

区块链模拟器 1.0 使用手册

特别注意：由于还未提交申请，某些杀毒软件可能会将.exe 文件自动删除，请手动添加到信任。

名称：区块链模拟器

版本：1.0

作者：裴尧尧 博士

邮箱：yaoyao.bae@foxmail.com

QQ 交流群：742346441

版权：湖北工业大学

目的：区块链基础知识科普与教学

如有任何疑问，请与作者联系。发现 bug，请及时反馈作者，感激不尽。

基本规则。目前模拟器初始节点 12 个，最多可增加至 16 个。全部为诚实节点，后期会加入恶意节点功能。货币最小单位为分，创世区块给每个节点 1000 元创世币，单笔交易费为 10 分，挖矿奖励为 500 分。采用和比特币一样的共识机制 pos。获胜的矿工获得挖矿奖励和交易费。

原理。除了没有搭建真正的 P2P 网络，其他技术均或多或少来自比特币，广度上都包含，深度可能不够，后期会继续更新。

哈希算法：sha256d(双哈希)

不对称加密：P2PKH，后期会增加新算法。

钱包：普通钱包。不包含 HD 钱包，可能后期加入。

共识机制：POS，和比特币一样。后期会尝试一些新的共识机制。

节点类型：目前只有全节点，后期加入轻节点，目前全为诚实节点，后期会让节点干坏事。

智能合约：无，后期制作模拟商城加入。

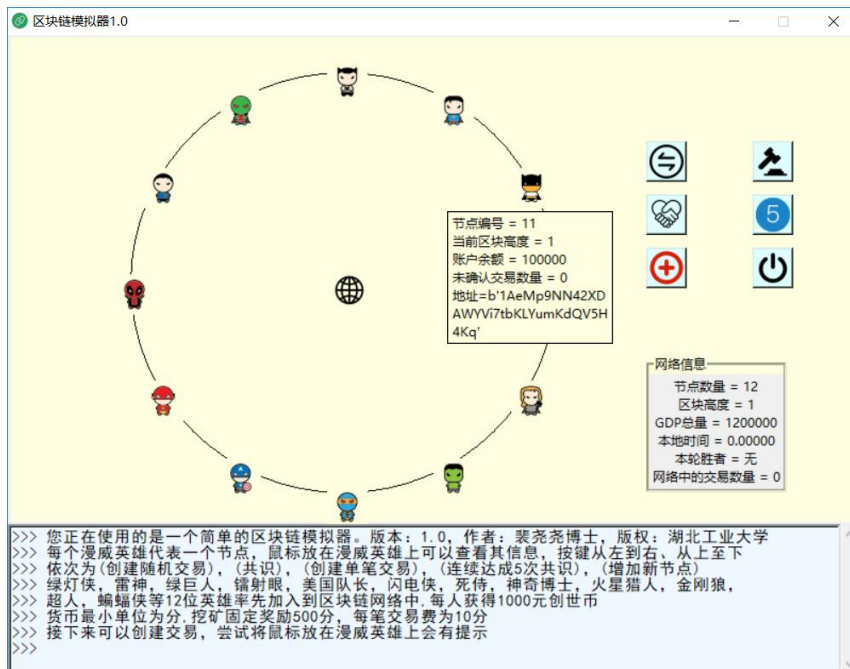
如果你想了解模拟器的细节，可以加群或者和作者进行交流，知无不言，言无不尽。8-9 月会将源码发布到 github，请大家多指导。

使用步骤：

1、运行程序。

双击.exe 文件打开。会率先生成 12 个节点，每个节点为一个漫威英雄，**圆形**表示他们是对等节点。鼠标放在英雄图标上可以查看节点信息。

虽然程序采用了多线程，每个按钮事件是相互独立的，但为了防止 bug，作者锁死了同时随机交易、挖矿和 5 次共识按钮的事件，**也就是三者中同时只能同时进行其中一件**。这并不影响做该程序的教学目的。



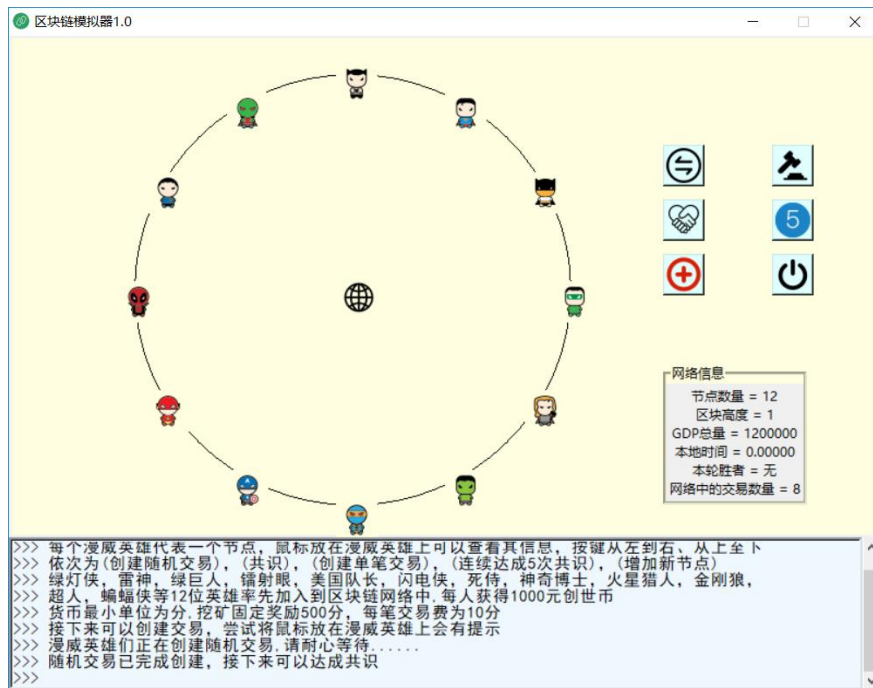
当交易发出后，在达成共识前，交易双方虽然余额显示无误的，但会显示有未确认交易。

2、按键介绍。

右边的6个按钮依次为--网络中随机创建交易--达成共识(挖矿)--创建单次交易--达成5次共识--添加新节点--退出程序。

3、创建随机交易。

点击右边第一排第一个按钮，网络中的节点会随机创建交易。就目前而言，网络中的所有节点都是诚实节点，后期后允许节点干坏事。

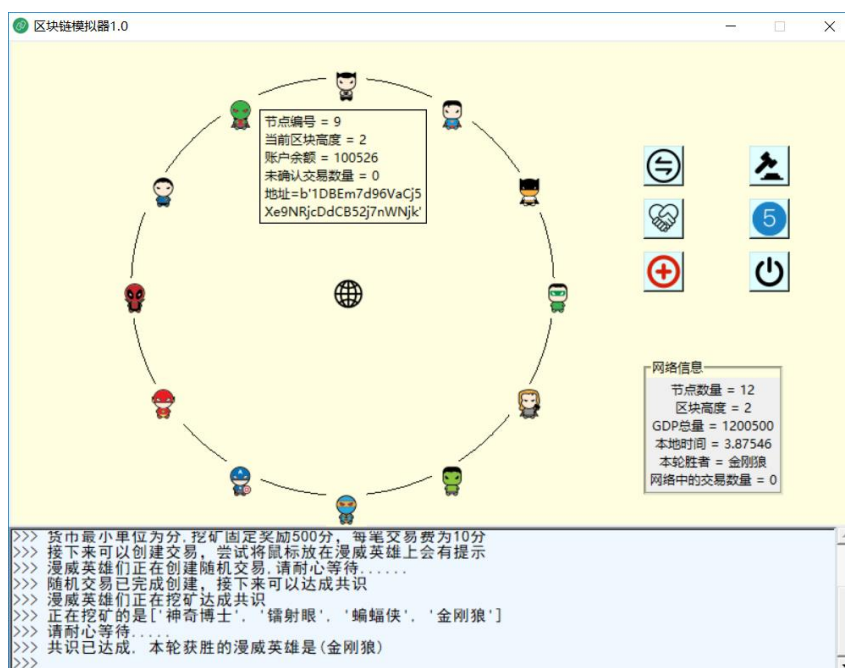
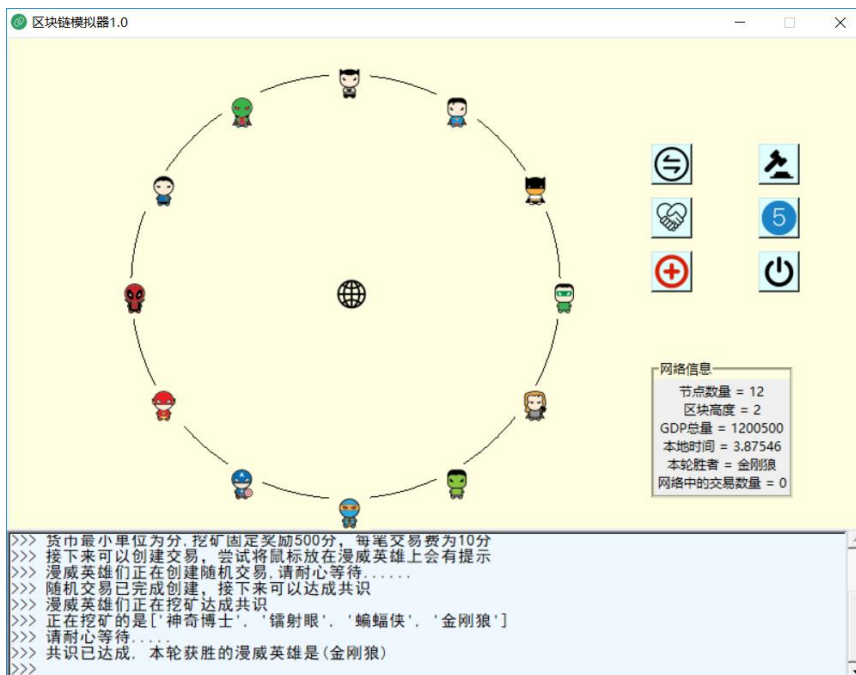


当前随机交易数量为 8，接下来可以达成共识。

4、达成共识。

第一排第二个按钮是共识按钮。与比特币一样，采用的是 pow。

本地时间是挖矿时间。



本次获胜的是金刚狼，获得 500 的奖励，但是他的余额是 100526 表示加上 110 的交易费，还有人给他转账 126。

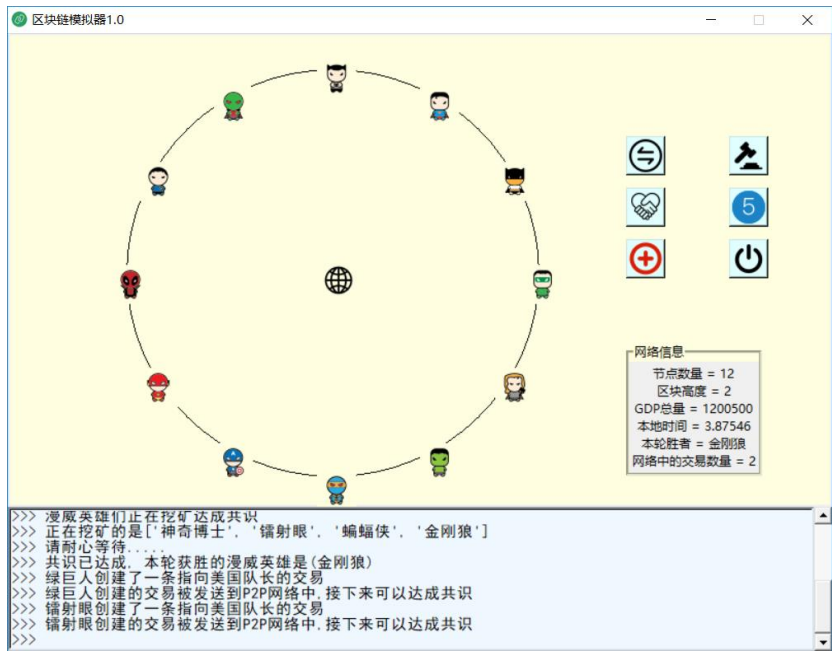
5、创建单次交易。

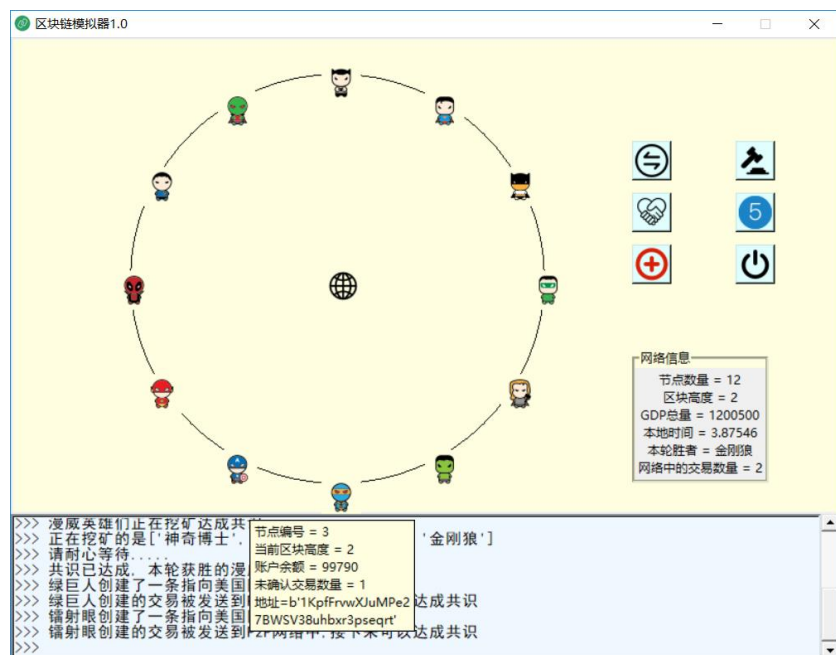
点击第二排第一个按钮可以指定英雄之间相互交易。软件设置交

易最小金额为 5，最大金额为 1000。超过 1000 安 1000 算。

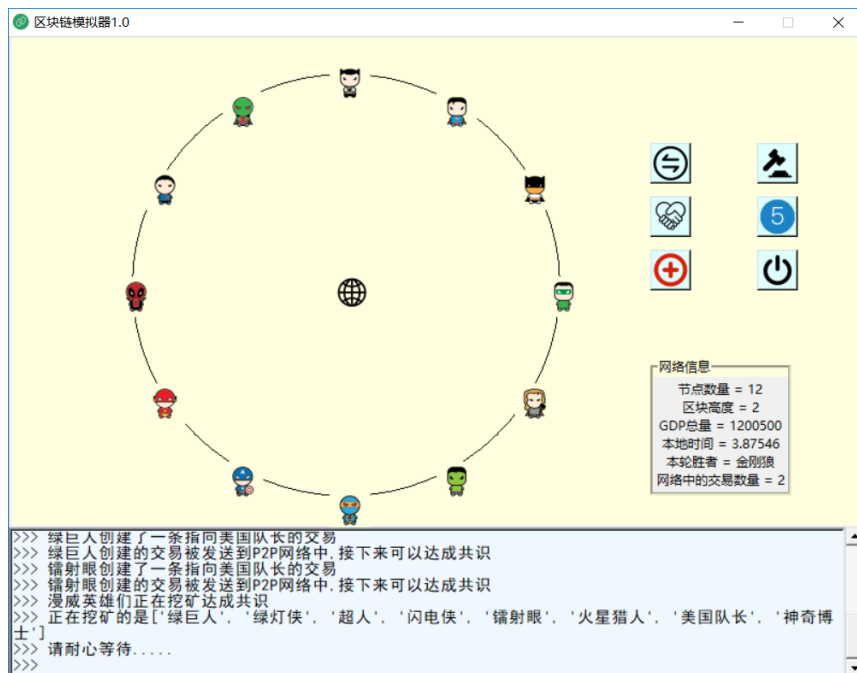


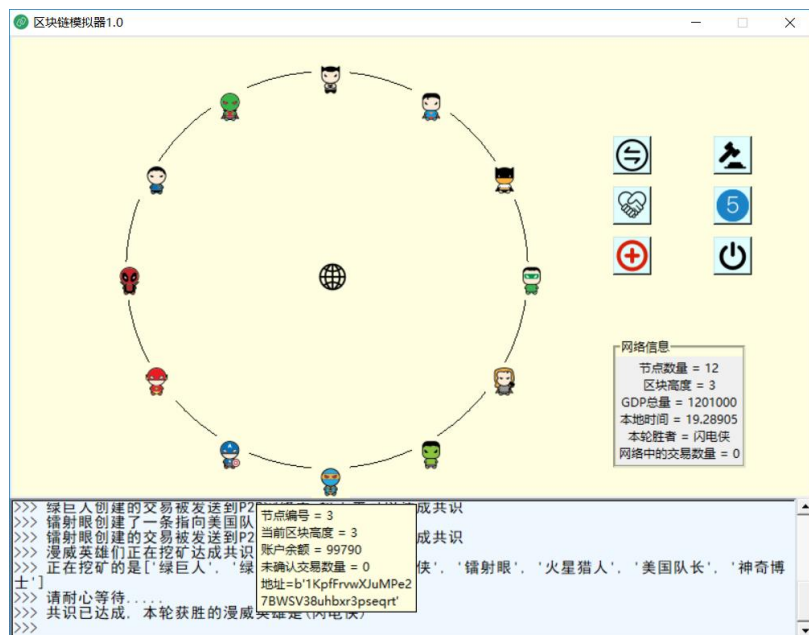
比如让镭射眼给美国队长 200，确认后。





镭射眼和美国队长都有未确认交易，我们可以通过挖矿确认交易。





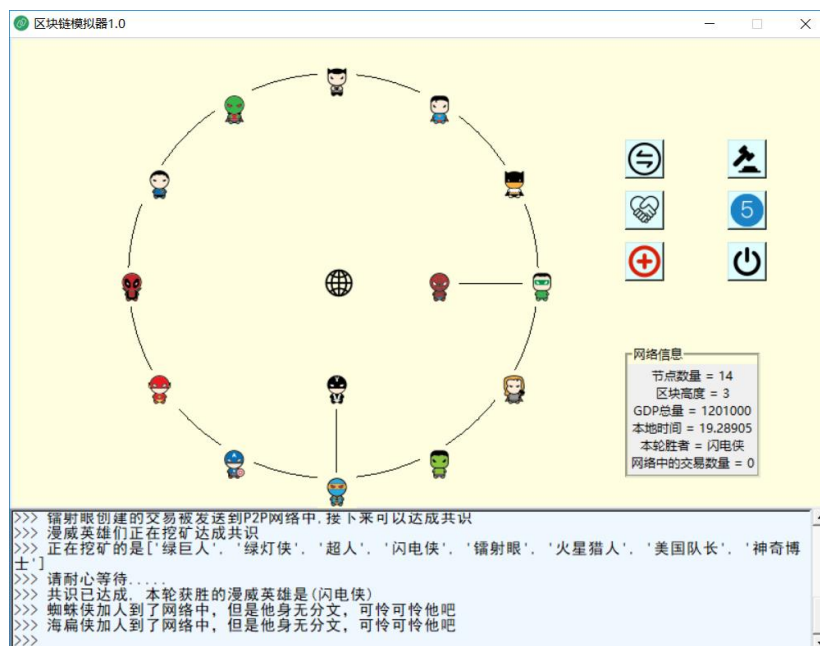
挖矿完成后，大家都不再有未确认交易。

6 连续 5 次共识。

第二排第二个按钮连续执行 5 次随机创建交易并达成 5 次共识。

7、添加新节点。

第三排第一个节点将会增加新节点，但是节点没有余额。



8、后记。

笔者并没有读比特币源码，也没有适用过目前市场上流行的各种区块连开发工具，在读完《精通比特币》一书的基础上，花费了2个月左右高强度工作（常常 16+小时/天，算上自身工作时间在内，特别是整个时间段类单位的大事件，让我无法完全投入其中）完成源代码部分，花费4天做GUI（所以比较简陋，望谅解），所以可能会存在错误之处，望您不吝赐教，随时指出。