缠结

作者： Serguei Popov
译者：熊志敏 (xiongzm@163.com) 黎明 谭志红

摘要

在本论文中我们分析了 IOTA（一种用于物联网 IOT 行业的加密货币） 中所使用的主要技术。 该技术作为区块链技术的下一个延续发展阶段， 具有在全球范围内实现小额支付的特征。

1 系统的一般介绍

在过去的六年中比特币的兴起和成功证明了区块链技术的价值所在。然而，这种技术也有许多缺点， 阻碍了它成为全球范围内加密货币的唯一平台。 在这些缺点中， 特别值得提及的就是比特币无法进行小额支付， 而小额支付在迅速发展的物联网行业中的重要性不断增加。 这就需要寻找一些完全不同于基于比特币和其他加密货币的区块链技术的解决方案。在本论文中，我们提出了一个称之为 IOTA 的加密货币系统，可用于创建全球范围内基于现有硬件的物联网系统中的一种货币。

在一般情况下， IOTA 按如下方式运行。如前所述，不存在全局的区块链，这里是一个 DAG（有向无环图），也称之为 Tangle（缠结）。通过节点发出的所有交易构成了这个有向无环图 DAG 的集合。这个图中的边是这样形成的：当一个新的交易到达， 它必须验证之前的两个交易， 这些验证关系就通过有方向的边来表示，如图 1 所示（在图中，时间走向总是从左到右） 。如果从交易 A 到交易 B 之间至少有两个有向边的路径存在， 我们就说交易 A 间接地验证了交易 B。我们假定节点检查认证的交易是否存在冲突， 同时节点不会直接或者间接地认证具有冲突的交易。 其想法是随着交易被越来越多的直接或者间接的交易所验证， 这个交易就会被系统所接受； 换句话说， 要接受一个双花交易是极为困难的 （或者至少在实践上是几乎不可能的） 。

在随后的章节中， 我们要讨论选择两笔交易予以接受纳入系统的算法， 用于衡量整体交易的验证算法（第 3 节，尤其是 3.1 节），以及可能会受到的攻击情况（第 4 节）。另外，如果读者对文中的一些公式有所恐惧的话，可以直接忽略并跳转到相应章节中的“ 结论 ”部分。

此外，应该指出的是， 有关有向无环图在加密货币领域中的想法已经有一些时日了，比如文献 [1,2,3,4]。尤其需要指出的是，文献 [2] 中提出了一种类似于我们的解决方案。

译者注： 本文 (V0.1)基于 IOTA白皮书 V0.5 版本翻译而成。翻译中可能存在理解错误，仅供各位参考，如有错误，请批评指正，并联系我们修改。本论文的翻译不构成任何投资建议。欢迎到 IOTA中国社区（ QQ 群 526351486）及微信群讨论交流 IOTA相关技术和项目。

2 权重及相关概念

在这里，我们定义一个交易的自身权重及其相关概念。 交易的权重与发送这笔交易的节点所投入的工作量成正比；在实践中，权重可以假定为 3^n 的一些数值，其中 n 属于可以接受的具有非空间隔的正整数。

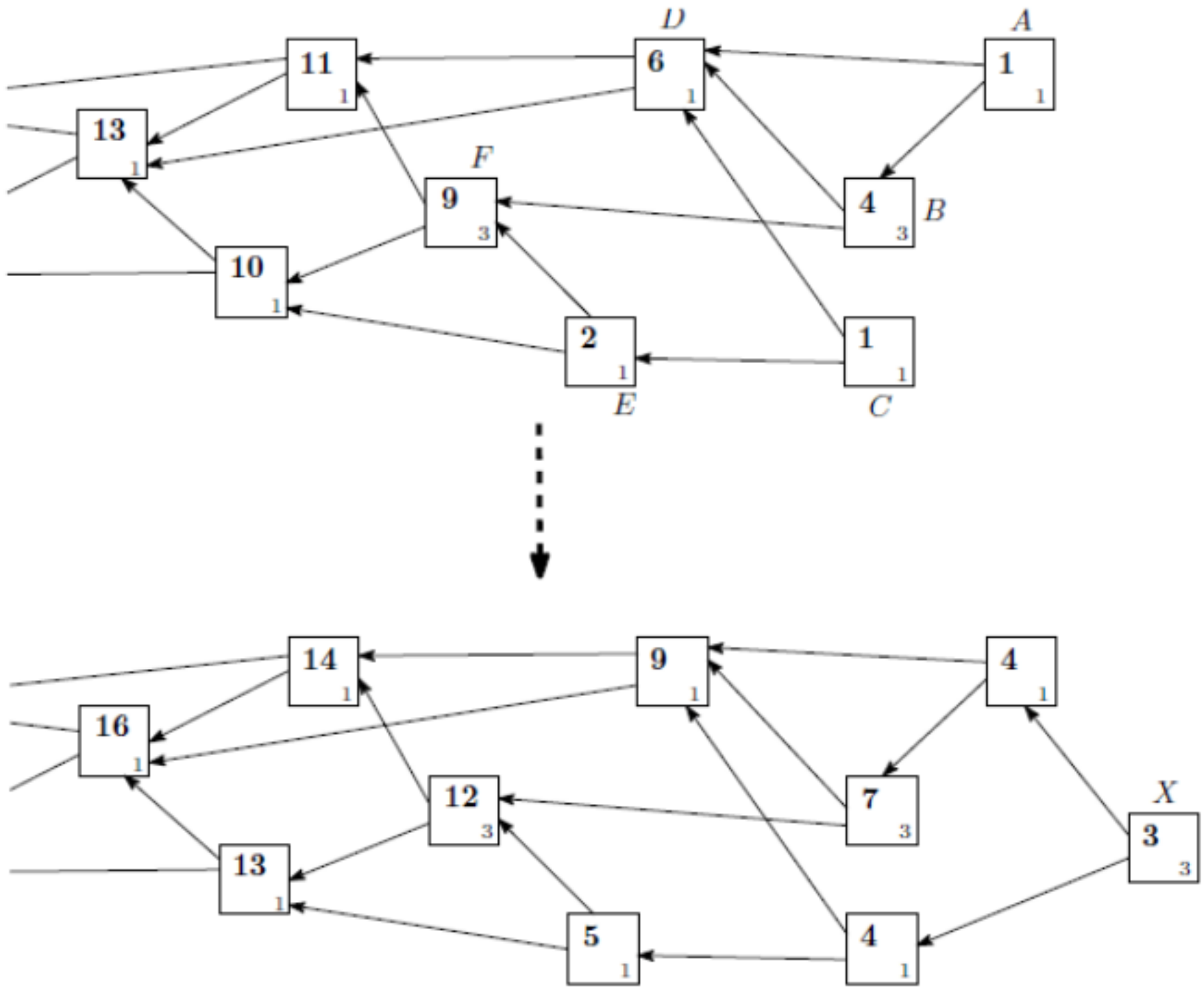

图 1 权重的（重新）计算

我们所需要的一个重要符号就是一个交易的 累积权重 :它被定义为这个交易的自身权重与其他直接以及间接验证这个交易的所有交易的自身权重之和。 累积权重的计算方法如图 1 所示。其中方框代表交易， 方框右下角较小的数字表示这个交易的自身权重， 而字体较大且加粗的数字是这笔交易的累积权重。 例如， 交易 F 经交易 A, B, C, E 直接或者间接被验证。 交易 F 的累积权重就是交易 A, B, C 和 E 的各自自身权重之和，即 9 = 3 + 1 + 3 + 1 + 1。

在图 1 中没有被验证的交易（即 “ tips）”只有交易 A 和交易 C。若一个新的交易 X 进入系统并且对交易 A 和 C 进行了验证，那么交易 X 就是系统中唯一的 tip 了，同时系统中其他所有的交易的权重增加 3（即交易 X 的自身权重）。

为讨论验证算法， 我们需要引入一些其他的变量。 首先， 对于缠结中的一个顶点（比如，一笔交易），我们引入它的：

高度，定义为自创世交易至当前这个交易的所有路径中最长的长度；

深度，定义为自这个交易到某个 tip 尖端的最长路径；

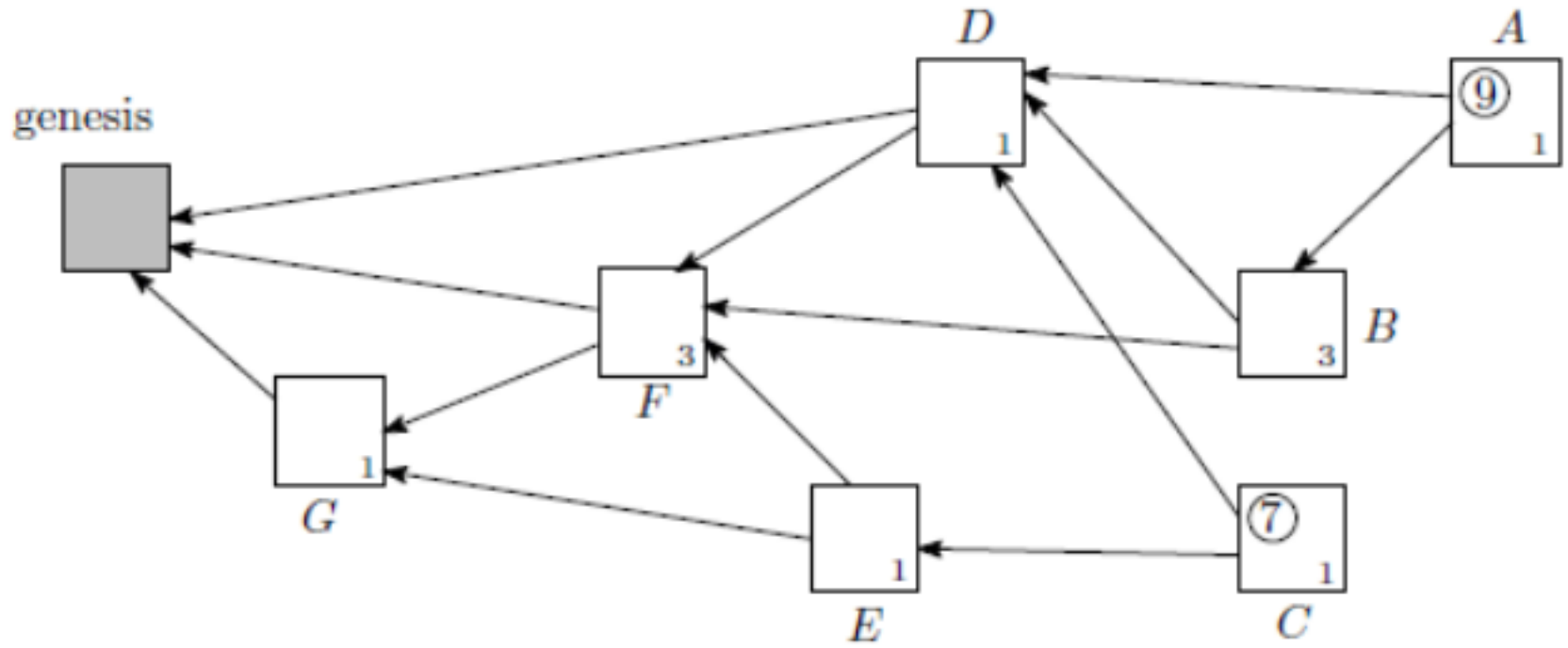

图 2 关于交易的积分计算（带圆圈的数字）

比如，在图 2 中，交易 G 的高度为 1，深度为 3（因为反向路径 F, B, A）；而交易 D 的高度为 2，深度也为 2(译者注：根据论文这个版本中关于高度和深度的定义，译者认为高度为 3，深度为 2；关于高度和深度可参考作者向 Ledger 杂志投稿论文的最新定义)。接下来，我们引入积分的符号。一笔交易的积分定义为它的自身权重与所有它验证的那些交易的自身权重之和， 如图 2 所示。同样的，仅有的 tips 有交易 A 和 C。交易 A 直接或者间接地验证了交易 B, D, F, G，因此交易 A 的积分为 1+3+1+3+1 = 9。类似地，交易 C 的积分为 1 + 1 + 1 + 3 + 1 = 7。

3 系统的稳定性和截断集合

记 L t 为 t 时刻系统中 tips 的总数。当然，大家期望随机变量 L t 保持稳定（更精确地说是正递归的）。直观上， L t 应当围绕一个恒定的常数波动，而不是趋于无穷大（这样的话系统中会存在大量未经验证的交易） 。

为了分析 L t 的稳定性，我们需要一些前提假设。 假设 为交易输入流的速率（泊松分布）；为简单起见，我们假定交易输入流的速率保持恒定。假设所有的设备都大概具有同等的计算能力； 并假定系统总交易数为 N，其中 L 个未经验证的情形下，一台设备要发送一笔交易所需要的平均时间为 h L, N 。首先我们考虑如下的一种策略， 即在要发送一笔交易的时候， 节点从 L 个 tips 中随机任意选择两个并验证它们。 在这种策略下， 可以假定不同 tips 的验证到达时间是相互独立的，那么有速率 /L （可参考文献 [5] 中的定理 5.2)。因此，

在 h L, N 时间内没有任何交易验证给定的一个 tip = exp $\frac{h \ L, N}{L}$ (1)

这意味着在我们的设备发起交易时，　　tips 总数所增加的期望值等于

$$1 \quad 2\exp \quad \frac{h \ L, N}{L} \tag{2}$$

（在上面的公式中，“ 1 ”对应于通过这笔交易所创建的新　tip，而第二项是被“ 擦去 ”的　tips 的期望值）。现在可以看到，　L t 实际上是在空间　　1,2,3,... 上近邻之间进行转换的一个连续无规行走。　如果所选择的两个交易已经被其他交易所验证，那么这个过程就接下来往左跳转一步；　如果所选择的两笔交易都没有被验证，那么接下来就往右跳转一步；除此之外最后的可能性就是保持在原地。

接下来，为理解这个过程的一般行为，我们注意到公式（　2）中的漂移项在 L 较小的时候为正数，而在 L 较大的时候为负（至少在 L　　时，h L, N　o L ；或者只需要假设对计算和交易扩散的主要贡献不是来自于对　　tips 的处理）。在公式（ 2）趋于零时，　L 得到典型值，即　L_0 ，

$$L_0 \quad \frac{h \ L_0, N}{\ln 2} \quad 1.44 \ h \ L_0, N \tag{3}$$

很显然，上面所定义的　L_0 也就是　tips 的典型数量。同时，一笔交易被首次验证所需要的时间大概估计就是　$L_0/$　。

同时，注意到（至少在交易节点试图验证　tips 的情况下）对任意固定　t 时刻，在某一个阶段　s　t,t　h　L_0, N　内那些 tips 构成了一个截断集合，　意味着在时间 t'　t 时发起的交易到创始交易的任何路径都必须通过这个集合。至少在某些偶然的情况下这个截断集合的大小变得非常小，　这是极为重要的。 我们也许可以使用这个较小的截断集合作为检查点，作为　DAG可能的剪枝或者用做其他用途。

上述“ 纯随机 ”策略在实际中不是很好，　因为这种策略不鼓励节点去验证交易：比如“ 较懒 ”的用户也许总是去验证几个较早的固定交易（因此也就对最新交易的验证不做贡献），而这种行为也不会受到惩罚。为消除这类行为，我们需要采用一种策略，以便使得新的交易偏向于验证那些具有较高积分的　　tips。

如下是上述策略的一个例子。选取一个固定的参数　　0,1 ，然后基于　tips 的积分在最前面　L 个 tips 中间任意选取两笔交易。与前面策略中的案例进行相同的分析，于是可以得到这个　tips 集合的典型大小为

$$L_0 \quad \frac{h \ L_0, N}{\ln 2} \quad 1.44 \quad ^{1} \ h \ L_0, N \tag{4}$$

因此，在这种情况下，　求解一笔交易第一次被验证所需要的时间的期望值，　　就有一点复杂了。我们分两个区间进行分析，如图　　3 所示。

低负载区：交易流足够的慢，因此即使　tips 数量相当小，也不太可能发生不

同的交易验证同一个 tip 的情况。

高负载区：交易流足够大，因此 tips 保持较大的数量。

在低负载区域，这种情况就相对简单：在 $^{-1}$ 的时间尺度上会发生第一次验证，因为第一个（或者第一批中的一个）进入的交易将会验证我们的这些交易。

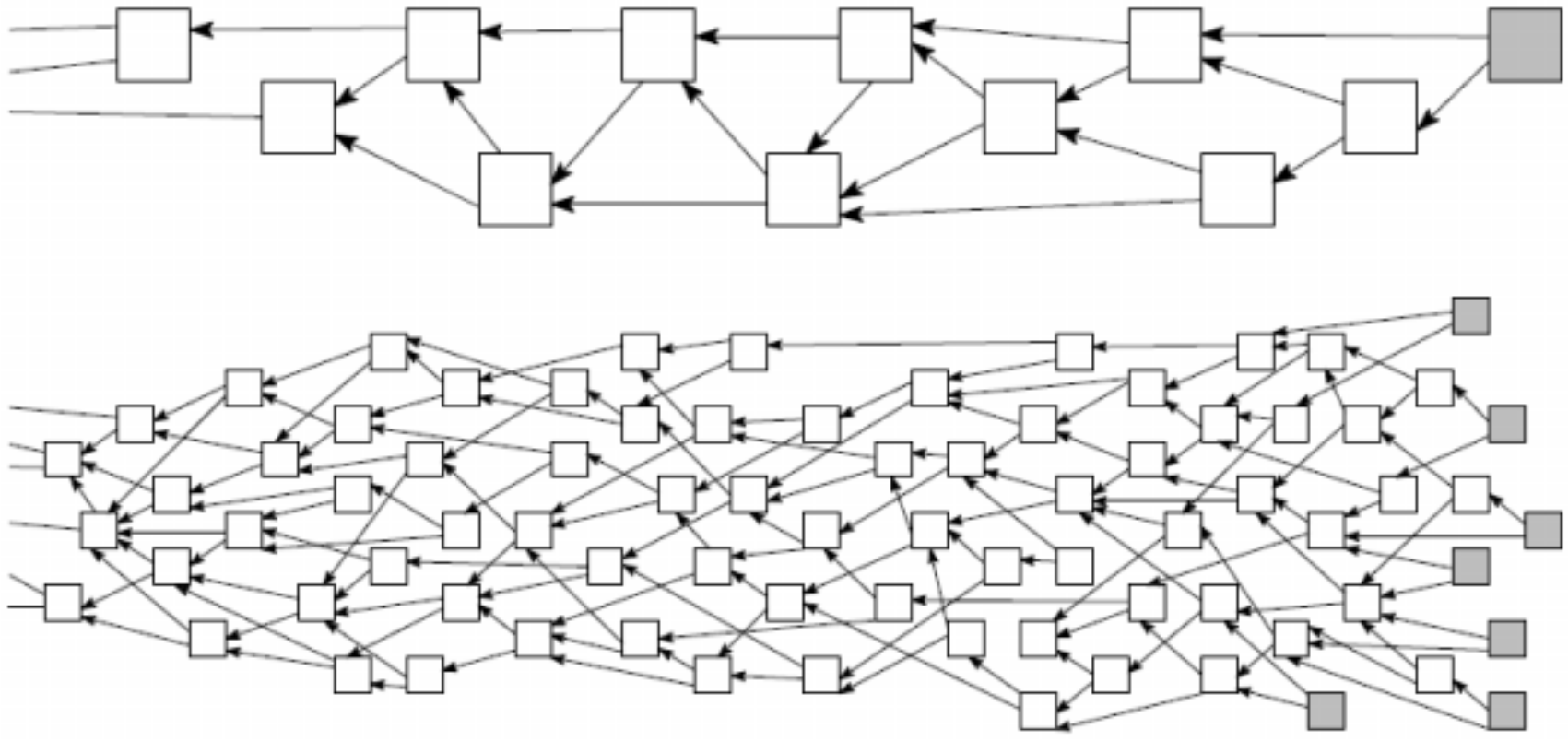

图 3 缠结及其在低负载和高负载情况下典型的 tip 集合（具有阴影的方框） 。需要注意的是在高负载情况下，一些交易也许需要等待较长时间从而得到第一次验证。

现在我们来考虑高负载区域的情况。首先，对于那些没有进入前 L 个 tips 的交易，他们的等待时间将会非常长，大概需要的时间尺度为 $\exp cL_0$ （因为对于较小的 L 值来说，有一个趋向于 L_0 的偏移，同时 tip 集合的大小需要变得比 L_0 还要小，这样才能有被验证的机会） 。因此，在这种情况下，一个较好的策略就是这笔交易的发送者重新发送一笔空白交易， 并且指向和验证前面自己的交易，并希望这个新的交易进入前 L 个 tip 之中。同样的，类似于上面的情况，

另一个比较容易的策略就是选择，比如 5 个随机 tips（在所有的 tips 之中选择），然后对这 5 个 tips 中的最前面的 2 个 tips 进行验证。同样地，如果你的交易在 $L_0/$ $h\ L_0, N$ 时间尺度内没有被验证， 一个好的办法就是发起一个新的空白交易并去验证和推广这笔交易。

我们也注意到上述验证策略可以进行进一步地改进， 以便于防止垃圾信息攻击。举例来说，节点可以偏向于验证那些自身具有较大权重的 tips，从而使得攻击者的垃圾信息交易更加不容易被验证。

接下来，注意到基于高度和积分的验证策略可能会受到特定类型的攻击， 见 4.1 节分析。我们将在那一节中讨论更加详细的策略来防止这样的攻击。无论如何，这种最简单的 tip 选择策略（“ 随机验证两笔交易 ”）仍然是值得考虑的，因为这对于分析来说最简单， 从而也许会给出系统行为方面的一些定性和定量方面

的理解。

结论：

1. 我们区分了两个区间，低负载和高负载区间，如图 3 所示。
2. 在低负载区，通常没有多少 tips（比如说，一个或者两个），一个 tip 在 [1] 时间尺度内得到第一次验证，其中 是进入系统内的交易流速度。
3. 在高负载区， tips 的典型数量取决于验证策略（比如，新的交易如何选择其他的两个交易进行验证）。
4. 对于“随机验证两个 tips”策略， tips 的典型数量由公式（ 3）确定。可以看到这种策略在 tips 的典型数量上是理想的， 但是在实际中不会选用这种策略，因为这种策略不会鼓励新的交易去验证 tips。
5. 对于“随机验证前 L t 个 tips 中的两个 tips”这种策略方案（没有前面那种策略的劣势），其典型的 tips 数量由公式 (4)确定。
6. 然而，我们需要更多精细的策略，这类策略将在 4.1 节中进行讨论。
7. 在高负载区，一个 tip 获得验证所需要的时间尺度为 h ，其中 h 是一个节点的平均计算 / 传播扩散时间。 但是，如果在上述时间间隔内没有获得第一个验证，那么（对于交易发送者或者交易接收者）一个好的方法就是额外发送一笔空白交易来提高验证速度。

3.1 累积权重的增长有多快？

在低负载区，交易被验证几次后，它的累积权重将以 w 的速度增加，其中 w 是一个普通交易的平均权重， 因为本质上来说所有新的交易都将间接指向我们的交易。

在高负载区， 就如上述所观察到的一样， 如果交易足够老并且具有较大的累积权重，那么其累积权重就会同样地以 w 的速度增加。当然，我们看到刚开始的时候交易需要等待一定的时间被验证， 很显然其累积权重在初始时会以较为无规的形式增长。为了弄明白一个交易在得到几个验证之后其累积权重的变化行为，我们记 H t （为简单起见，我们自交易创建开始计时）为 t 时刻该交易的累积权重期望值，并用 K t 表示在 t 时刻验证我们的这笔交易的 tips 数量的期望值。在此，我们简记为 h： h L_0, N 。同时，我们做一个简化假设，认为 tips 的总数大体保持恒定不变（等于 L_0）。这里我们采用“随机验证两个 tips 的策略；可期望其结果大体上与“随机验证前 L t 个 tips 中的两个 tips”策略所得到的一样。

在 t 时刻进入系统中的一笔交易通常是基于 t h 时刻时系统的状态， 来选择两笔交易进行验证。 不难得到至少验证一个 tip 的概率是 $\frac{K_{t-h}}{L_0}$ 2 $\frac{K_{t-h}}{L_0}$ 。

因此我们可以写下如下的微分方程（类似于文献 [5]中的例子 6.4）：

$$\frac{dH\ t}{dt} \quad w \quad \frac{K\ t\ \ h}{L_0} \quad 2 \quad \frac{K\ t\ \ h}{L_0} \tag{5}$$

为了能够使用方程 (5)，我们首先需要计算 K t 。如何立刻去计算 K t 是很困难的，因为在 t h时刻的一个 tip 也许在 t 时刻已经不是一个 tip，并且，在新进入的交易验证了这样一个 tip 的情况下，那么验证原来交易的 tips 总量就会增加 1 个。现在，根据（ 1）和（ 3）可以观察到关键的问题是在 t h 时刻的一个 tip 在 t 时刻仍然保持为 tip 的概率为 1/2。因此，在 t 时刻，有 K t h 的一半的“ 以前 ”的 tips 仍然保持为 tips，而另一半已经至少被一笔交易所验证。让我们用 A 表示（大概）在 t h 时刻 tips 中的 K t h /2 在 t 时刻仍然保持为 tips 的这些交易的集合，而用 B 表示另外一半已经被验证过的 tips。假定新进入的交易至少验证了集合 B 中一笔交易而没有验证集合 A 中任何交易的概率为 p_1 ；同时假定同时验证了集合 A 和集合 B 中的交易的概率为 p_2。显然， p_1 和 p_2 分别对应于在新交易到达时，目前“ 我们 ”的 tips 增加或者减少 1 的概率。因此，得到一些基本关系式：

$$p_1 \quad \frac{K\ t\ \ h}{L_0} \quad 1 \quad \frac{K\ t\ \ h}{2L_0} \qquad \frac{K\ t\ \ h}{2L_0}^{2}$$

$$p_2 \quad \frac{K\ t\ \ h}{2L_0}^{2}$$

类似于方程（ 5），关于 K t 有如下微分方程：

$$\frac{dK\ t}{dt} \quad p_1 \quad p_2 \qquad \frac{K\ t\ \ h}{L_0} \quad 1 \quad \frac{K\ t\ \ h}{L_0} \tag{6}$$

仍然很难准确地求解方程（ 6），因此我们进一步进行简化假设。首先，我们可以看到，对于任意固定 0，在当 K t 达到 L_0 水平之后，K t 将会迅速增长到 L_0。现在，当 K t 相对于 L_0 非常小的时候，我们可以舍弃掉方程 （6）右边最后一项。同时，用 K t h$\frac{dK\ t}{dt}$代替 K t h ，我们可以得到方程（ 6）的简化版（记住 $\frac{h}{L_0}$ ln 2）：

$$\frac{dK\ t}{dt} \quad \frac{}{1 \quad \ln 2} \quad 0.59\frac{K\ t}{L_0} \tag{7}$$

其中边界条件为 K 0 1。求解上述微分方程可以得到

$$K\ t \quad \exp \quad \frac{t \ln 2}{1 \quad \ln 2\ h} \quad \exp \quad 0.41\frac{t}{h} \tag{8}$$

因此，对（ 8）式取对数，我们得到 K t 达到 L_0 的时间大概是：

$$t_0 \quad 1 \quad \ln 2 \quad ^{1} \ h \quad \ln L_0 \quad \ln \quad ^{1} \quad 2.44h \ln L_0 \tag{9}$$

再回到方程（ 5）（并且，如前面一样，舍弃掉右边最后一项） ，我们可以得到在“ 调整阶段 ”（例如，在 t t_0 的时候， t_0 为（ 9）式的结果）具有如下方程：

$$\frac{dH\ t}{dt} \quad \frac{2w}{L_0 \exp \ \frac{\ln 2}{1 \quad \ln 2}} K\ t \quad \frac{2w}{L_0 \exp \ \frac{\ln 2}{1 \quad \ln 2}} \exp \ \frac{t \ln 2}{1 \quad \ln 2\ h}$$

因此，

$$H\ t \quad \frac{2\ 1 \quad \ln 2\ w}{\ln 2} \exp \ \frac{t \ln 2}{1 \quad \ln 2\ h} \quad 2.25w \exp \ 0.41\frac{t}{h} \tag{10}$$

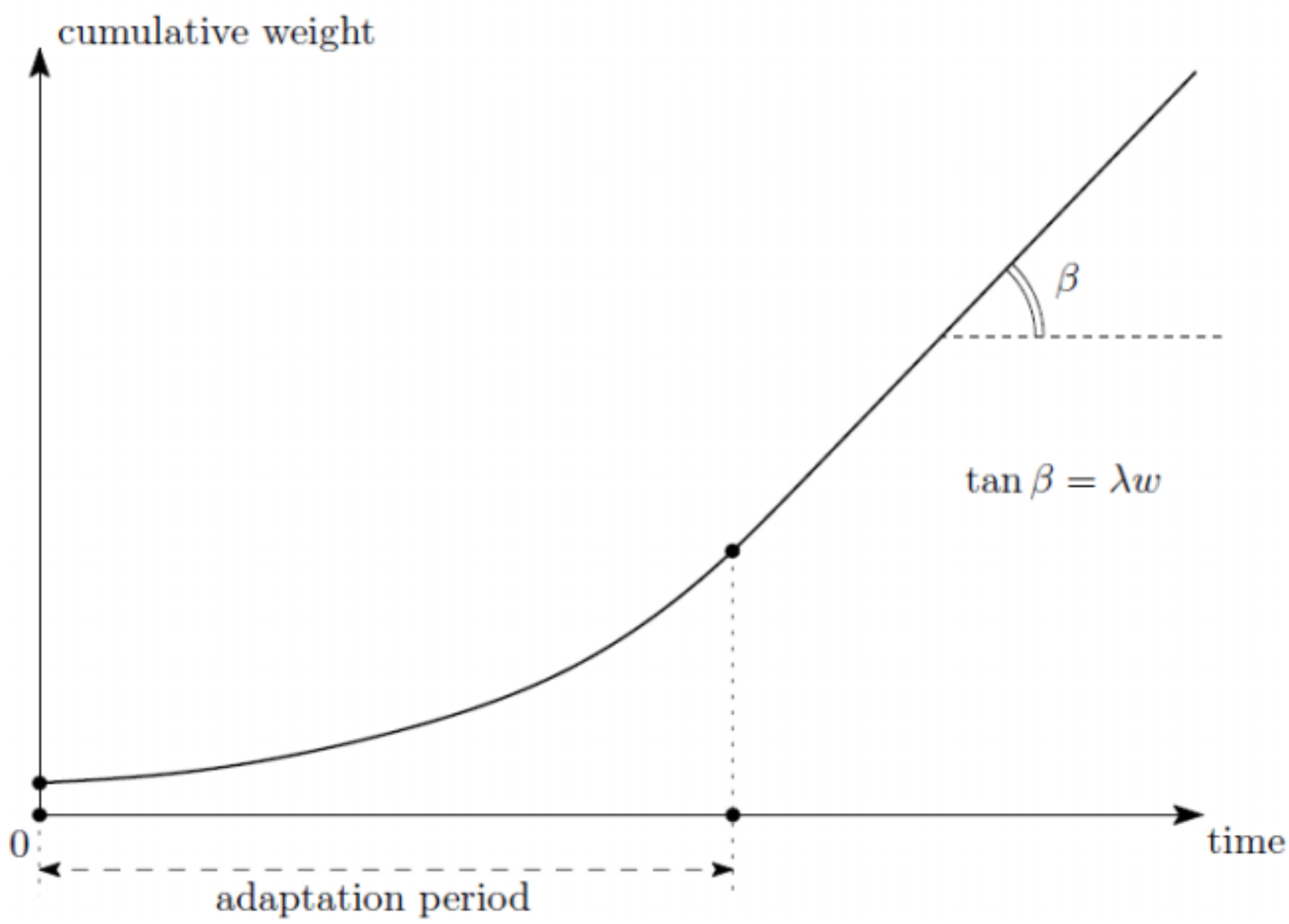

图 4 累积权重的增长