

# 矩阵币：一个通过区块链矩阵构建的高效点对点的电子货币系统

段志朝

mistakenine@gmail.com

摘要：区块链系统中，因为只有一条链所以限制着每秒的交易数量，使得交易效率很低。本文在区块链的基础上提出一个新的数据模型——区块链矩阵，通过多链并行的方式解决交易效率的问题。多链并行并不能简单的使用区块链中的规范，为此，我们通过建立挖矿地址的选区，把每个挖矿地址和处于区块链矩阵中的区块链达成均匀满射对应；将处于区块链中的每个区块链看成一个交易通道，把每一笔发生在系统中的交易与交易通道达成均匀满射对应；重新定义如何识别一个有效的交易、如何选择有效的区块链矩阵这些共识最终形成一个全新的规范标准。在此规范标准下，就能建立高效率交易的点对点电子货币系统。该系统理论上能支撑每秒无上限的交易量。这一规范标准可以被绝大多数现有的共识算法（如 POW, DPOS 等）经过更新后使用，从而达到高效交易的目的。而且在此规范标准下，算力占优发起的攻击，是意义很小的，只有在算力占优且在一段较长的时间内同时控制绝大多数的节点，才能攻击成功，但这意味着绝大多数节点在一个较长的时间内已经认可了新的规则。 文章中 1~5 给出了一个区块链矩阵系统应该遵循的规范标准，第 6 部分给出在遵循区块链矩阵规范标准下，矩阵币系统的基本实现原理。

## 1、区块链矩阵

对于一个 $m \times n$ 的矩阵 $A = \{a_{i,j}\}$ （其中 $1 \leq i \leq n, 1 \leq j \leq m, \{n, m\} \in Z^+$ ），对于任意 $a_{i,j} \in A$ 是一个区块链， $A$ 就是一个区块链矩阵。

对于任意的 $a_{i,j} \in A$ ， $L(a_{i,j})$ 表示区块链 $a_{i,j}$ 的高度。易知， $L(a_{i,j})$ 是属于整数域且随着时间的推移不断地变大的。

对于任意的 $a_{i,j} \in A$ ， $0 \leq k \leq L(a_{i,j})$ ， $k \in Z$ ， $B(i, j, k)$ 表示区块链 $a_{i,j}$ 上高度为 $k$ 的区块。

每条区块链上产生的数字货币是完全相同的数字货币。我们通过构建复杂的跨链交易，保证这一点。

## 2、选区

### 2. 1、挖矿地址

在区块链系统里，所有节点都希望争夺记账权，争夺到记账权意味着挖出一个区块，会有矿工费和 coinbase 奖励，这笔奖励会打到矿工给出的一个地址上，这个地址我们称为挖矿地址。

### 2. 2、选区

在以比特币为代表的区块链系统中，这一地址是和挖矿过程无关联的。即挖到这个区块之后，可以随时弄个账户。在区块链矩阵系统中，地址需要和挖矿关联，也就是说，挖矿对地址是有要求的，换句话说，矿工挖出区块，如果提供的地址不对，其他节点依然不认可这一区块，任何节点是允许拥有任意多个地址的，所以只要矿工提前准备好地址，就不会产生这一尴尬。

区块链矩阵 $A$ 中拥有 $m \times n$ 个区块链，每个区块链都需要在线节点争夺记账权，我们可以看成是所有在线的挖矿地址争夺记账权，我们不能让这一争夺是混乱的，所以我们会把这些地址平均的分配到区块链矩阵 $A$ 上的每一个元素所代表的区块链上。就相当于我们把挖矿地址分成了不同的选区，每个选区对应唯一的一个在 $A$ 中的区块链。

下面，我们使用正规的方式去定义一个选区。记区块链矩阵系统中所有挖矿地址的集合为 $M$ ，记区块链矩阵 $A$ 中所有元素的集合为 $A'$ ，易知 $A'$ 中共有 $m \times n$ 个元素，若存在一个映射 $f: M \rightarrow A'$ ，使得 $f$ 是一个满射，且定义域 $M$ 中的元素通过该满射 $f$ 能够足够均匀的映射到陪域 $A'$ 的元素上，我们称 $f$ 是一个均匀的满射。对于一个均匀的满射 $f$ ，对 $\forall a_{i,j} \in A'$ ，所有满足： $f(addr_{i,j}) = a_{i,j}$ ,  $addr_{i,j} \in M$ 的 $addr_{i,j}$ 的集合 $ADDR$ 称为在 $f$ 下的属于 $a_{i,j}$ 的选区。

针对不同的系统可能会对地址的定义不同，需要不同的均匀的满射来保证选区的生成；如果针对某个系统对地址的定义，能找到一个均匀的满射来保证选区的合理性，那这个方案就是符合区块链矩阵基本规范的。对此 $f$ 我们在 6 中给出了一个例子。

### 2.3、小结

在区块链矩阵系统中，任意两个选区之间的交集为空，所以竞争记账权可以看做是独立进行的。

## 3、交易

### 3.1 交易基础

区块链矩阵系统中交易（记为 $Tx$ ）是在比特币系统中对交易上增加了3.2~3.4的内容。本文的读者先要具体理解比特币交易系统中对交易的各种定义。我们先简单的看一下比特币中对交易的定义，一笔交易是一个含有输入值和输出值的数据结构，该数据结构植入了将一笔资金从初始点（输入值）转移至目标地址（输出值）的代码信息。交易的基本单位也是一个未经使用的交易输出，即 $UTXO$ 。每一笔交易都会有一个交易哈希值作为唯一标识，即 $txid$ 。其中，每个 $UTXO$ 必然对应一个 $Tx$ ，一个 $Tx$ 可能对应多个 $UTXO$ ， $Tx$ 和 $txid$ 是一一对应的。

### 3.2 交易通道

我们把区块链矩阵 $A$ 中的 $a_{i,j}$ 代表的区块链称之为第 $(i,j)$ 个交易通道。易知，区块链矩阵 $A$ 中一共存在 $m \times n$ 个交易通道。

同选区一样，我们必然可以找一个从所有交易的集合到所有交易通道集合的均匀的满射 $f$ 。我们在 6 中给出了一个例子来证明这样的满射是可以被找到的。

当一个交易 $Tx$ 发生时，它都可以通过 $f$ 知道自己应该属于哪个交易通道，全网所有的节点也都知道 $Tx$ 应该属于哪个交易通道，该交易通道对应的选区就会接受这个交易，然后把它打包在这个交易通道区块中。

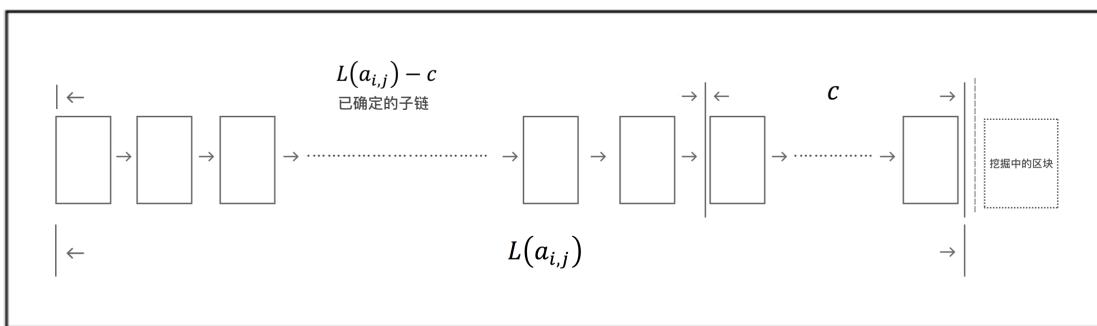
当大量的交易同时发生时，通过 $f$ 可以较为均匀的把这些交易映射到不同的交易通道上，因为每个交易通道上的竞争记账权是独立进行的，所以在不改变原有区块链系统的算法下，使用区块链矩阵模型可以让交易效率提高约 $m \times n$ 倍。

### 3.3、100%已确认的交易

在比特币系统中，如果一个交易被记录在某一个区块 $B$ 中，那么人们都认为，在区块 $B$ 后面再加上 5 个区块即可认为是一个已确认的交易，相当于 6 个区块的确认，而现在普遍的比特币钱包采取的是 3 个区块的确认。而基于 DPOS 的算法下，那么人们认为需要再加上 14 个区块即可认为是一个已确认的交易，即 15 个区块的确认。。

但是，在区块链交易系统中，是没有 100%交易确认的，只能是这个确认概率无限接近于 1，也就是说，依然存在极低概率，在大家认为交易已经被确认的时候，发生攻击事件导致交易完全失败。但是这在工业级的应用领域，是不被允许的。

我们现在给出一个标准，在该标准下，交易是被 100%确认的。在区块链矩阵 $A$ 中，对于任意的 $a_{i,j}$ ，对于给定的共识算法 $P$ （本文中，所有的共识算法 $P$ 都是现有的能在区块链系统中较稳定运行的算法，比如比特币的 POW 和 BTS 的 DPOS），必然存在一个最小的正整数 $c$ ，如果人们普遍认为 $a_{i,j}$ 中高度小于等于 $L(a_{i,j}) - c$ 的所有区块中的交易都是已确认的交易，那么我们判定这些交易都是 100%确认的交易（在下文中，如果我们称一个交易是已确认的交易，如无特殊说明，则认为该交易是 100%确认的交易）。我们把在 $a_{i,j}$ 中从高度从 0 到 $L(a_{i,j}) - c$ 的区块构成的子链称为已确认的子链，记为 $S(a_{i,j})$ ，如下图表示。



显然，在一个区块链矩阵 $A$ 中，所有 $a_{i,j}$ 对应的 $c$ 都是相同的，因为对于给定的 $A$ ，算法 $P$ 是一定的。

### 3.4、交易类型

基于对交易的设定，交易和交易之间是有依赖性的，因为每一个交易的输入都是一系列未经使用的交易输出，即一系列 $UTXO$ 的集合。这样，每一笔交易才能溯源。我们定义：一个交易 $Tx$ 的输入中所有的 $UTXO$ 集合记为 $UT$ ，把 $UT$ 中每个 $UTXO'$ 替换成对应的交易 $Tx'$ ，则获得一个集合记为 $T$ ，则 $T$ 集合中元素的数量必然不大于 $UT$ 中元素的数量，我们称 $T$ 为 $Tx$ 的依赖交易集合，对于 $\forall Tx' \in T$ ，我们称 $Tx$ 依赖于 $Tx'$ ，记为 $Tx \gg Tx'$ 。

#### 3.4.1、同链交易

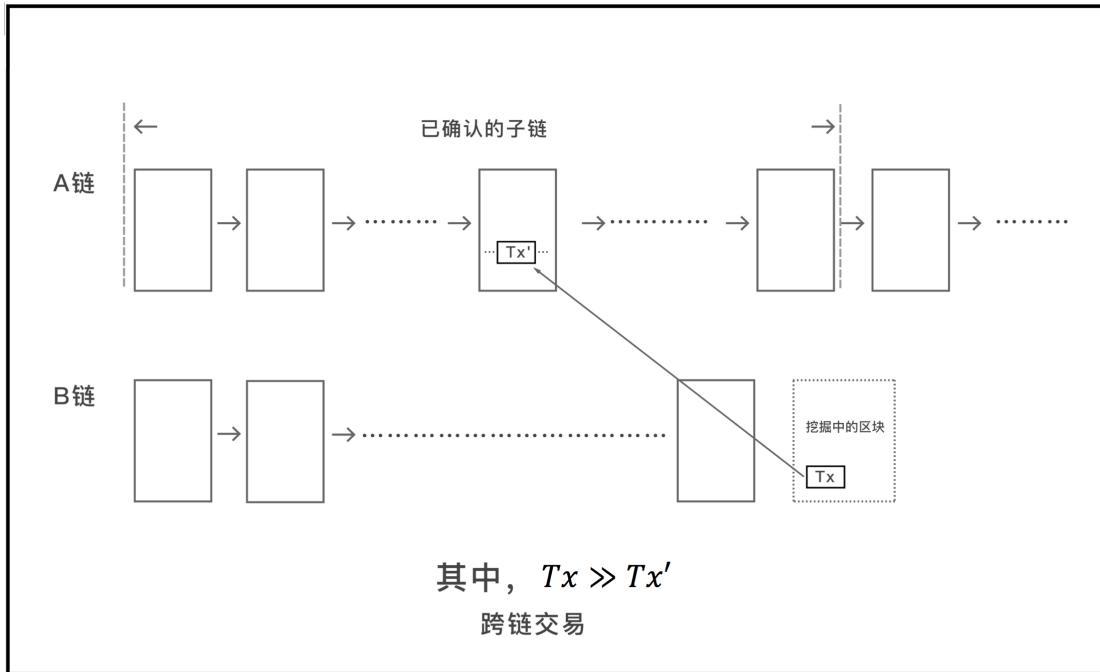
如果对于一个交易 $Tx$ ， $Tx$ 的依赖交易集合 $T$ 中的任意交易 $Tx'$ 对应的交易通道均和 $Tx$ 对应的交易通道相同，则我们认为 $Tx$ 是一个同链交易。

如果一个交易 $Tx$ 是同链交易，我们称 $Tx$ 是一个有效交易。

#### 3.4.2、跨链交易

如果对于一个交易 $Tx$ ， $Tx$ 的依赖交易集合 $T$ 中的存在一个 $Tx'$ 对应的交易通道和 $Tx$ 对应的交易通道不同，则我们认为 $Tx$ 是一个跨链交易。

一个跨链交易 $Tx$ ，如果 $\exists Tx' \in T$ ， $Tx'$ 在区块链矩阵 $A$ 中不是一个已确认的交易，则我们认为这是一个无效的跨链交易。否则，就是一个有效的跨链交易。我们称无效的跨链交易为无效交易，有效的跨链交易为有效交易。下图给出了跨链交易的形象的解释。



## 4、区块标识和子阵

### 4.1、区块标识

在区块链系统中，一个区块头是只拥有父区块哈希值的，换句话说，区块本身是不知道他自己的高度的。我们需要在区块头中插入区块所属的区块链和区块本身的高度，以明确单个区块的位置。

### 4.2、子阵和已确认的子阵

区块链矩阵 $A$ 中的每个区块链 $a_{i,j}$ 中的从高度 $l_1$ 到高度 $l_2$ 的子链可以用 $subchain(l_1, l_2)_{i,j}$ 来表示，其中 $\{l_1, l_2\} \in Z^*, l_1 < l_2$ ，如果 $l_1 = 0$ ，我们称该子链是一个源子链。

对于一个 $m \times n$ 区块链矩阵 $A = \{a_{i,j}\}$ ，如果存在一个 $m \times n$ 的区块链矩阵 $G = \{b_{i,j}\}$ ，如果 $\forall i, j, 1 \leq i \leq m, 1 \leq j \leq n, b_{i,j}$ 均为 $a_{i,j}$ 的一个源子链，我们称 $G$ 为 $A$ 的子阵。如果 $G$ 中的每一笔交易在 $A$ 中都是 100% 已确认的交易，那么称 $G$ 为 $A$ 的已确认的子阵。

$G_1, G_2$  是区块链  $A$  的两个子阵，如果  $\forall b_{i,j} \in G_1, b'_{i,j} \in G_2, L(b_{i,j}) \leq L(b'_{i,j})$ ，则我们认为  $G_2$  比  $G_1$  大。对于  $A$  的一个子阵  $G$ ，如果不存在另外一个子阵比  $G$  大，则称  $G$  为  $A$  的最大子阵。明显的， $A$  的最大子阵就是它自己。

令  $G$  是  $A$  的已确认的子阵，如果不存在另外一个已确认的子阵比  $G$  大，则称  $G$  为  $A$  的最大已确认的子阵。

## 5、区块链矩阵的共识

基于本文 1~4，我们可以给出一个区块链矩阵的共识规则。区块链矩阵的去中心化共识由所有网络节点的 4 种独立过程相互作用而产生：

- (1)、每个全节点能独立的验证每个交易的合法性；
- (2)、挖矿节点能够独自创造出新的区块；
- (3)、每个节点能够独立的检验新的区块并把它接入到已有的区块链矩阵中；
- (4)、每个节点能够独立的判断并选择最新的合法的区块链矩阵。

### 5.1、交易的独立校验

每个节点产生的交易随后将被发送到区块链矩阵网络临近的节点，从而使得该交易能够在整个区块链矩阵网络中传播。

然而，在交易传递到临近的节点前，每一个收到交易的区块链矩阵节点将会首先验证该交易，这将确保只有有效的交易才会在网络中传播，而无效的交易将会在第一个节点处被废弃。

对于一个区块链矩阵中的采用的共识算法  $P$ ，它必然是能对交易做独立校验的。在算法  $P$  的校验基础上，交易必须遵守由区块链矩阵规定的一条

规则：每个交易必须是有效交易，即每个交易要么是同链交易，要么是有效的跨链交易。

如果一个节点设定了挖矿地址，那么他就会把该挖矿地址所在选区对应的交易通道上的交易按照某种合理的顺序收集到一个池子里，每一个不同的交易通道对应一个不同的池子。

## 5.2 构建新区块

对于一个区块链矩阵中采用的共识算法 $P$ ，他必然能够在单个区块链上独立的构建新区块。因为每个挖矿地址对应一个选区，所以可以认为挖矿是互相没有交集的挖矿地址在竞争，每个选区上根据算法 $P$ 确定该选区对应的区块链 $a_{i,j}$ 的记账权，生成这个区块的时候，胜出矿工节点会把他在该交易通道获取的交易和挖矿地址打包进区块。

构建区块之后，节点会把区块发给它所有的相邻节点。这些节点在验证该区块之后，也会继续传播此区块。

每个交易通道的区块创建，如果抛去区块里面的交易来讲，是完全独立的，完全取决于算法 $P$ 的。

## 5.3、校验新区块

当一个节点收到一个新区块时，会根据新区块的标识寻找到该区块对应的区块链 $a_{i,j}$ ，然后来验证新区块是否正确，若通过验证，则 $a_{i,j}$ 会拼接该区块，反之，则会拒绝该区块。

在校验中，需要验证如下几点：

- 新的区块加入对应的区块链时需要符合区块链矩阵所采取的共识算法 $P$ 的标准

- 该区块被挖出的挖矿地址，是否属于正确的选区，如果选区不对，则不被承认。
- 节点中在没有接受新的区块时的区块链矩阵为 $A$ ，要求新区块中所有交易是符合本文第3章定义的有效交易，即要么是同链交易，要么是有效的跨链交易。
- 如果上一条件不成立，则该区块将会被放在孤立块池子中，直到上一条件达成，或者被清理出孤立块池子。

- 如果新接收的区块和异于该区块所在链上的区块发生均依赖同一个交易的情况时（即异链“双花”），取已发生分歧的区块上生成区块更多的那条链为准，废弃另外一条链上分歧区块及之上的所有区块。

最后一条保证了不会出现异链“双花”问题。

在获取过程中，因为是并行的链，所以我们需要证明如下问题：即在现有区块链矩阵 $A$ 的状态下，不存在两个新区块 $B(i, j, k)$ 和 $B(p, q, t)$ ，使得 $B(i, j, k)$ 加入 $A$ 是依赖于 $B(p, q, t)$ 先加入 $A$ 中，而 $B(p, q, t)$ 加入 $A$ 是依赖于 $B(i, j, k)$ 先加入 $A$ 中的，即出现死锁。

假设上述问题出现，则在区块链矩阵 $A$ 中， $B(i, j, k)$ 对应的区块链 $a_{i,j}$ 和 $B(p, q, t)$ 所对应的区块链 $a_{p,q}$ 必然是两条不同的链，否则易知不会出现上述问题。则在 $a_{p,q}$ 必然存在一个区块 $B(p, q, t')$ ,  $t' < t$ ,  $B(p, q, t')$ 不是 $a_{p,q}$ 已确认的子链 $S(a_{p,q})$ 中的区块，而当 $B(p, q, t)$ 加入 $A$ 中后， $B(p, q, t')$ 就变成是 $S(a_{p,q})$ 中的区块，并且使得存在：一个交易 $Tx'_1$ 是记录在 $B(p, q, t')$ 内的，一个交易 $Tx$ 是记录在 $B(i, j, k)$ 内的，且 $Tx \gg Tx'_1$ 。

如果这两个块都是诚实节点给出的块，那么必然在网络中存在一个节

点 $M_1$ ，在 $M_1$ 上， $B(i,j,k)$ 还没生成的情况下， $B(p,q,t)$ 已经生成了。而根据假设， $B(p,q,t)$ 加入 $A$ 是依赖于 $B(i,j,k)$ 先加入 $A$ 中的。这明显矛盾。

所以不会存在锁死的问题，同理可证，不会出现环状死锁（即区块 $B_1$ 依赖 $B_2$ ， $B_2$ 依赖 $B_3$ ， $B_3$ 依赖 $B_1$ ）的问题。

#### 5.4、区块链矩阵的选择

对于一个新加入的网络节点，最开始只有 $m \times n$ 个区块，即每个区块链上只有一个区块。

在区块链矩阵中，本地节点会依顺序依次获取 $m \times n$ 个区块链，获取的过程中将遵循以下原则：

- 每个节点本地拥有一个最大已确认的子阵 $F$ ，对于新节点，最大已确认的子阵是每个区块链高度为 0 的区块链矩阵。
- 区块链矩阵 $A = \{a_{i,j}\}$ 中每个节点 $(i,j)$ 都会根据共识算法 $P$ 选择一条满足下个条件的最长的链。
  - 被选中的最长的链如果替换掉原有的区块链 $a_{i,j}$ ，检查新生成区块链矩阵的最大已确认的子阵 $F'$ ，要求 $F$ 必须是 $F'$ 的一个子阵，否则就不接受这个链。

#### 5.5、证明与分析

在区块链矩阵中，单个区块链分叉的问题由共识算法 $P$ 得到保障。下面给出一个论断：

给定一个区块链系统中的共识算法 $P$ ，如果 $P$ 是有效的，那么该系统变化为区块链矩阵系统之后，不可能产生最大已确认的子阵分叉。说 $P$ 是有效的，是指在算法 $P$ 下一个交易成交之后达成被公认是可确认的状态的条

件下，该交易永远有效。

事实上，若在算法 $P$ 下一个被公认的交易被攻击成功，那么去中心化的数字货币系统就是不可用的。

我们假定以上结论错误，则必然至少存在两个不同的最大已确认的子阵的分叉。即，存在一个区块链矩阵上的某个区块链中，至少存在两个处于同一高度的块，该块中的每一笔交易都是被确认的，且至少有一笔交易在两个块中是不同的。也就是说存在一笔交易，在算法 $P$ 下被攻击成功。这是矛盾的。

事实上，显而易见的，只要区块链矩阵系统正常的运行一段时间，每个诚实节点的链会因为“拥有自己的判断意识”，从而让攻击者很难短时间达到目的——即让其他的诚实节点接受他的链，攻击者唯一能做的就是既算力占优，又在一个较长的时间段内是节点占优的，这个攻击比算力占优的攻击难的多。而这种攻击一旦成功，其实变相等同于绝大多数节点认可了被攻击节点。

本文中给出同链交易的目的，是在于满足小额极速转账的需求，可以理解为同链交易是不需要确认即可转账的，跨链交易需要等到其他人确认，这意味着，如果用户使用的钱包够智能，完全可以实现到账之后立刻转出，这在小额频繁交易中很有用。

## 6、矩阵币系统概述

我们简单的给出一个例子，证明2.2和3.2中的满射是可以被找到的，当然，这个满射可能不够均匀，但是对于系统来说，足够使用。我们会在

另外的文章单独对满射的选取做出探讨，因为这并不是本文的主要内容。

在本例中，我们直接使用比特币系统中对交易的 $txid$ 的生成办法和矿工地址的生成办法。

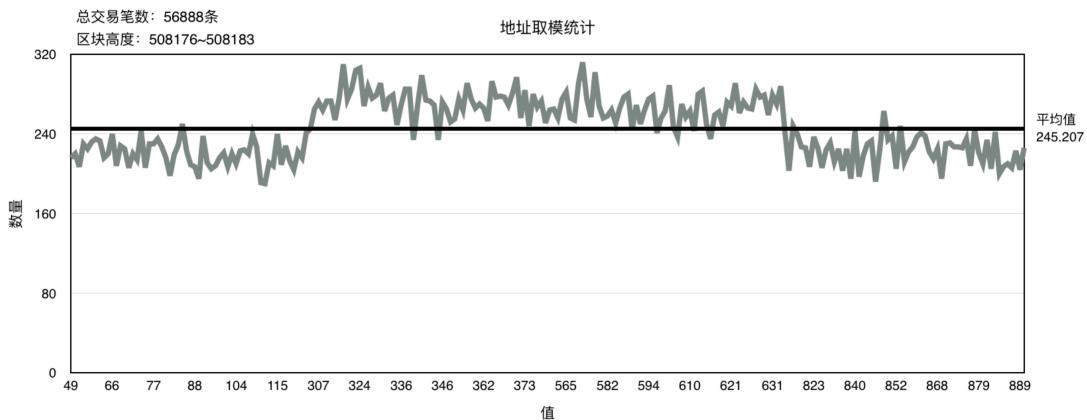
我们选取 $m=1024$ ,  $n=1$  这一区块链矩阵。

### 6. 1、矿工地址到选区的满射

下面，我们给出一个从矿工地址到选区的较为均匀的满射 $f$ 。

对于任何一个矿工地址  $addr$ ，把该地址转换为 ASCII 码，再把该二进制换算成十进制，然后对 $m \times n$ 取模。易知，该 $f$ 是一个满射。在本例中，使用的是在比特币系统中矿工地址的生成方式。

本文的作者顺序的抽取了从高度为 508176 到 508183 的 8 个区块中共计 56888 个已经发生在比特币中的出现的矿工地址，然后根据 $f$ 算出了如下的分布结果：



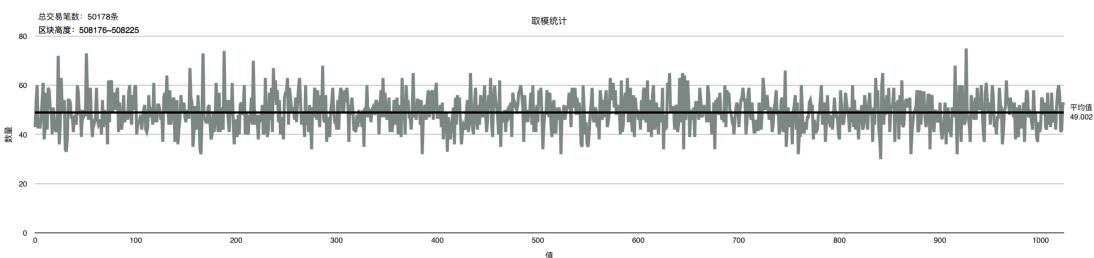
### 6. 2、交易到交易通道的满射

下面，我们给出一个从交易到交易通道的较为均匀的满射 $f$ 。

定义一个从所有交易的集合到所有交易通道的集合的映射 $f$ ，对于任何一个交易 $Tx$ ，把该交易对应的唯一的 $txid$ 换算成十进制，然后对 $m \times n$ 取模。易知，该 $f$ 是一个满射。在本例中，使用的是在比特币系统中 $txid$ 的

生成方式。

本文的作者顺序的抽取了从高度为 508176 到 508225 的 50 个区块中共计 50178 个已经发生在比特币中的交易对应的  $txid$ , 然后根据  $f$  算出了如下的分布结果:



### 6.3、激励探究

现在的区块链系统中都很凸显产生的数字货币总数不变，这是违背经济学原理的，在实际生活中，货币总数不变，必然会导致经济萎缩。对已有货币总数保证一定膨胀系数，是有利于促进经济发展的，每一笔交易中，矿工费从本质上来说是必不可少的，否则就不会有足够多的人参与到竞争记账的活动中来。每个区块被挖出时，第一笔获得的资金应该取决于一个现有总货币量的经济模型决定。

## 参考文献:

- [1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, <https://bitcoin.org/bitcoin.pdf>, 2008.
- [2] Andreas M Antonopoulos, Mastering Bitcoin, <https://github.com/bitcoinbook/bitcoinbook/blob/develop/book.asciidoc>, 2017.
- [3] dantheman, DPOS Consensus Algorithm – The Missing White Paper, <https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper>, 2017.
- [4] delegated-proof-of-stake-consensus, <https://bitshares.org/technology/delegated-proof-of-stake-consensus/>.
- [5] vitalik buterin, A Next-Generation Smart Contract and Decentralized Application Platform, <https://github.com/ethereum/wiki/wiki/White-Paper>, 2013.
- [6] Vlad Zamfir, introducing-casper-friendly-ghost, <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/>, 2015.