数据区块结构

hexdump程序把数据区块文件转化为十六进制+ASCII表示，每一个数据区块记录了六个内容：神奇数、区块大小、数据区块头部信息、交易计数、交易详情。在这当中，数据区块头部信息的HASH值是下一个新区块的HASH值的参考目标数，最后一项交易详情记录了该区块中所有的交易记录（编者会在以后详细说明交易记录的结构）。

数据区块结构如下图：



交易记录结构

数据区块的交易记录中，详细记载了比特币的交易记录和相关细节。其中在比特币收支详情里面，记录了收支的比特币地址和merkle节点值等情况，因此收支详情是交易记录中最重要的部分。

完整的交易记录结构如下表格：



比特币支出和接收交易的结构

在数据块中，比特币支出和接收交易是写在一起的，整个收支记录包括很多比记录。每一比记录都有自己的索引编号以供查询。

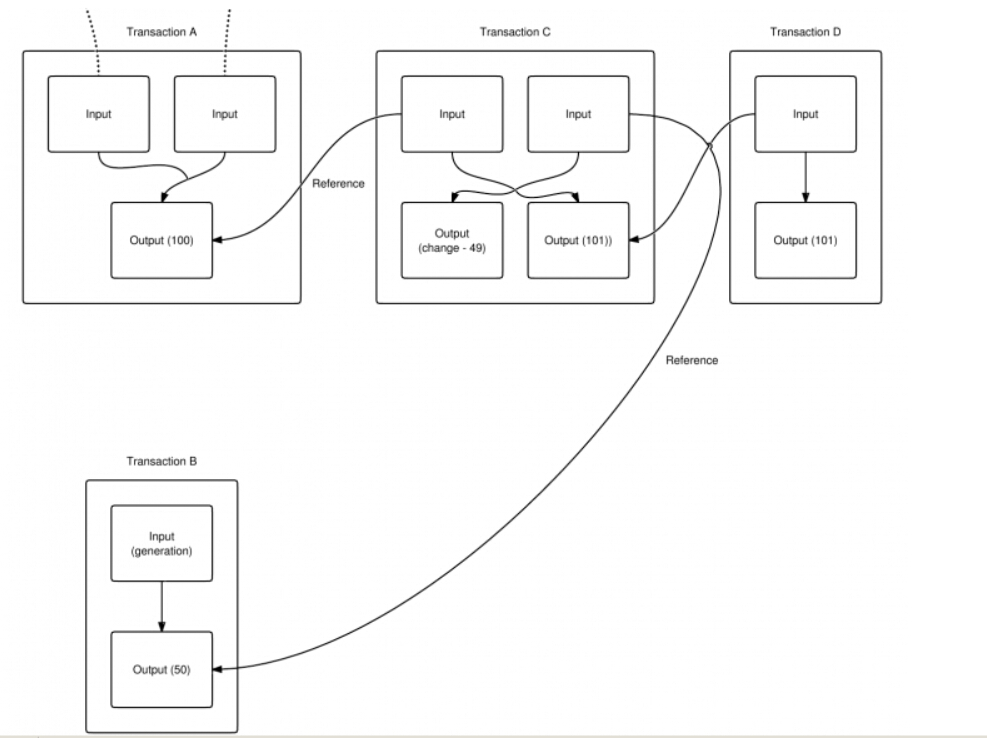


每一比记录中包括了生成时间、引用交易的哈希值、交易记录索引编号、比特币支出地址、支出地址数量等细节。每一比收支交易记录都有一个Merkle节点值，这个hash节点值是整个Merkle树的一部分，决定了每一个地址都不能重复交易和被伪造。

收支交易结构图如下：



因为每解决一个区块，都会得到新产生的比特币奖励，每个区块包含一个记录，记录中的比特币地址是有权获得比特币奖励的地址。这个纪录被称为生产交易、或者coinbase交易，它经常是每个区块的第一个交易。



A sends 100 BTC to C and C generates 50 BTC. C sends 101 BTC to D, and he needs to send himself some change. D sends the 101 BTC to someone else, but they haven't redeemed it yet. Only D's output and C's change are capable of being spent in the current state.



创世块的原始十六进制如下所示：

00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 …………….

00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 …………….

00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ….;£íýz{.²zÇ,>

00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A9F B8 AA gv.a.È.ÃˆŠQ2:Ÿ¸ª

00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)«\_Iÿÿ…¬+|

00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 …………….

00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 …………….

00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D ……ÿÿÿÿM.ÿÿ..

00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/

00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel

000000A0 6C6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of

000000B0 73 65 63 6F 6E 64 20 62 61 69 6C6F 75 74 20 66 second bailout f

000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksÿÿÿÿ..ò.

000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 \*….CA.gŠý°þUH’

000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gñ¦q0·.\Ö¨(à9.¦

000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F4C EF 38 C4 ybàê.aÞ¶Iö¼?Lï8Ä

00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 óU.å.Á.Þ\8M÷º..W

00000110 8A4C 70 2B 6B F1 1D 5F AC 00 00 00 00 ŠLp+kñ.\_¬….

f9beb4d9—神奇数

1d010000—区块大小 293 – 285=8

01000000 – 版本号

0000000000000000000000000000000000000000000000000000000000000000 -prev block

3BA3EDFD7A7B12B27AC72C3E67768F617FC81BC3888A51323A9FB8AA4B1E5E4A – merkle root

29AB5F49 – 时间戳

FFFF001D – 目标HASH值

1DAC2B7C – 随机数

01 – 交易个数

01000000 – 版本

01 – 输入

0000000000000000000000000000000000000000000000000000000000000000—previous outpoint txid

FFFFFFFF – previous outpoint index

4D – 脚本长度 bytes in coinbase

04 – bytes in height

FFFF001D--height

0104455468652054696D65732030332F4A616E2F32303039204368616E63656C6C6F72206F6E206272696E6B206F66207365636F6E64206261696C6F757420666F722062616E6B73 – scriptsig脚本 --arbitrary data任意数据

FFFFFFFF – 序列号 -sequence

01 – 输出

00F2052A01000000 – 50 BTC的收益

43 – 脚本scriptPubKey的长度

4104678AFDB0FE5548271967F1A67130B7105CD6A828E03909A67962E0EA1F61DEB649F6BC3F4CEF38C4F35504E51EC112DE5C384DF7BA0B8D578A4C702B6BF11D5FAC – 脚本scriptPubKey

00000000 –锁定时间

f9be b4d9—神奇数 -----------------4 bytes

d7000000—区块大小------------------4

//块头---------------80

01000000—版本号------------------------4

6fe28c0ab6f1b372c1a6a246ae63f74f931e8365e15a089c68d6190000000000—previous block----------------------------32

982051fd1e4ba744bbbe680e1fee14677ba1a3c3540bf7b1cdb606e857233e0e --merkle root---------------------------------32

61bc6649—时间戳-------------------4

ffff001d—目标HASH值---------------4

01e36299—随机数----------------------4

//交易

01--交易个数-----------------------------------1

01000000—版本------------------------------4

01—输入--------------------------------------1

0000000000000000000000000000000000000000000000000000000000000000—previous outpoint txid------------------------------32

FFFFFFFF – previous outpoint index-------------------------4

07—脚本长度 bytes in coinbase------------------------1

04-- bytes in height----------------------------------------------1

ffff001d---height

0104-- scriptsig脚本 --arbitrary data任意数据

FFFFFFFF – 序列号 -sequence------------------4

01—输出---------------------------------1

00F2052A01000000 – 50 BTC的收益-------------------------8

43 – 脚本scriptPubKey的长度-----------------------------------1

410496b538e853519c726a2c91e61ec11600ae1390813a627c66fb8be7947be63c52da7589379515d4e0a604f8141781e62294721166bf621e73a82cbf2342c858eeac– 脚本scriptPubKey---------------------------------43->67

00000000—锁定时间---------------4.

==========================================================================

**交易费：由多个地址输出时，通常需要付交易费；**

**创建区块的矿工可以自由支配所获得的奖励和交易费**

**IP地址：矿工的IP地址**

**播报方：发掘出区块的矿工**

**首次播报IP：同一个播报方发掘的区块首次播报IP地址不同**

**播报方IP地址：此IP仅表示blockchain.info首次收到此交易信息的节点地址，并不意味着此地址就是交易的实际来源。**

**估计交易量：每笔交易估计的实际的交易量（付给别人的）**





一对一；多对一；（其中有一个出现输出地址）；

**洗币：**

Shared Coin provides privacy for your transactions by combining your transaction with other people's.

Shared Coin is a method of making transactions which requires less trust in the service. Shared Coin is based on the CoinJoin concept which acts as a meeting point for multiple people to join together in a single transaction. Having multiple people in a transaction improves privacy by making transactions more difficult to analyse.

TRUSTLESS.

FREE.

FAST. 30 SECONDS.

How does it work?

Shared Coin is a method of making transactions which requires less trust in the service. Shared Coin is based on the CoinJoin concept which acts as a meeting point for multiple people to join together in a single transaction. Having multiple people in a transaction improves privacy by making transactions more difficult to analyse. The important distinction between traditional mixing services is the server cannot confiscate or steal your coins.

镕币付款是交易的一种需要更少信任的手段。

多人参与单笔交易，更难分析，因而提高隐私性。

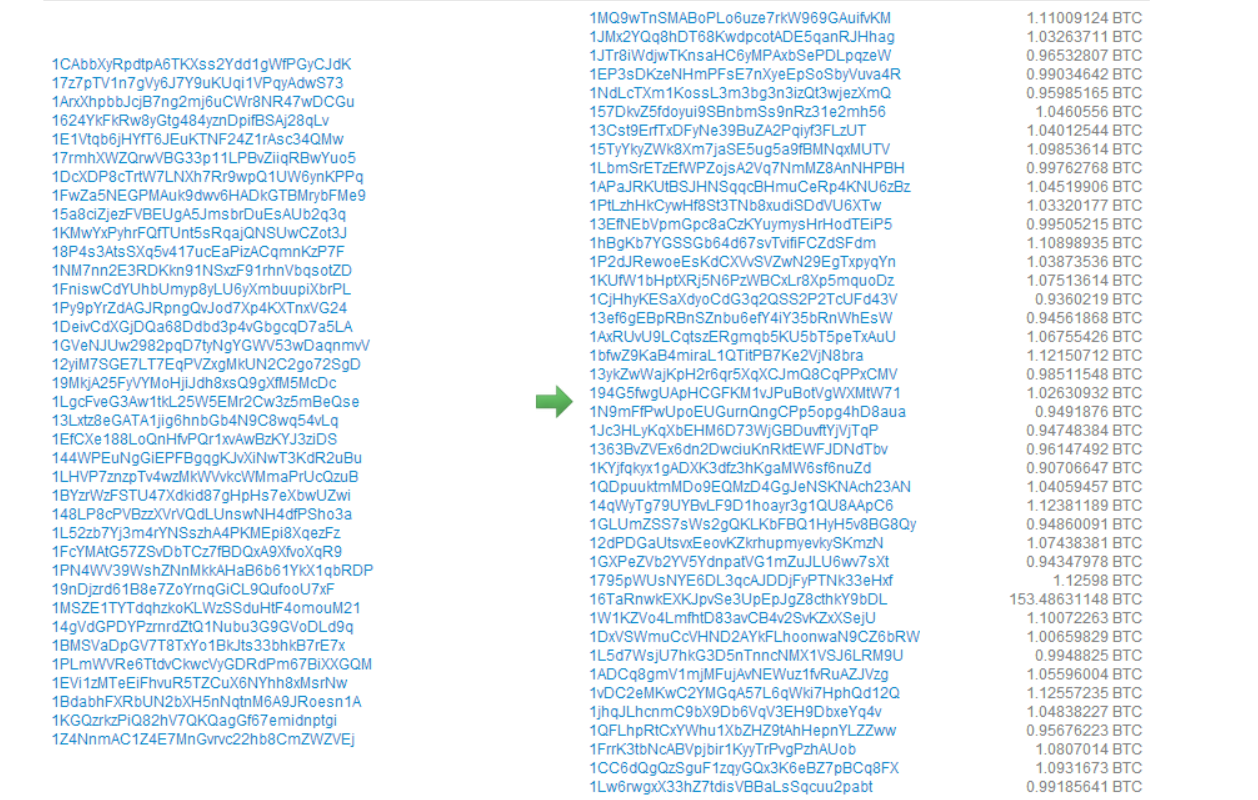
与传统的混合服务之间的重要区别是服务器不能没收或窃取你的硬币

What logs are kept?

The server does not need to keep any logs and transactions are only kept in memory for a short time. However if the server was compromised or under subpoena it could be force to keep logs. If this were to happen although you haven't gained any privacy you haven't lost any either.

服务器并不需要保存日志，交易只需要在内存中保存很短的一段时间。但是若服务器没收或被起诉他会被强制要求保存日志，即使这种事情发生，你的隐私也不会泄露。

What does a Shared Coin transaction look like?



How long do shared transactions take?

Between 30 seconds to 5 minutes depending on the number of iterations.

Is there a maximum transaction size?

The maximum transaction size is 50 BTC.

Is there a minimum transaction size?

We recommended you do not send transactions less than 0.01 BTC

Are there any fees for shared transactions?

Shared Coin is a free service however a bitcoin network fee of 0.0005 BTC is required.

How to use it safely without accidently leaking info?

- Tor can prevent leaking of information through your ip address.

保护你的信息不会从ip地址泄露

- Sending coins to or from tagged addresses reduces privacy.

从被标记的地址付款或收款可能会降低隐私

- When creating a Shared Coin transaction your browser generates a number or temporary/intermediate addresses（中间地址）. The balance of these addresses is not checked on blockchain.info itself unless the "Recover Intermediate Addresses" button is used. Looking up the balance of these addresses is an information leak as if blockchain.info was keep logs it would show you had an interest in these addresses. So don't use the "Recover Intermediate Addresses" tool unless there has been an error with a transaction.

出现错误？

熔币交易时，会经过一系列的地址进行周转。如果熔币加工过程被中途打断或发生错误，部分资金可能会留存在周转地址中。点击下面的按钮来取回所有暂扣于周转地址中的资金，整个过程可能需要几分钟才能完成。

周转地址残币回收

What limitations does it have?

Shared Coin can never completely sever the link between the input and destination address, there will always be a connection between them, it is just more difficult to analyse.

Is Shared Coin Open Source?

Yes. The Shared Coin client and server code can be found in blockchain.info's github repository https://github.com/blockchain

一、 比特币的匿名性

比特币网络通过以下三个措施进行隐私保护或匿名：

1、地址的生成无需实名认证；

2、通过地址不能对应出真实身份；

3、同一拥有者的不同账号之间没有直接关联，无法得知特定用户的全部比特币数量。

二、 比特币的匿名性弱点

1、与法币的兑换环节。比特币交易所的实名认证，是有效的反匿名措施，其他要求实名的比特币服务商也如此。有人说可以用假身份证件来逃过，在目前这是可行的，但以后交易所的身份验证一定会越来越严格。

2、交易公开。只需知道一个地址就可以找到关联人的一系列地址。另外，在论坛、微博、TWITTER、REDDIT、BBS等留下的许多信息，通过大数据分析可以汇总起来，会发现一系列的线索，除非你谨慎得像中本聪。

3、交易的汇总输入会暴露拥有人的其他地址。一旦你发送钱包中的大部分币给某人或某交易所，基本上会把你的全部地址都暴露无遗。因为交易会汇总大部分地址中的币打出去。

4、比特币的通讯协议未加密，向外打款时，协议分析软件可以找出IP地址与比特币地址的对应关系，如果在全国布署了这种监控系统，那定位到你的单位或小区就不是问题。(当然可以用TOR、VPN之类逃避)

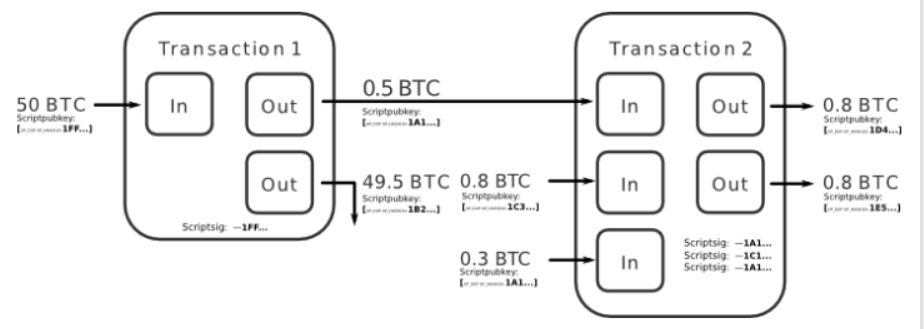
三、比特币块链的混币

为了解决以上隐私问题，有些网站提供了混币服务。 混向原理是割裂输入地址和输出地址之间的关系。

1、混币原理(CoinJoin)：许多人参与，一个交易中包括大量输入和输出，很难在输入和输出中找出每个人的对应对，输入与输出之间的联系被事实上割裂。多次混币、每次少量币，效果更好。

2、 以中心化网站(Blockchain.info)、Darkwallet(实际上也是中心化的，i混币需求要通过暗钱包服务器收集)，但是这些中心化和分布式服务都需要服务器，在服务器上会有混币纪录，不是很安全。Blockchain.info就会纪录混币需求一段时间后才删除，以应付有可能的司法检查。

3、Darkwallet引入Stealth Address隐身地址，打乱了块链的交易连续性，在较大程度上加强了匿名性。



Atlas CoinJoin Sudoku

Three criteria were used to identify a given transaction as a potential SharedCoin transaction: The transaction contained more than four inputs, the transaction contained more than four outputs, and the transaction was relayed internally by Blockchain.info.

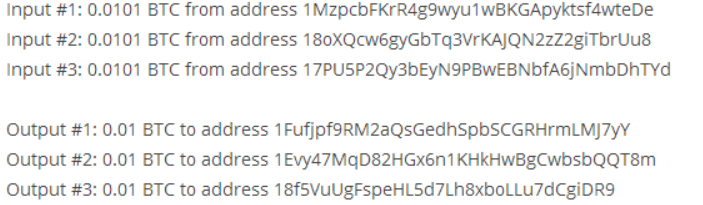
判断一个事物可能是shared coin有三个准则：交易大于4个输入；交易大于4个输出；交易被blockchain.info内部传输。

最好采用十次repetitions

生成新地址以避免隐私泄露；可能的话，不要从池中选出多个地址。

Coinjoin：比特币输入输出可以有多个，单笔交易的多个用户的资金不需要第三方托管；当所有的交易对象都签单的时候，（同步地），结果才会被提交到blockchain；

SX’s CoinJoin：用户在一个聊天室里，每个人**贡献和接受相同的资金**，由CoinJoin server统一调配；



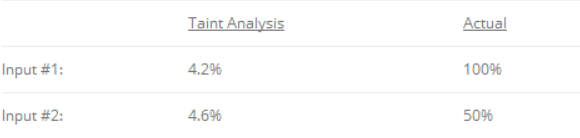
剩余0.0003作为交易被迅速确认的交易费

由于这种方法不允许改变地址，在参与CoinJoin操作之前，事实上，所有的参与者都必须在输入地址上等效平衡。

Shared Coin 共同特征：

* 它们被blockchain.info内部IP地址传输
* 它们输入大于9
* 它们输出大于9
* 输入和输出的数目通常不同
* 总是包含矿工费，费用多为常数（目前为0.0001BTC）

加大输出数目，或分裂用户资金和加入一些随机数地址



寻找大量输入和输出的共同所有方，并按数值将其配对；