AR 介绍

AR 是衡量区块链账户价值的方式。

账户价值（AR）的具体算法分两部分：

基于账户资产中值的价值衡量指标 α

资产中值的定义为在一定时期内账户所持有的资产的中位数，即资产中值为 x 的账户意味着该账户至少持有 x 资产超过一半的时间，防止同样一笔资产被多个账户利用，保证了账户的基本价值。

随后计算具体资产中值指标时对资产中值使用了我们独创的 Wilbur 函数 f：

$$f(x) = \frac{x}{1 + (a/x)^b}$$

其中输入为 x 为一段时间内的资产中值，输出 $f(x)$ 为资产中值指标，即 $f(x) = \alpha$。可以证明，Wilbur 函数满足

(a) $f(x + y) > f(x) + f(y)$，严格地抵抗了女巫攻击，

(b) $\lim_{x,y\to\infty} f(x + y) = f(x) + f(y)$，防止大户的绝对统治。

举例：假设一个用户的资产为 100，如果所有 100 资产都存在于一个账户里，则该账户的资产中值指标为 $f(100)$。假设该用户将 100 资产分开存在两个不同的账户里，每个账户存 50，则两个账户的资产中值之和为 $2f(50)$，根据性质 a 可知 $f(100) > 2f(50)$，说明用户建立新账户并拆分资产不会获得收益，防止了女巫攻击。

性质 b 保证了当大户资产足够多时，其账户总价值不会超过多个总资产相同的散户的总价值太多。

基于账户出入度的价值衡量指标 β

(a) 首先根据账户一定时期内的转账交易记录构建转账交易有向图，每条边的方向代表代币流转方向，权重代表对应代币流转的数量，每条边的时间戳对应该交易发生的时间。

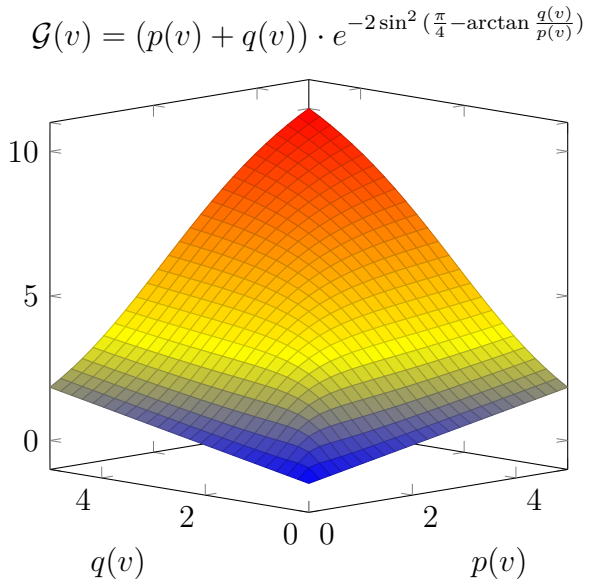

Figure 1: 出入度计算函数曲线

(b) 对转账交易图进行去环操作，所谓一个环指的是，图中存在一个有向环，从环上某个点出发绕环一周所经过的所有边的时间戳都是递增的。所有简单的循环转账必定会产生这样的一个环。对于此类环，我们将环上所有的边的权值均减去该环中权值最小边的权值。此操作保证环上权值最小边被删除（权值变为 0），实现去环目的。

(c) 针对去环算法后剩下的交易图，记录账户的出入度 x, y, 通过下面公式计算出入度指标：

$$G(x, y) = (x + y)e^{-2\sin^2(\frac{\pi}{4} - \arctan\frac{x}{y})}$$

其中

- x, y 分别为账户的入度和出度。
- $G(x, y)$ 为账户的出入度指标。
- 可以证明，固定 $x + y$, 当 $x = y$ 时，$G(x, y)$ 最大。当 x 或 y 有一个为 0 时，$G(x, y)$ 最小，两者差距为 e 倍。

(d) 对 $G(x, y)$ 计算 Wilbur 函数作为出入度最终结果 β。

AR 的计算

账户的价值 AR 定义为资产中值指标乘以出入度最终结果，即 $\alpha\beta$。