商来维持，所以，需要像比特币那样建立一套Token和矿工体系，通过Token的流转实现一套经济激励机制来调动矿工对网络进行维护，以维持网络的安全运转。如下图所示，通过法币、物联网币COT实现外部能源对系统的输入，维持整个网络系统的可靠运行。

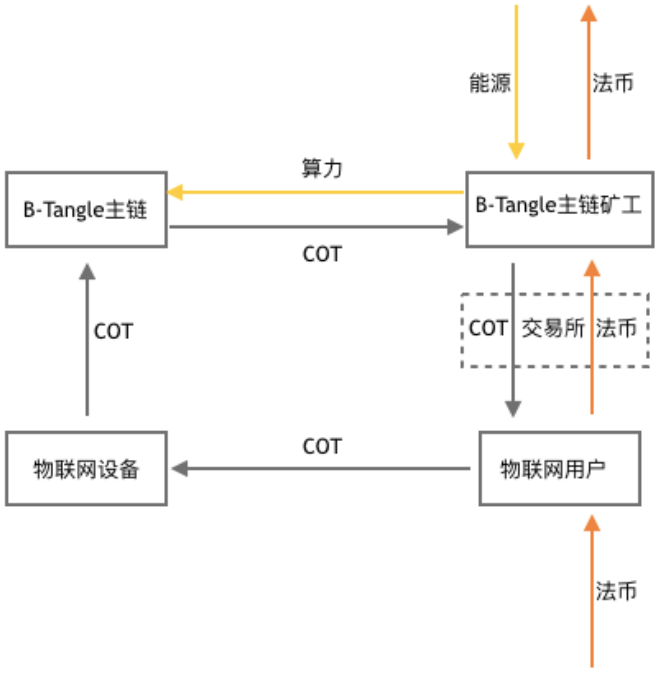

图7. COT代币在B-Tangle生态系统中的流通经济模型

附录：安全性分析

系统设定权重和最大的分叉为合法链，假设交易以6个区块确认为准。比特币网络的最近6个Nonce值分别为：N^0 、N^1、N^2、N^3、N^4、N^5，如果有恶意节点想更改已6个区块之前的区块的交易历史，他将需要获得最近六个区块的打包权，也即需要：

$H^0 = G^0 \ / \ D^0 > H_0$；即 $G^0 > H_0 * D^0 = H_0 * \sqrt{((X - N^0)^2 + L^2)}$；

$H^1 = G^1 \ / \ D^1 > H_0$；即 $G^1 > H_0 * D^1 = H_0 * \sqrt{((X - N^1)^2 + L^2)}$；

$H^2 = G^2 \ / \ D^2 > H_0$；即 $G^2 > H_0 * D^2 = H_0 * \sqrt{((X - N^2)^2 + L^2)}$；

$H^3 = G^3 \ / \ D^3 > H_0$；即 $G^3 > H_0 * D^3 = H_0 * \sqrt{((X - N^3)^2 + L^2)}$；

$H^4 = G^4 \ / \ D^4 > H_0$；即 $G^4 > H_0 * D^4 = H_0 * \sqrt{((X - N^4)^2 + L^2)}$；

$H^5 = G^5 \ / \ D^5 > H_0$；即 $G^5 > H_0 * D^5 = H_0 * \sqrt{((X - N^5)^2 + L^2)}$；

需要花费总量：$G = G^0 + G^1 + G^2 + G^3 + G^4 + G^5$ 数值大小的代币才能成功。

由于Nonce是足够随机的，也即可以认为恶意节点获得区块打包权的概率p与其挖矿投入的Gas成正比，因而，其6次都获得区块打包的概率为：