图解比特币白皮书

理解加密货币的大爆炸

2018年11月是中本聪所著的**比特币白皮书**诞生10周年。
今天，围绕着炒作，暗网营销，加密货币的碳足迹和对立的技术标准等争议愈演愈烈。
在比特币进入大众视野前，它代表着一种伟大的**理念**：**全球电子现金**。
这种理念仍然存在，只是很少人能够真正明白它的**绝妙之处**。
希望这则漫画能帮助大众了解比特币。

- 斯科特· 麦克劳德 2018年11月

比特币:
种点对点电子现金系统

“一种双方无需借助金融机构可以直接在线支付的点对点电子现金。”

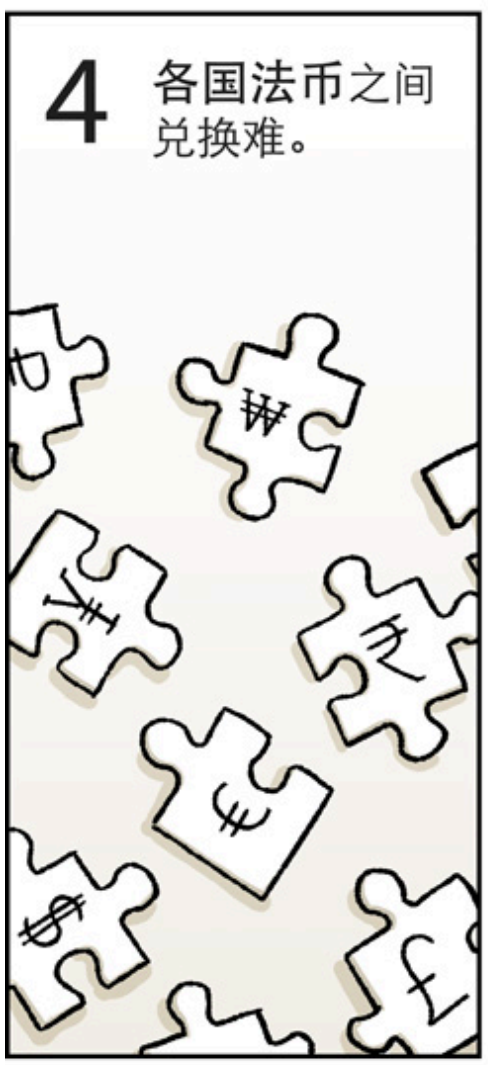
-中本聪

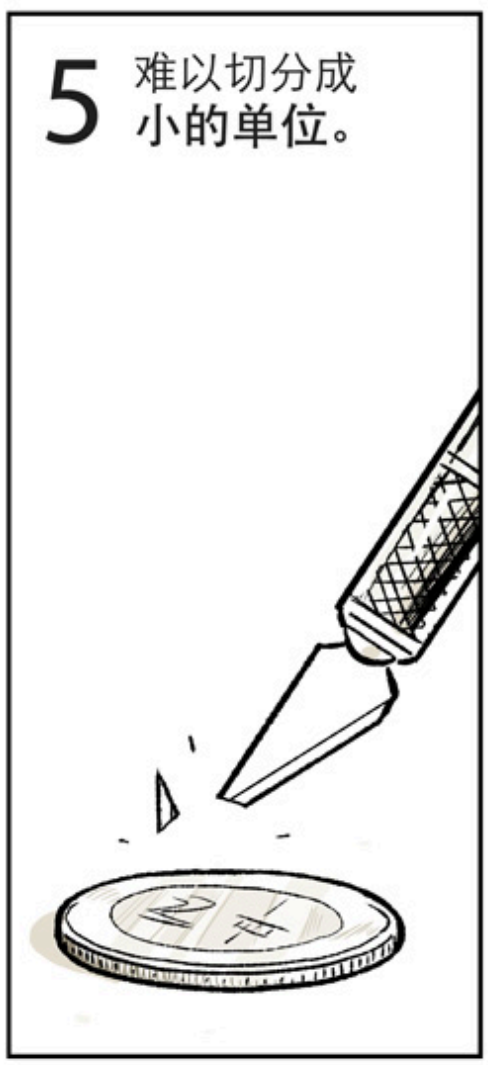

呃，
我这样解释下吧。
当今的金融体系下，
金钱：

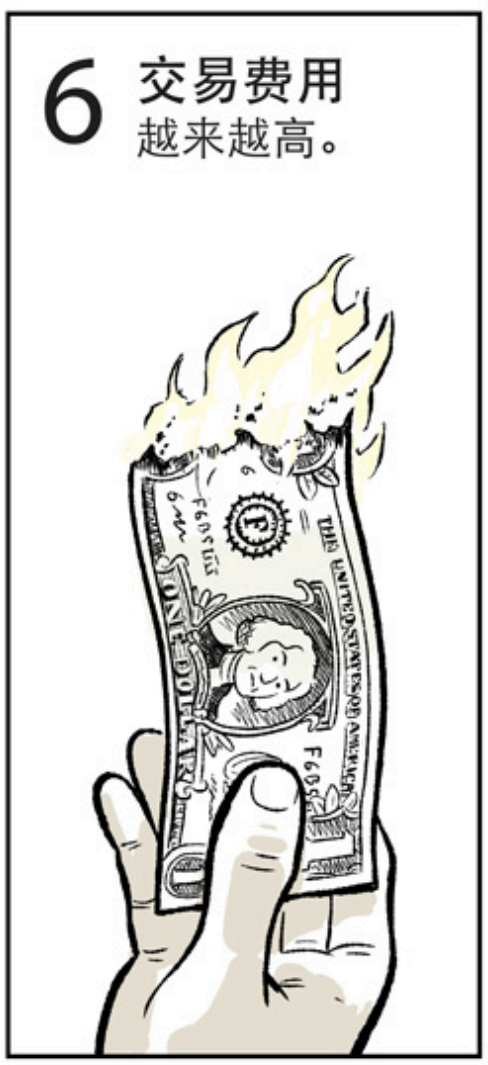

1 容易超发，
容易管理不当。


2 越来越
没有隐私性
可言。


3 容易受到攻击。


4 各国法币之间
兑换难。


5 难以切分成
小的单位。


6 交易费用
越来越高。


7 有20亿人都
难以使用上。


好吧，
好吧。
我们的
法币太糟糕了。


但是，我怎么才能相信
这种点对点现金
不会比现有的更差劲，
比现有的更不稳定?
嗯，
关键在于...


不要依赖信任!
啊!
你哪位呀!

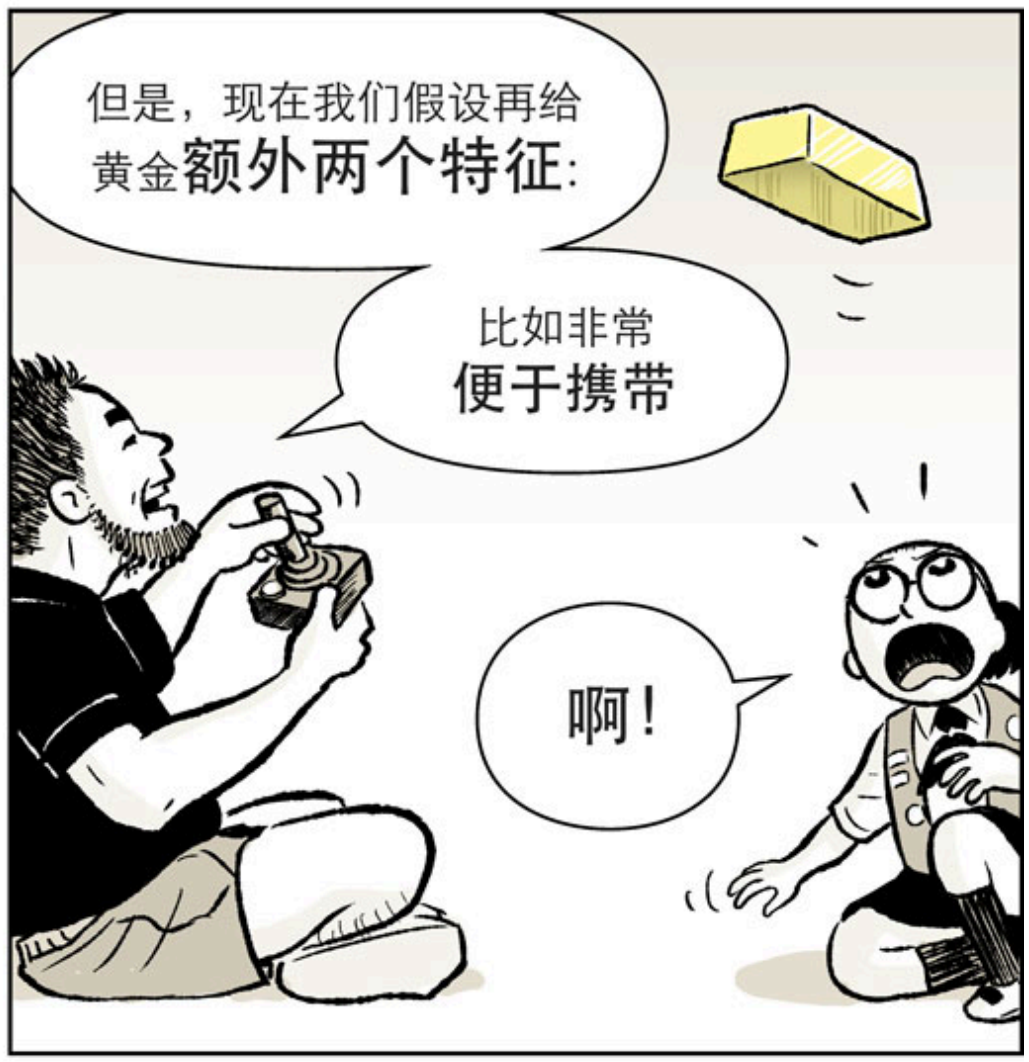

我就是中本聪
啥，
我以为刚刚
那老头是中本聪。
WRRRRRR...


现在让我们假设：
要是我用手上的
金块换取你手上的饼干。
!!
好呀好呀


现在
我可以品尝
这些饼干了，但是
你却不能吃下这些
金块，对吧。

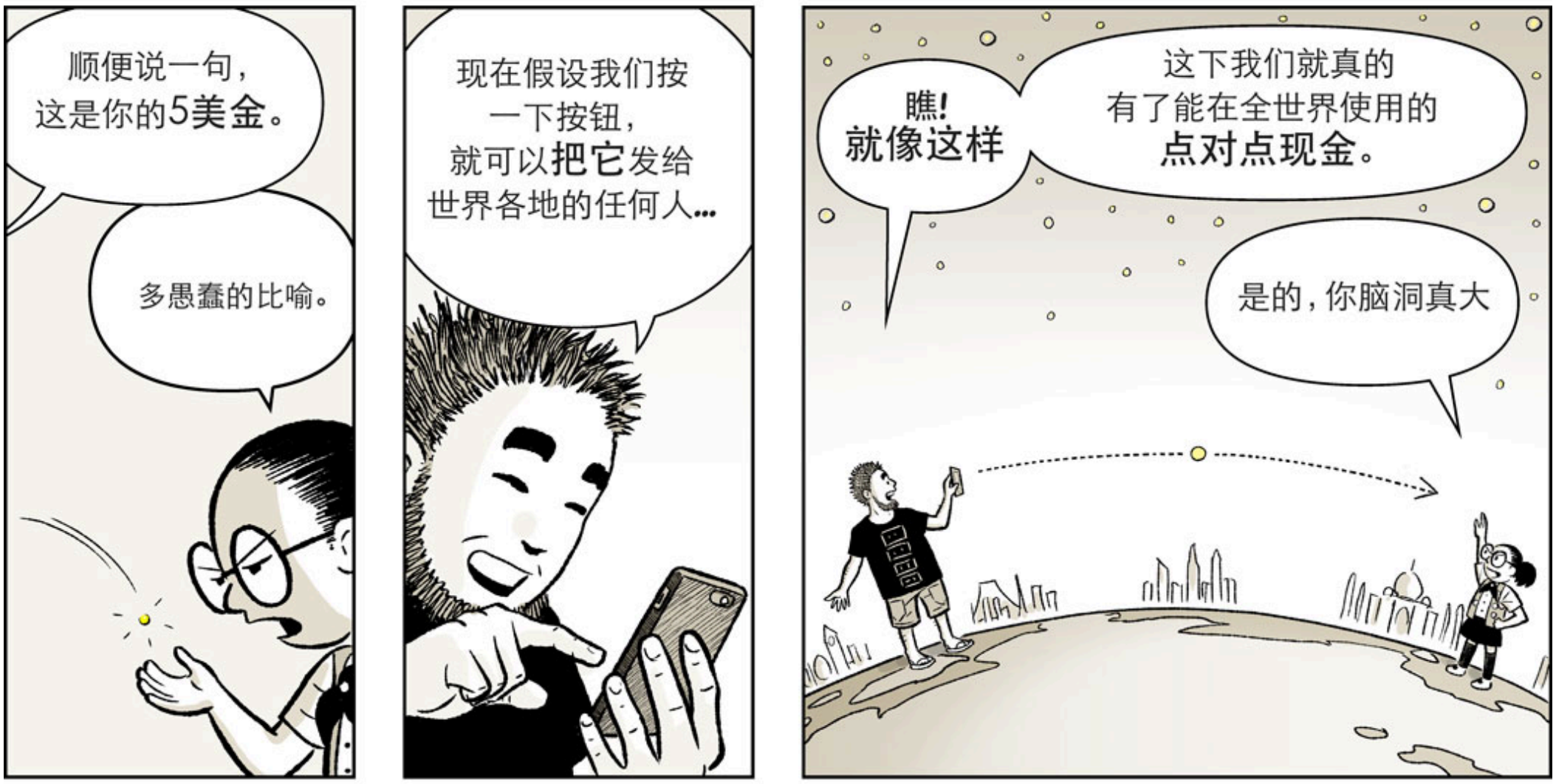

OOF!
是的，
我不能吃下。
但是我可以卖掉!
然后再买
10万盒饼干!

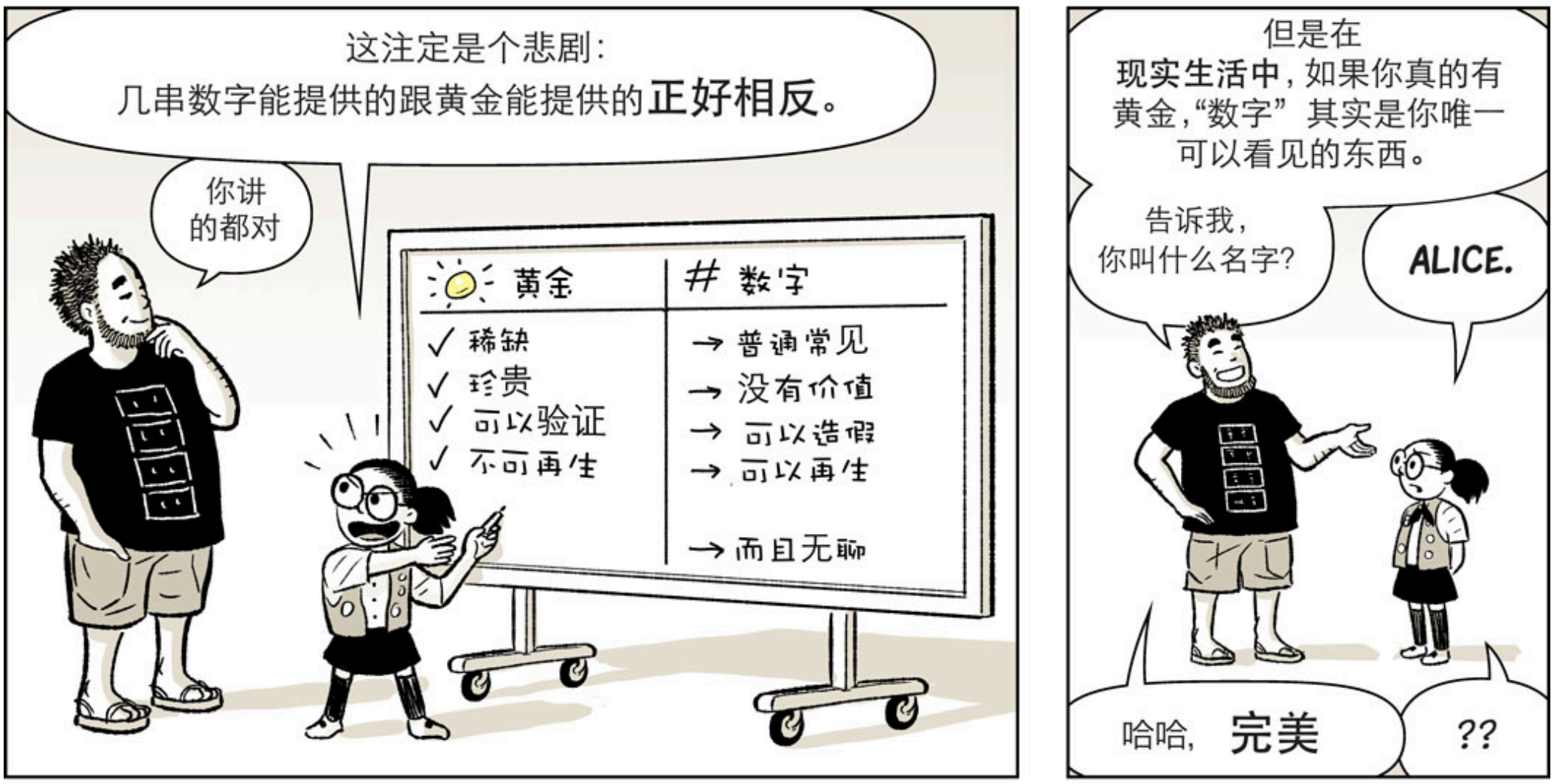

真聪明，
金块很稀缺。
人们都想要
黄金，所以它
非常珍贵。
它的价值是可以
被验证的。
而且不可再生！


但是，现在我们假设再给
黄金额外两个特征：
比如非常
便于携带
啊！

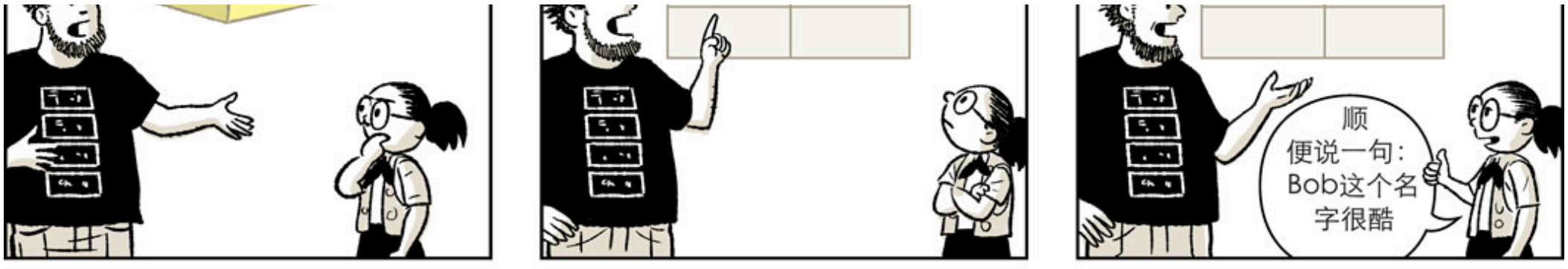

而且还可以
不断切分
K-PASH!!
啊!

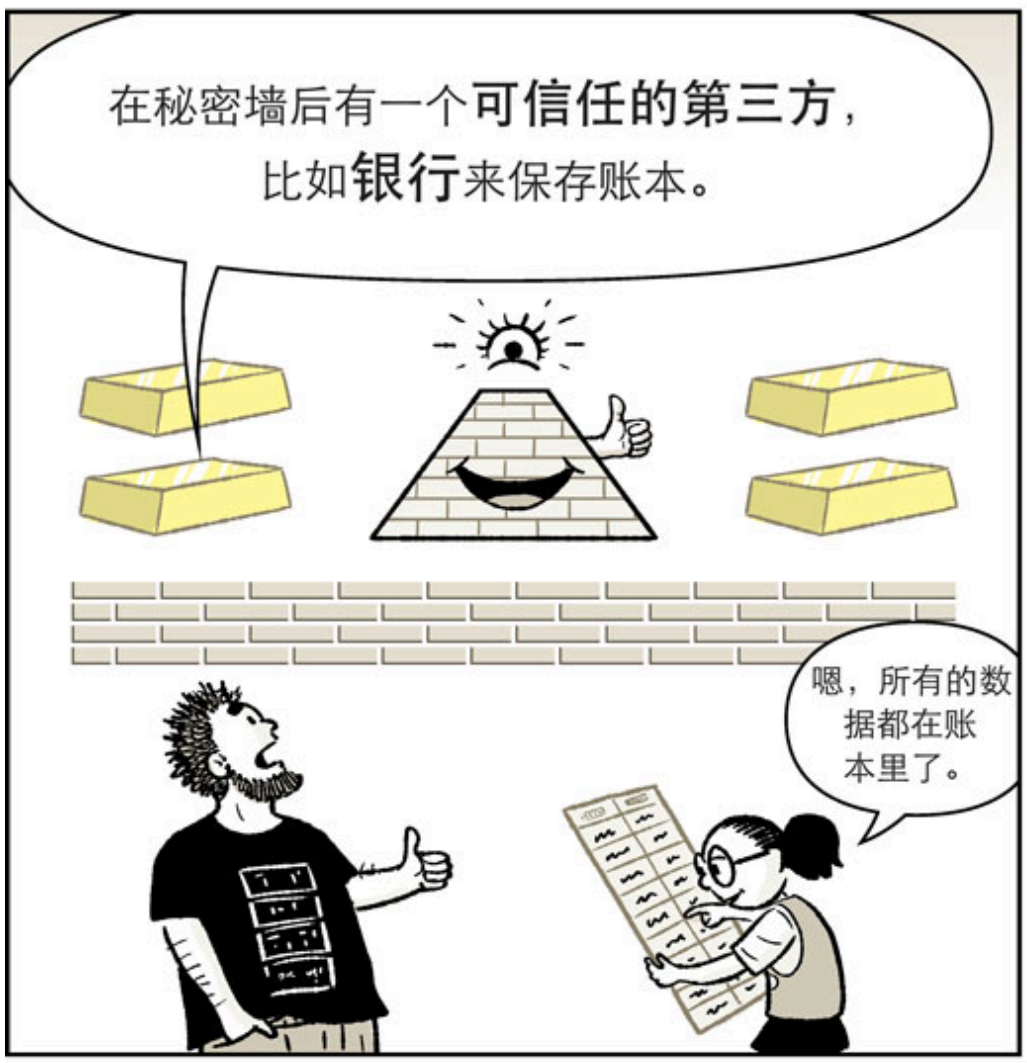

可以不断地
切分成更小的
单位。

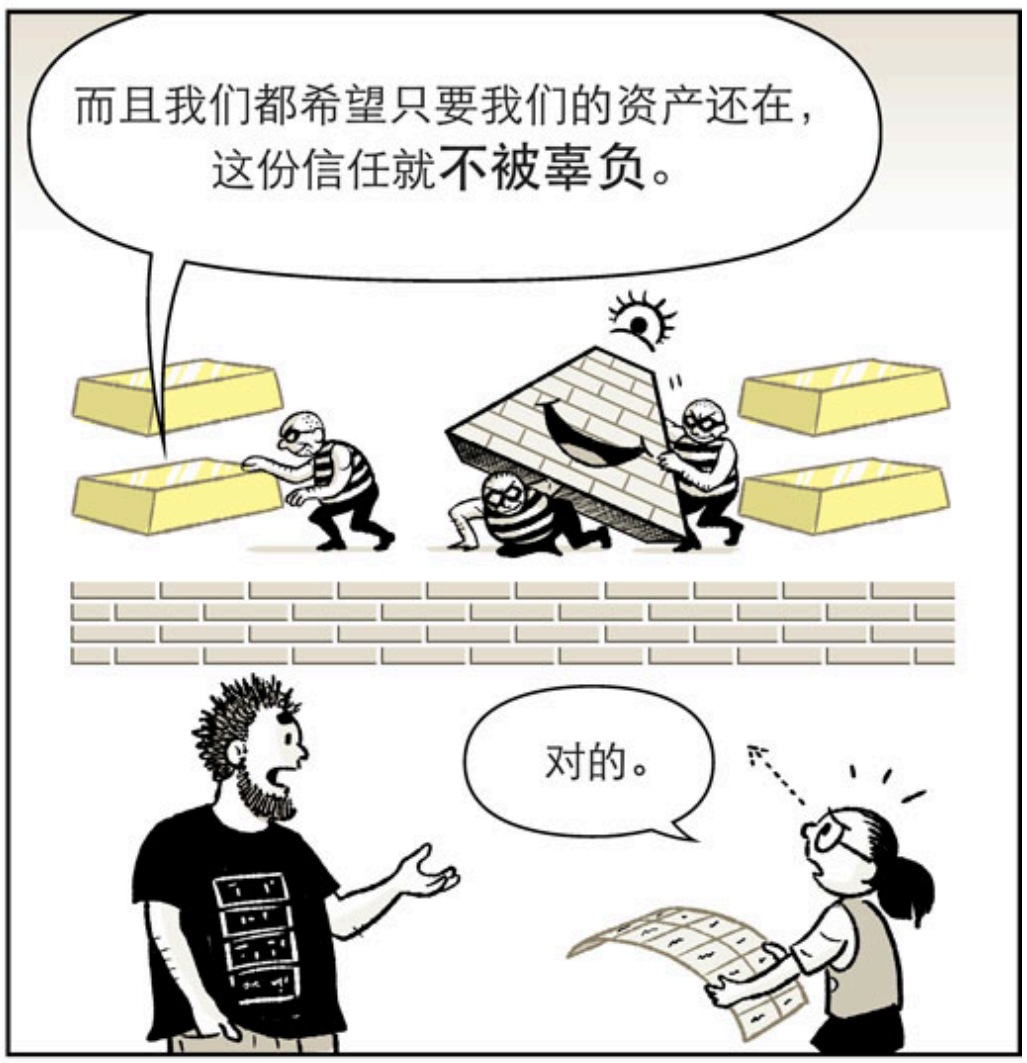

顺便说一句，
这是你的5美金。
多愚蠢的比喻。
现在假设我们按
一下按钮，
就可以把它发给
世界各地的任何人...
瞧！
就像这样
这下我们就真的
有了能在全世界使用的
点对点现金。
是的，你脑洞真大

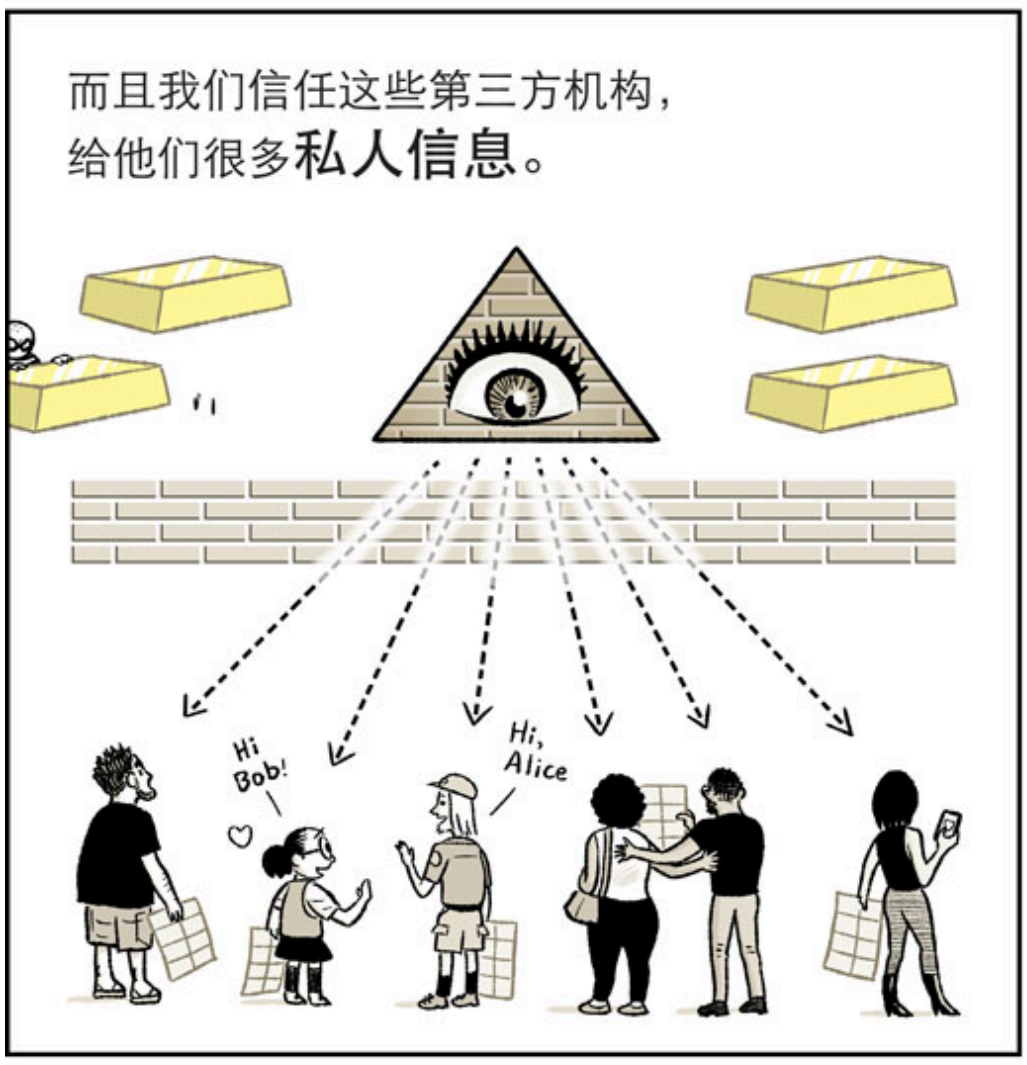

这注定是个悲剧：
几串数字能提供的跟黄金能提供的正好相反。
你讲
的都对
黄金
数字
✓ 稀缺
✓ 珍贵
✓ 可以验证
✓ 不可再生
→ 普通常见
→ 没有价值
→ 可以造假
→ 可以再生
→ 而且无聊
但是在
现实生活中，如果你真的有
黄金，“数字”其实是你唯一
可以看见的东西。
告诉我，
你叫什么名字?
ALICE.
哈哈，
完美
??

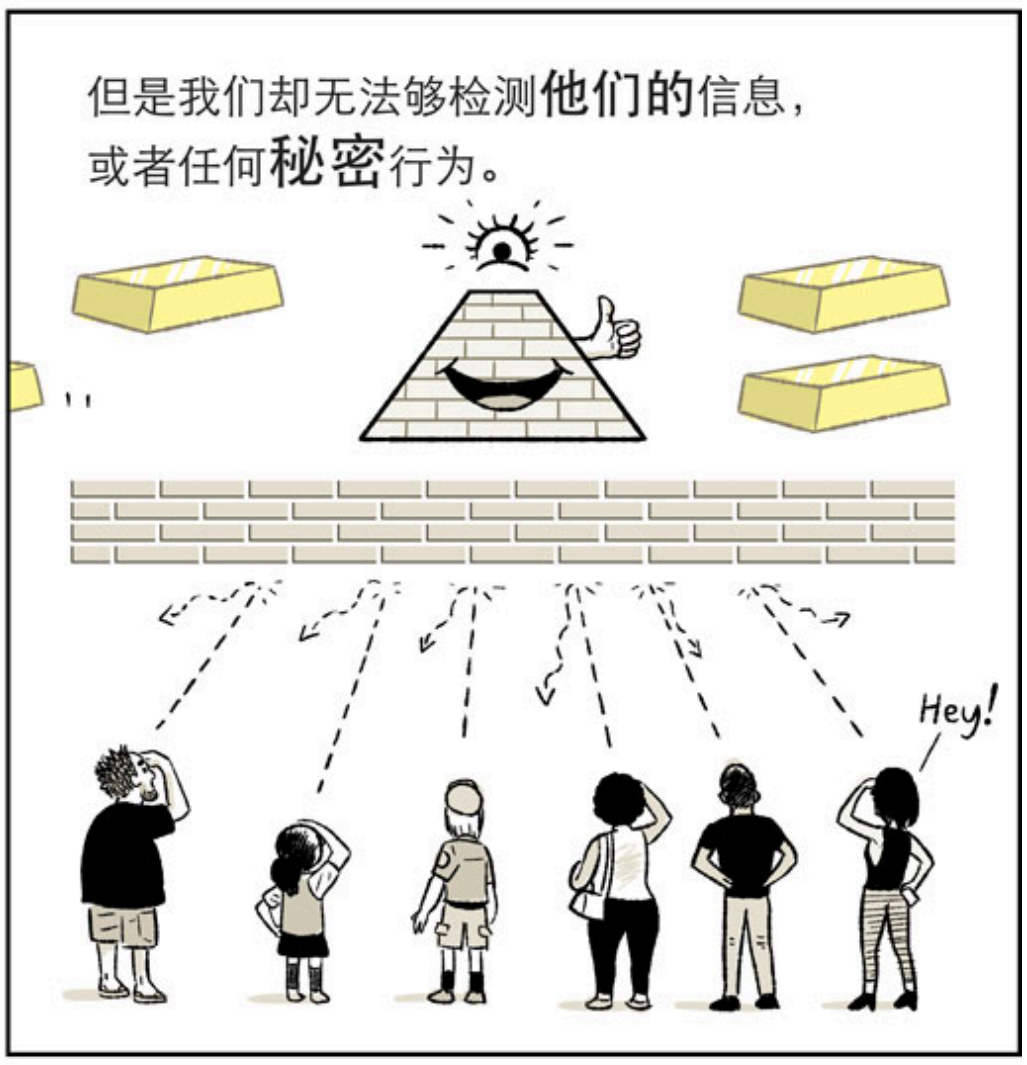

假如Alice
拥有5美金的黄金，
或者其他任何资产。
实物体积估计都比较大，
对吧
是的。
Alice想把她的名字印在了
某个账本上来表示她的
所有权。
owner
share
Alice
$5.00
如果
Alice给Bob两美金，
资金永远在那里，
没有改动，改变的只是账本。
明白了
owner
share
Alice
$3.00
Bob
$2.00


顺
便说一句：
Bob这个名
字很酷

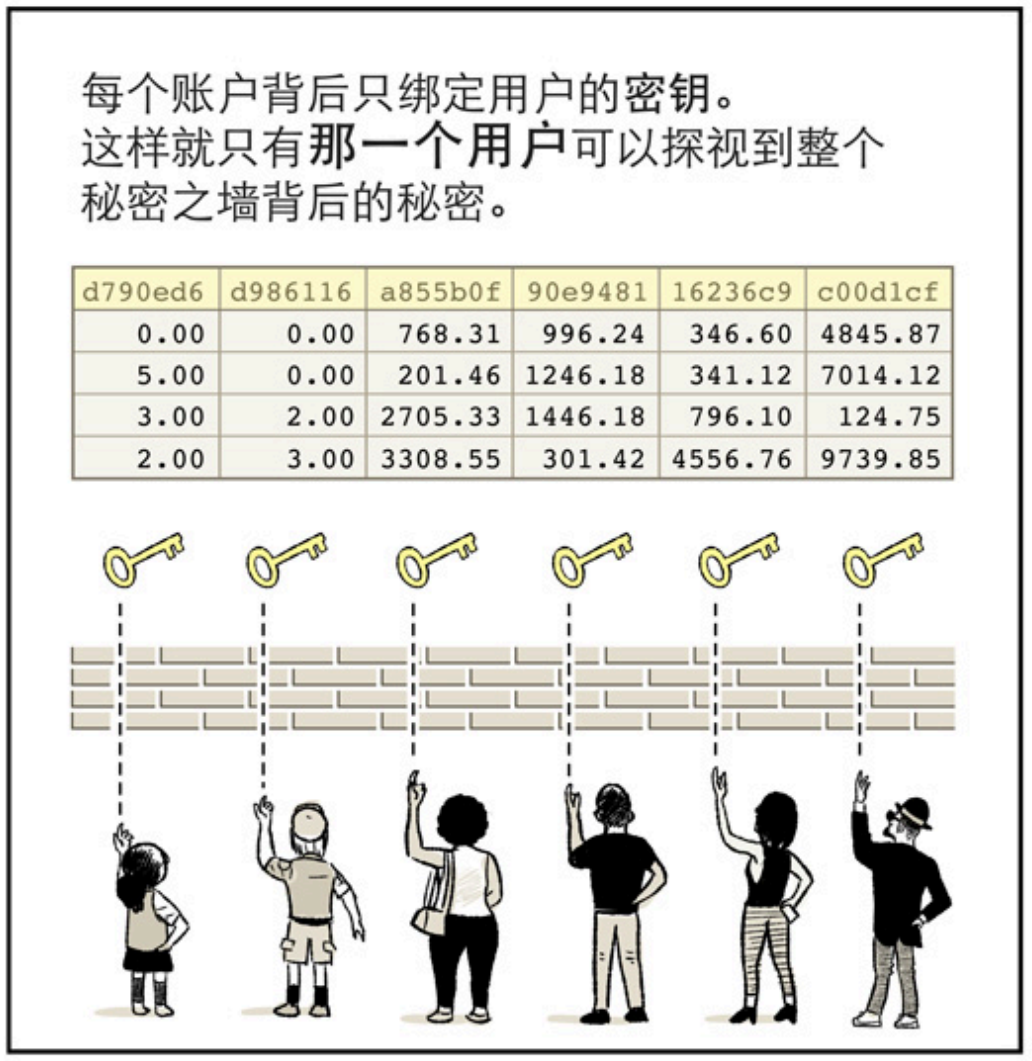

在秘密墙后有一个可信任的第三方，
比如银行来保存账本。
嗯，所有的数
据都在账
本里了。


而且我们都希望只要我们的资产还在，
这份信任就不被辜负。
对的。


而且我们信任这些第三方机构，
给他们很多私人信息。
Hi
Bob!
Hi,
Alice

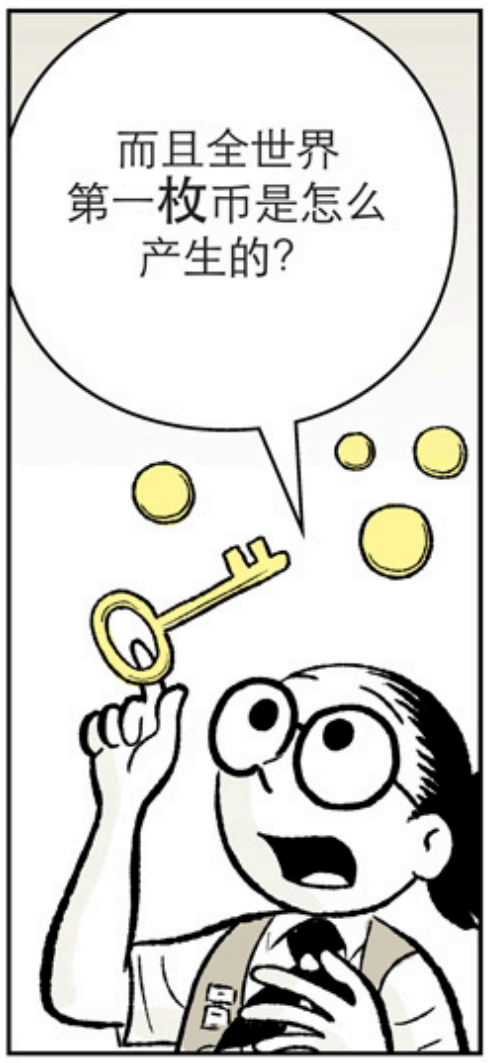

但是我们却无法够检测他们的信息，
或者任何秘密行为。
Hey!


真正的点对点
现金不需要信任，
只需要一个大的，
人人可见的账本。


每个账户背后只绑定用户的密钥。
这样就只有那一个用户可以探视到整个
秘密之墙背后的秘密。
d790ed6 d986116 a855b0f 90e9481 16236c9 c00d1cf
0.00 0.00 768.31 996.24 346.60 4845.87
5.00 0.00 201.46 1246.18 341.12 7014.12
3.00 2.00 2705.33 1446.18 796.10 124.75
2.00 3.00 3308.55 301.42 4556.76 9739.85


听懂了吗?
有啥问题吗?
我的天呢，
好多问题想问


谁保管这个账本，
钥匙是怎样运行的，
为啥私钥有任何价值?

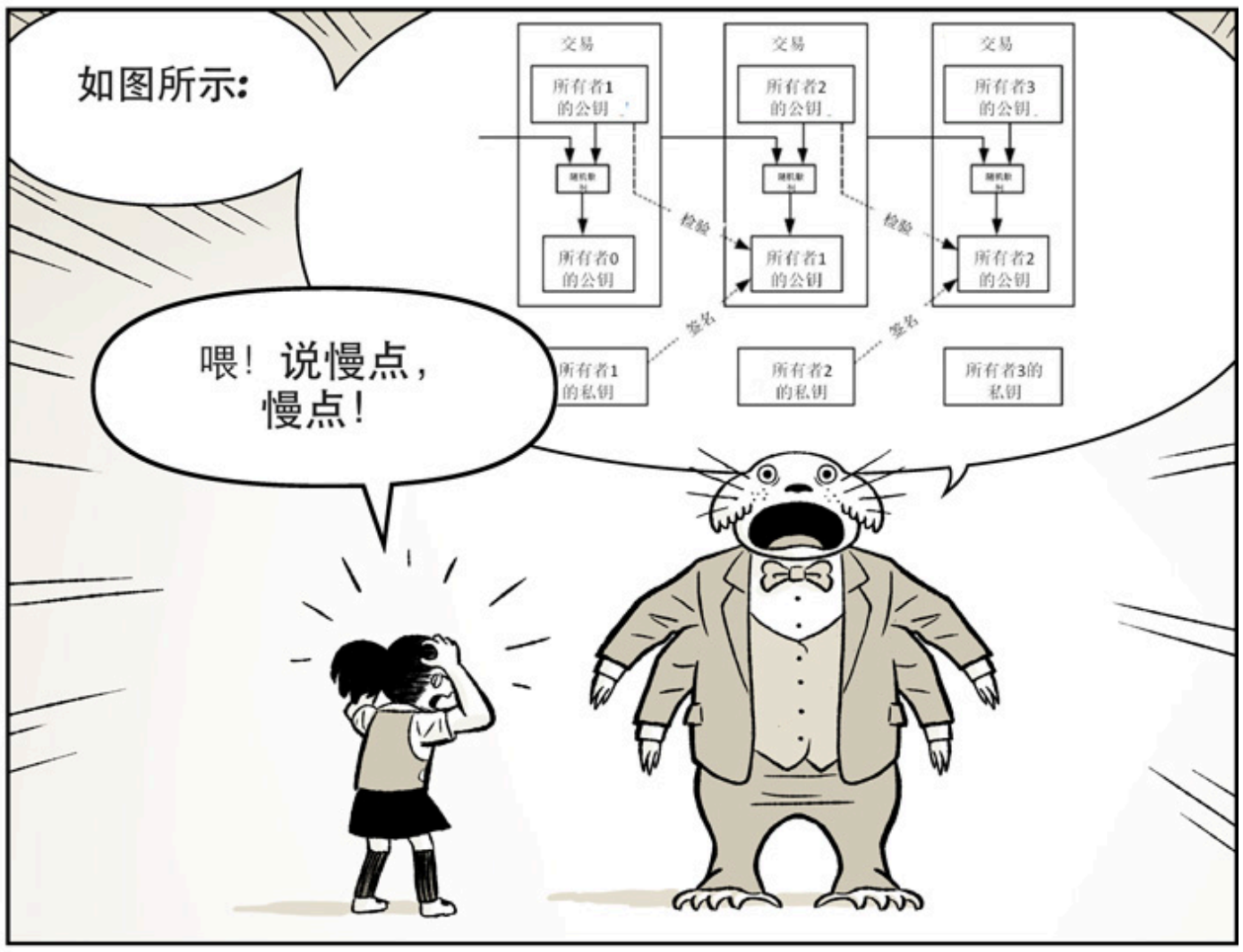

而且全世界
第一枚币是怎么
产生的?


一枚币就是一连串的数字签名
哎呦，我去


聪叔叔
什么是
哦，天，
人呢?
我是中本聪


哎呦!
我去...
好吧。聪叔，
“数字签名链”，
刚刚是这样说的吗?

人名Alice给人名Bob发送0.001比特币，通过**上一笔交易**的数字签名哈希Bob的**公钥**，一直到这笔币发送完成。

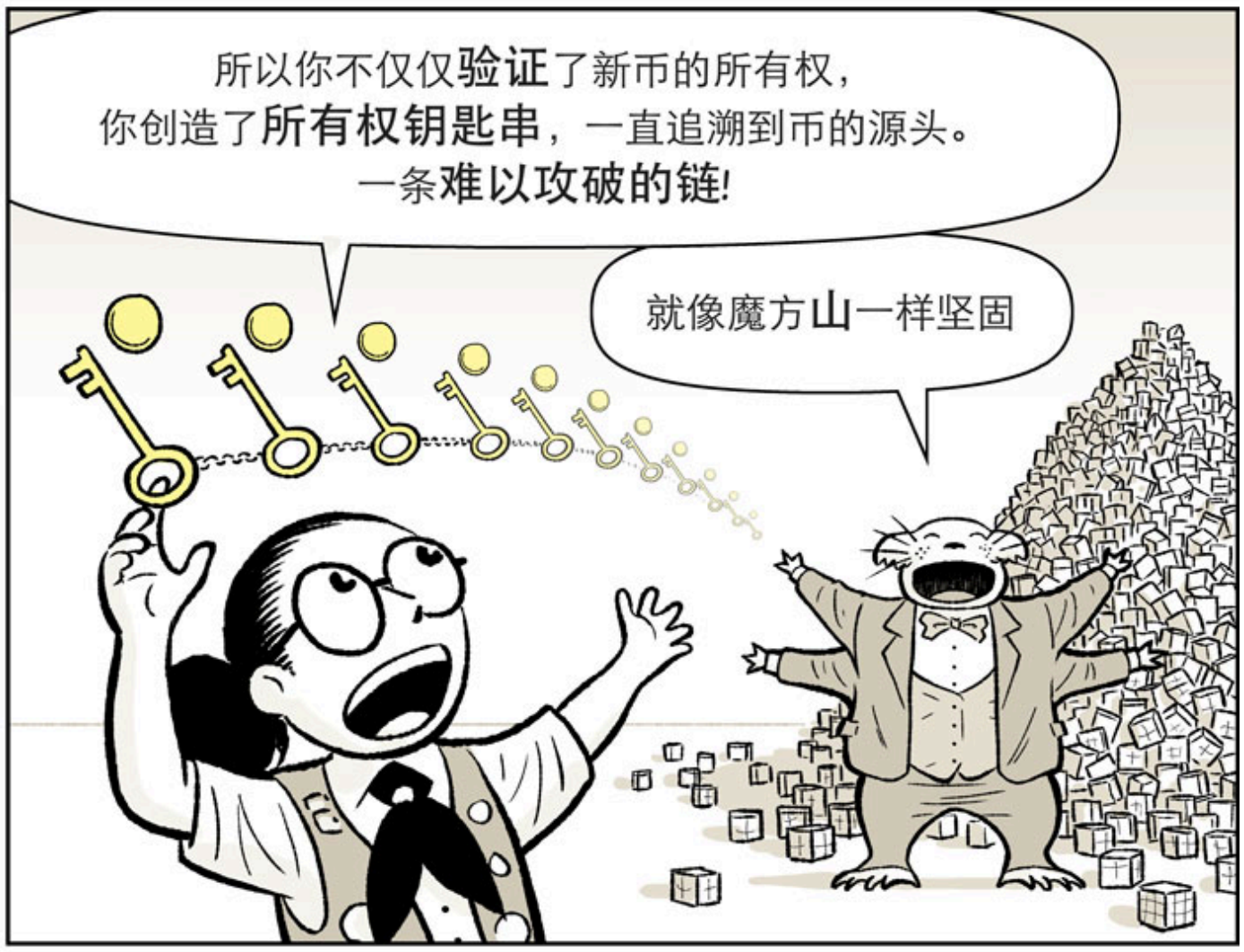


一个魔方！等一下，我想起来在数学夏令营中，他们有个类比说：

“打乱容易，拼一起就难了。”

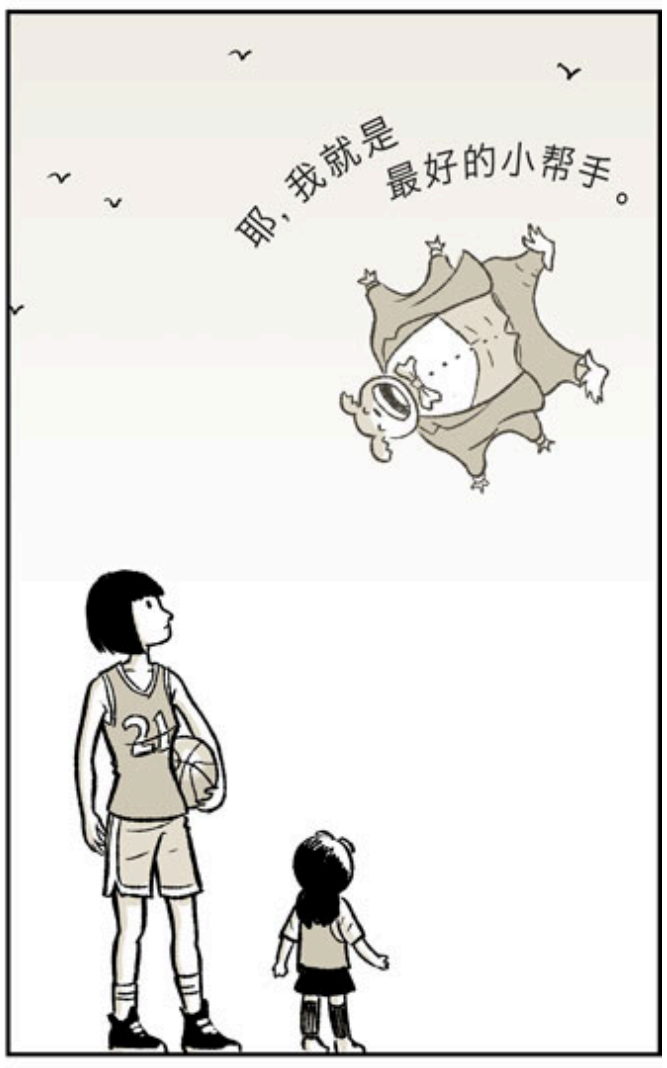
每个人都可以使用我的**公钥**来给物体加密，但是只有我的私钥才能**解开**这个东西


还有“哈希”...
就是上一笔交易的打乱版本。
正确!

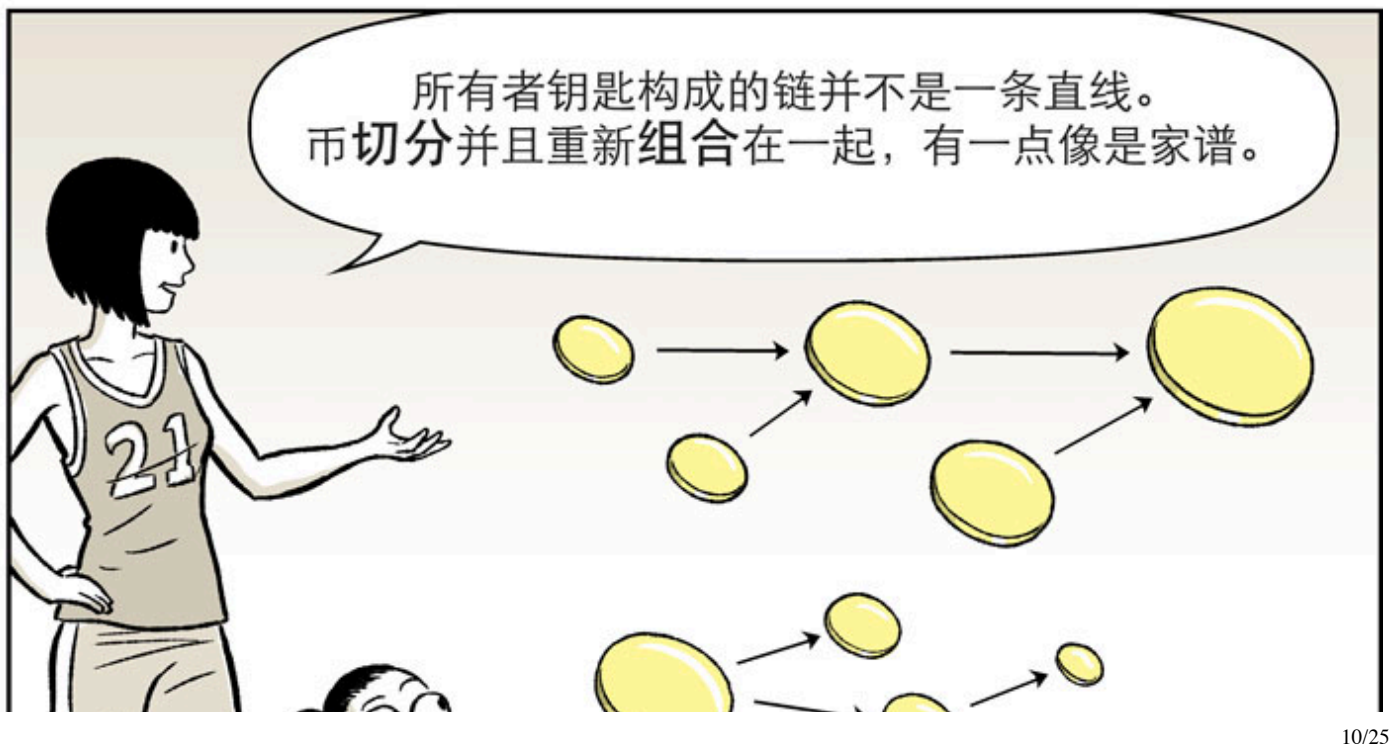

所以你不仅仅验证了新币的所有权，
你创造了所有权钥匙串，一直追溯到币的源头。
一条难以攻破的链!
就像魔方山一样坚固


嘿，这就是人人都在讨论的
区块链吗?
并不是


区块链就是一种全新的账本，
我们之后会提到的。
但是，没错，
所有者钥匙就是
区块链的一部分。
呃...


耶，我就是
最好的小帮手。


让我猜猜你是谁
中本聪
很高兴为你效劳


所有者钥匙构成的链并不是一条直线。
币切分并且重新组合在一起，有一点像是家谱。


假设家庭进行重新组合，重新融合，
嗯，确实有点像是家谱。

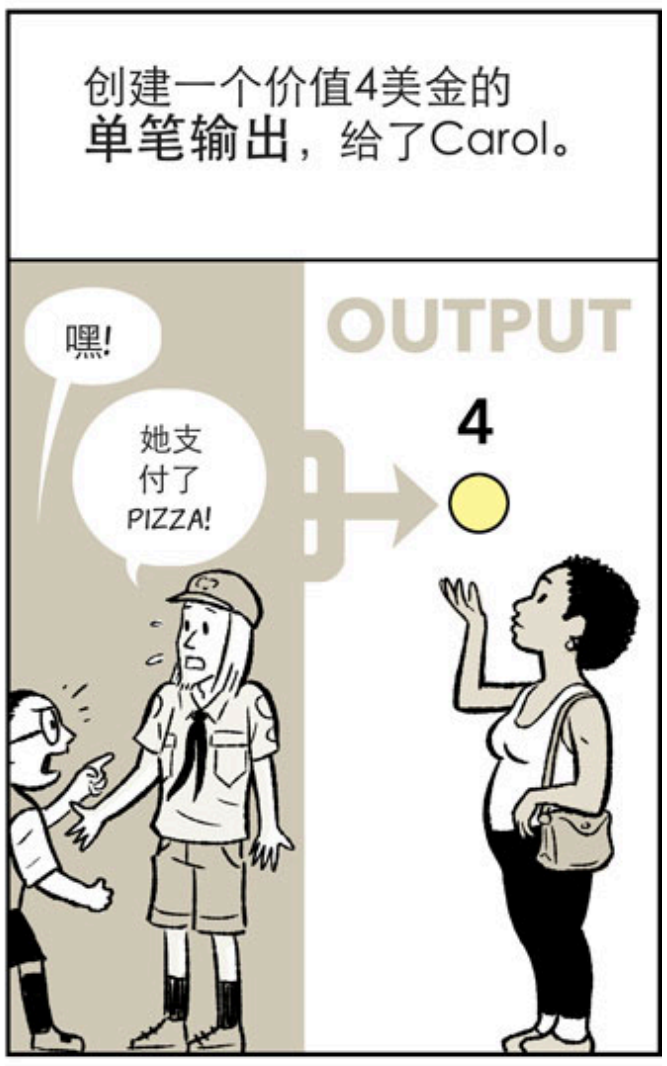

Alice有一枚价值5美金的货币，要给Bob发送2美金。

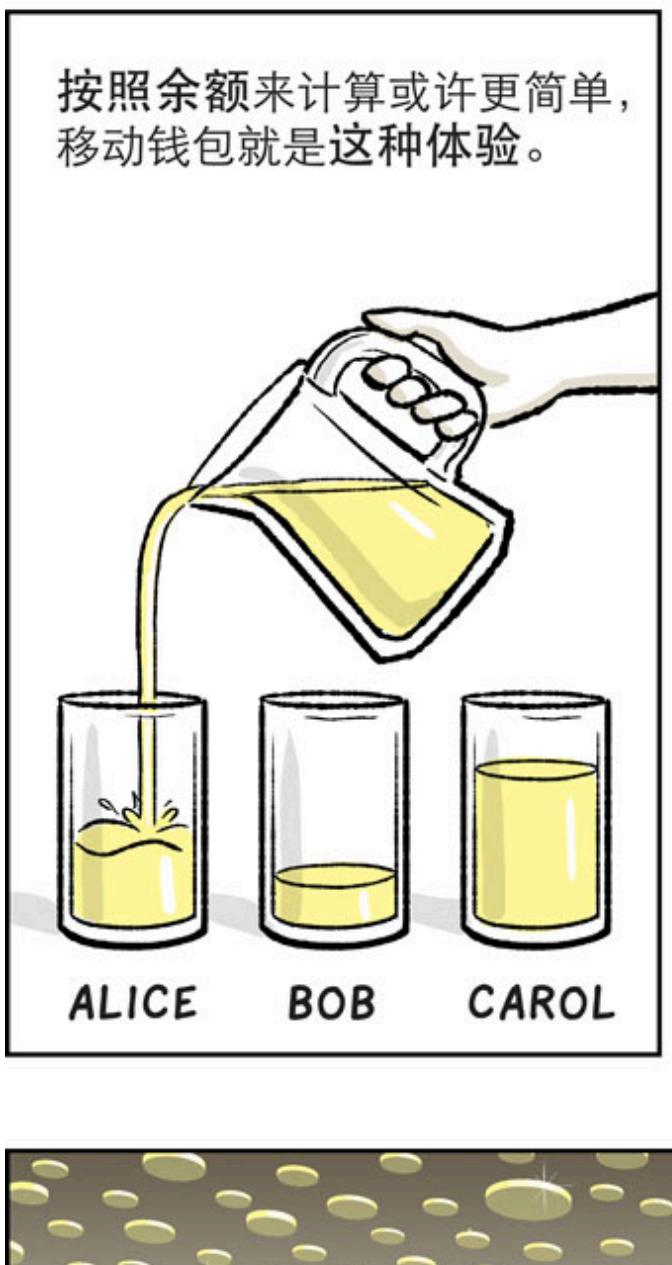

5美金就是那笔交易的唯一输入，也就是进入那笔交易的数量。
5


但是呢，有两笔输出。
2美金给了Bob，还要
3美金的余额留给了自己。
OUTPUTS
好奇
怪呀
2
3


确实奇怪，但是很高效。
Bob找零或者你把交易提前分割
都会变成多笔不同的交易。
啊

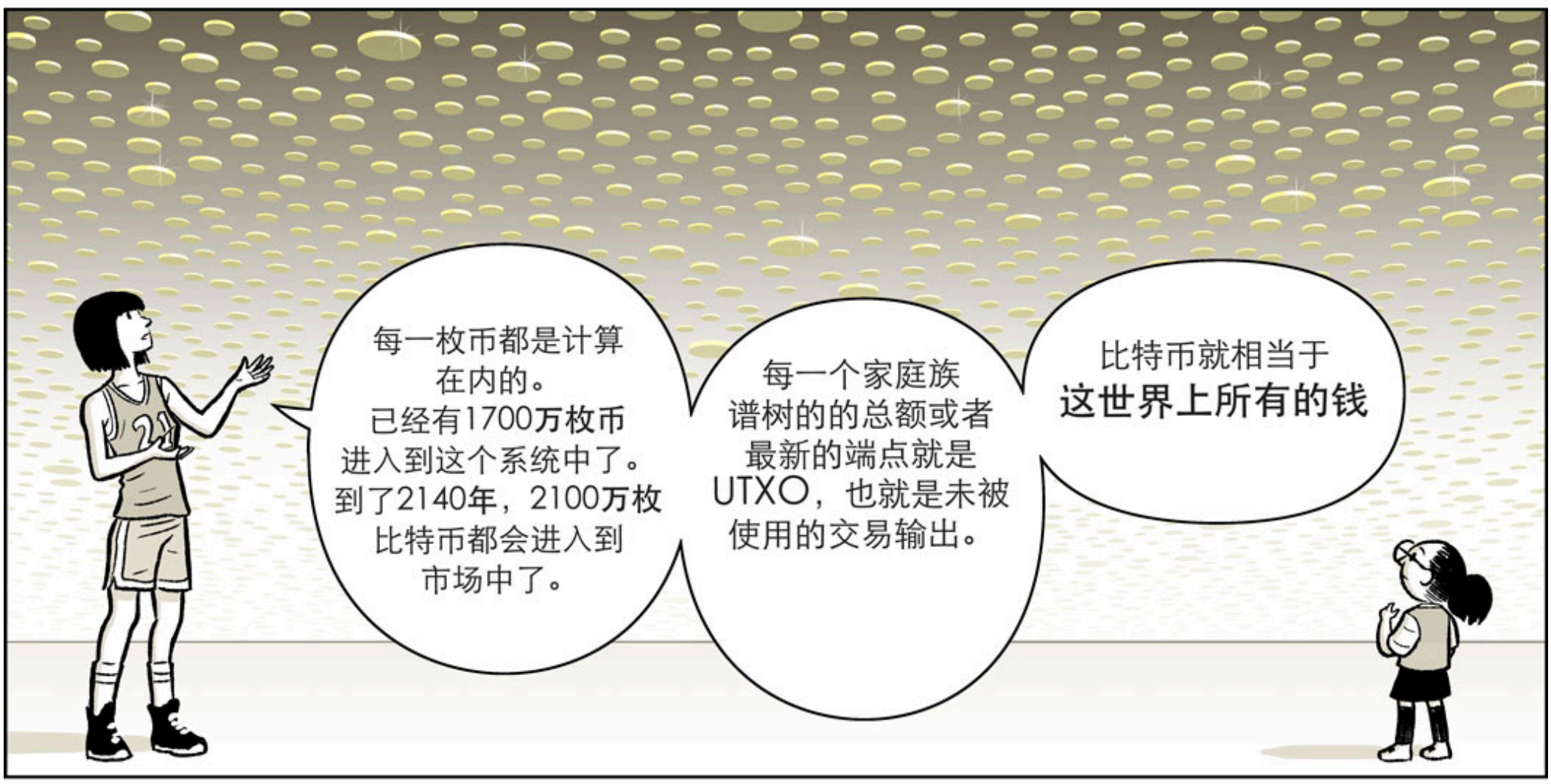

现在如果Bob拿到了2美金，
添加2笔一美金的币，
他就可以使用多笔输入。
1
1
2


创建一个价值4美金的
单笔输出，给了Carol。
OUTPUT
嘿!
她支
付了
PIZZA!
4

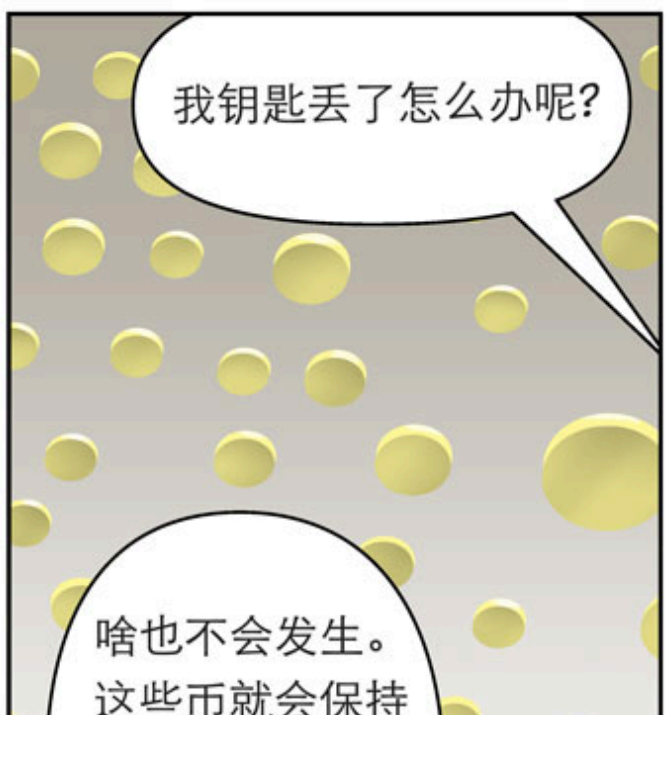

按照余额来计算或许更简单，
移动钱包就是这种体验。
ALICE
BOB
CAROL


但是余额往往跟
账户所有者的身份挂钩。
嘿！那是
我的杯子..
=好吧=


通过
这种方式，
所有者的私
钥可以来来
去去。
但是币的身份却
一直存在。


每一枚币都是计算
在内的。
已经有1700万枚币
进入到这个系统中了。
到了2140年，2100万枚
比特币都会进入到
市场中了。
每一个家庭族
谱树的的总额或者
最新的端点就是
UTXO，也就是未被
使用的交易输出。
比特币就相当于
这世界上所有的钱


币结合或者分割，通过钥匙转来
转去，但币实际上并没有任何
转移。
它们一开始就从没
存在过某个地方。


我钥匙丢了怎么办呢?
啥也不会发生。
这些币就会保持


这也就是为什么长期来看，
这些货币是通货收缩的。
流通量会逐渐减少。
直到
2140年

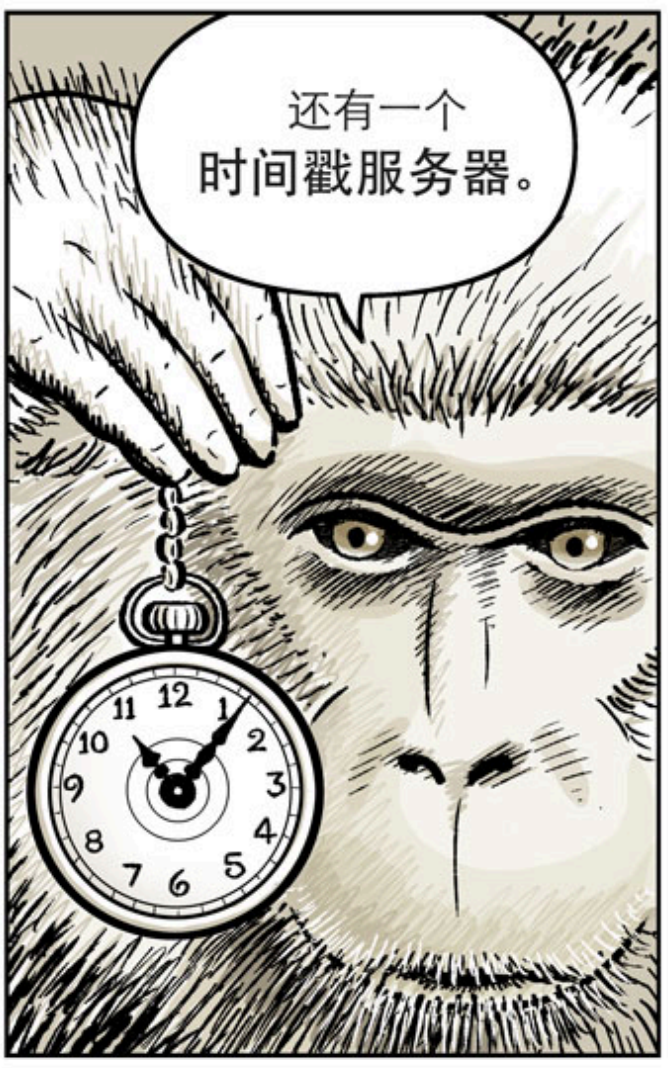

无人领取的状态。
或许永远都没人
认领了。


对的


但是还是只是一串数字呀。
怎么防止我跟其他五个国家的5个朋友使用同一个钥匙和币，并且不会在同一时刻购买一块糖果块？ 理论上来讲....

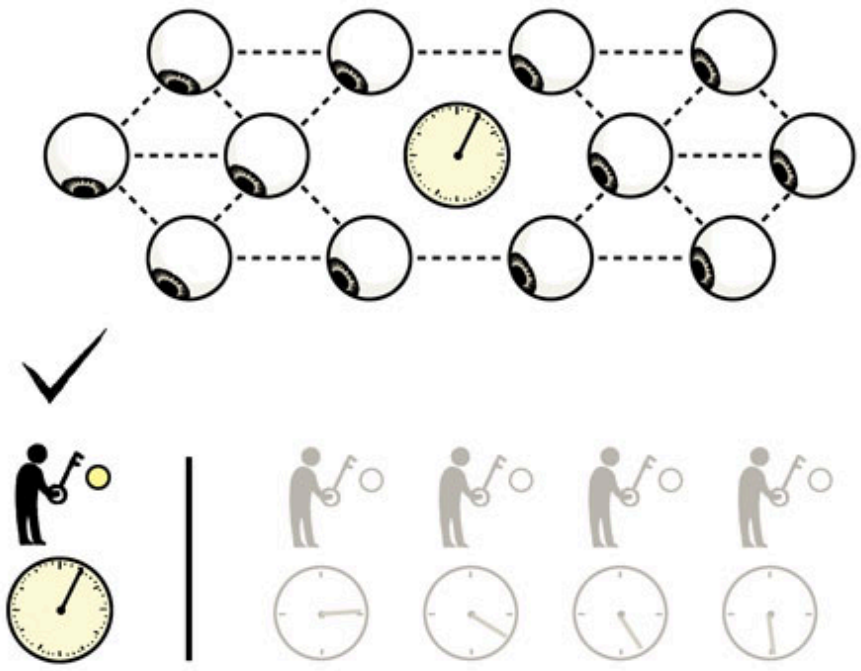

要想证明一笔交易没有发生，
就必须认证所有的交易。
！


讲得好，中本聪。你怎么又变成一只猴子了?
这就是为什么我们需要一个全球统一的账本。
对吧?
是的。

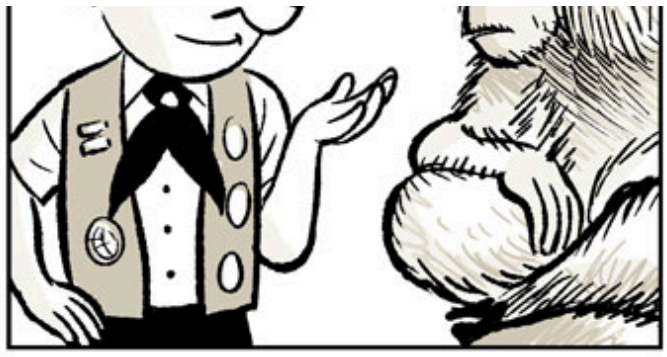

还有一个
时间戳服务器。


你跟你那5个有犯罪倾向的
小伙伴提出了
“双花”问题。
犯罪?
他们才不是
我是说。。

点对点分布式时间戳会按照**时间顺序**来证明每一笔交易的发生。并且只认可**第一笔被认可的**交易。



其他待定的交易快速广播给其他节点，只有一笔交易会**被商家看到**。诈骗的**几率很小**。




就是!
为什么我们要没日没夜的劳作!
我们有一种骑士精神。
其实是为了钱，对吗?


呃，是的。是为了钱。
帮助确认交易可以获得比特币奖励。
还有手续费。
嘿，你们是德国人吗?


我们都是中本聪。
呃，大叔别闹


不要小瞧德国人嘛。
不是也有一些日本元素吗?
没人告诉过我们需要啥元素。
我花了几个小时才打扮成这个样子。

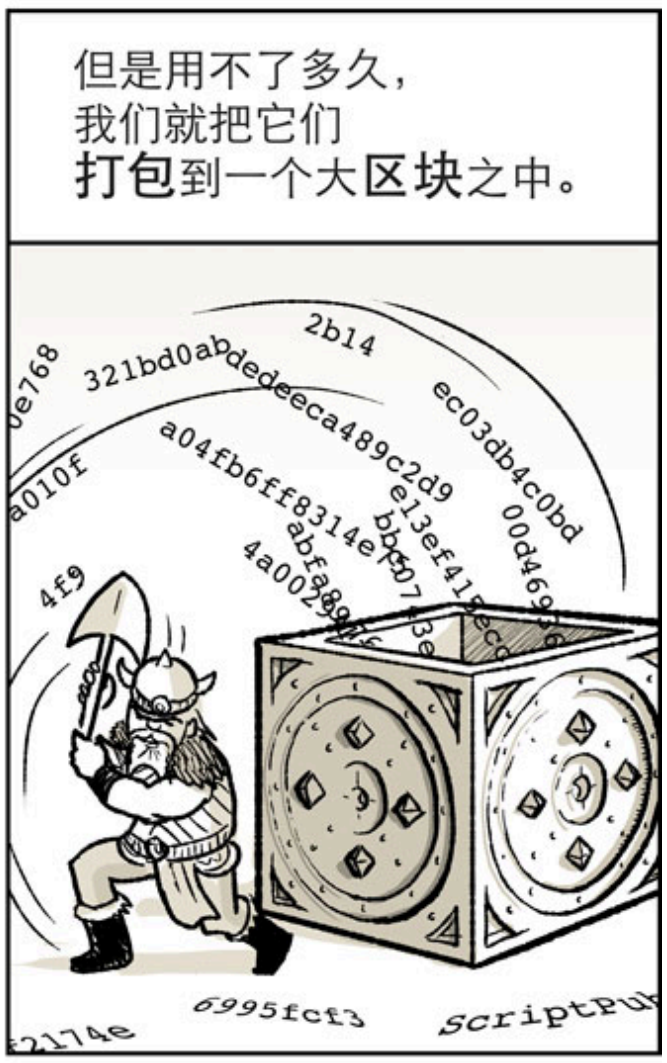

不用在意这些细节。所以在我给Bob发送一笔交易的时候，这笔交易其实是待定状态。
你可以立马看到这个吗?
是的。
其他的也都是这样!

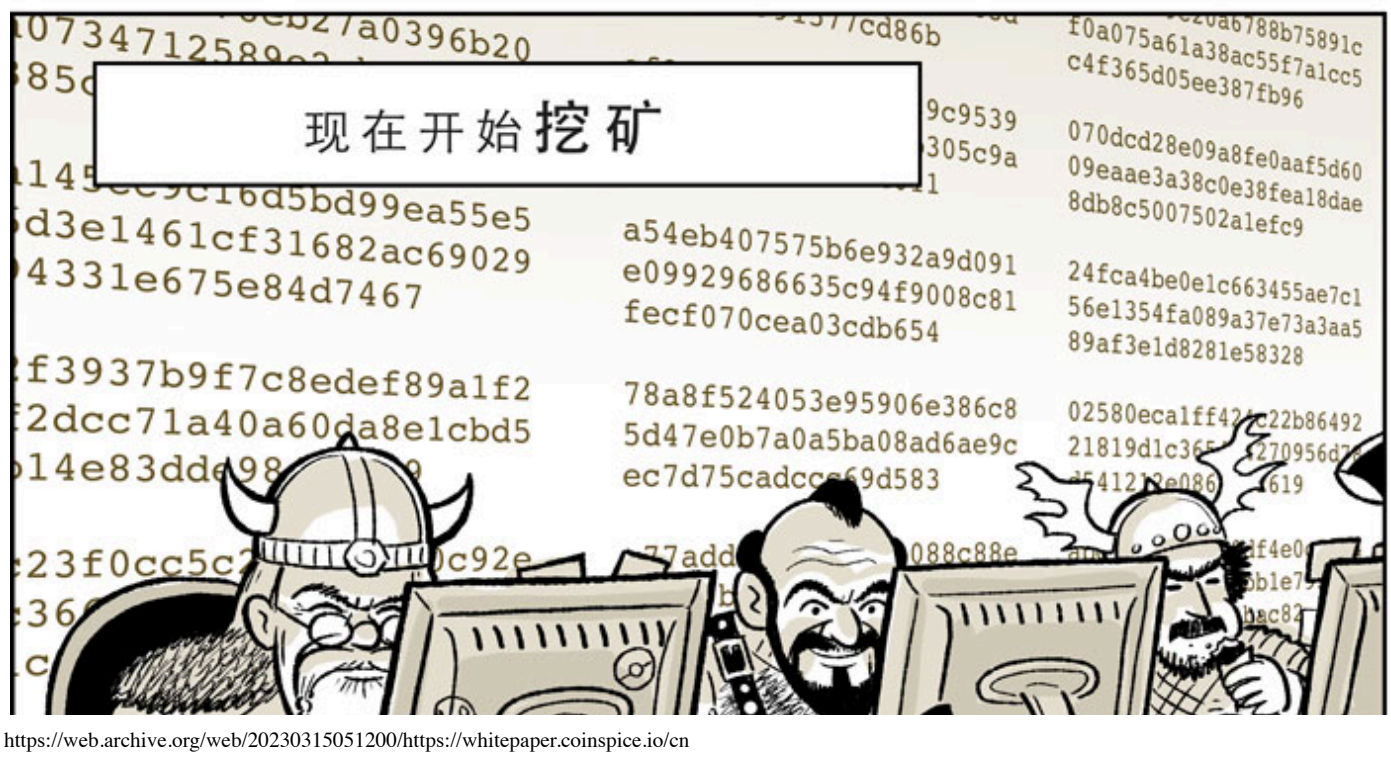

Input:
Previous tx:
c14ca9164792c453362a57f99235d58168908c5f85060030ddb2d4a00cfd2dd4
Index: 0
scriptSig:
26e6631530817fe35c2a42064b085e61934d8368bcc8c28385bf9fd2798f0f073d00
9e782c14ca9164792c453362a57f99235d58168908c5f85060030ddb2d4a00cfd2dd
4bb4cf5a
Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160
65b6be5ecb63294560df81492125483020634ea8
OP_EQUALVERIFY OP_CHECKSIG
看!
有人来了!
哦，我的天呢!
看到了各种
输入和输出。
还有钥匙。
还有上一笔交易
的哈希。


哇，感觉自己像是在
监督他人一样。
是真的正在某处
发生着一笔交易。
虽然对方的
住址和身份
全靠猜测


稍等!这一笔交易是价值50亿
美金吗？！
是的，但是是
50亿聪啦。
比特币的最小单位。
哦, 那也就是50美金。

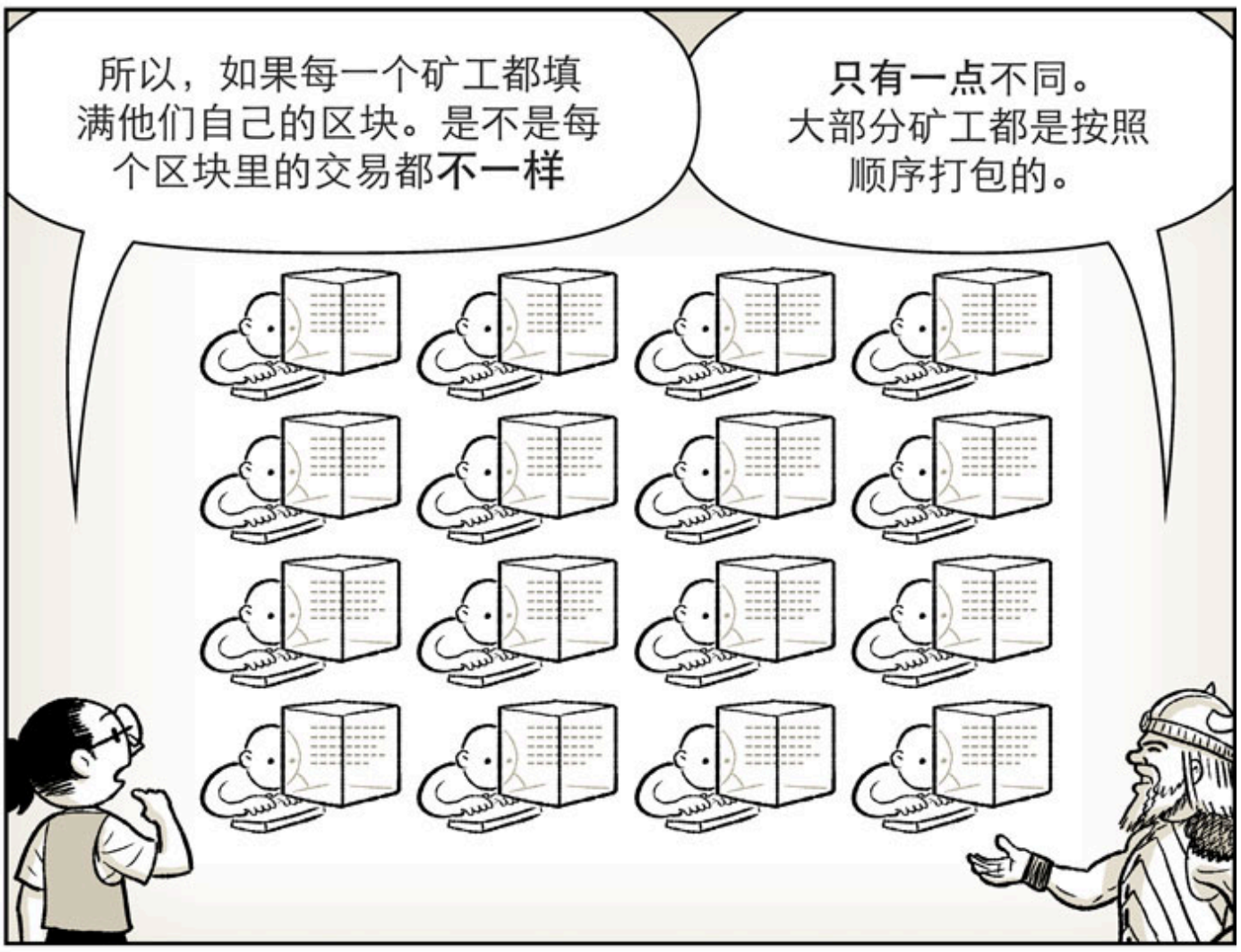

每时每刻都在减少，
一个没有任何感情，
不会终结的新交易。


但是用不了多久，
我们就把它们
打包到一个大区块之中。
6995fcf3


现在开始挖矿


我们似乎放弃了刚才的
比喻，难道不是吗?
嗯，是的，也
不能一直用一个比喻


但是我确实听到了block 这个单词
是的，小姑娘。区块链的构成要靠我们


所以，如果每一个矿工都填满他们自己的区块。是不是每个区块里的交易都不一样
只有一点不同。大部分矿工都是按照顺序打包的。


如果你发给Bob的交易这一次没有被打包进区块里，也会被打包进下一个区块的。
那什么才是可以胜出的区块呢？我可以获胜吗？


你可以。如果你可以解决一个特殊加密难题


呃，
听起来很多工作量呀
确实如此


工作就是把链打造起来的火。
工作就是最初的货币。
嗯，我听不懂啥意思。
RRAAAR!
WOO! HOO!


每个区块的成分都不一样。
包括已经被确认的交易。
NAKAMOTO


所以一个独立的区块头包括之前获胜的区块哈希。


默克尔根：一个包含所有交易哈希值的哈希。


各式各样的元数据


一个一次性的随机数，最后一个时间戳。


我们把所有的东西都揉碎在一起，使用特别强大的SHA-256加密算法。还有。。。
WHRRRR

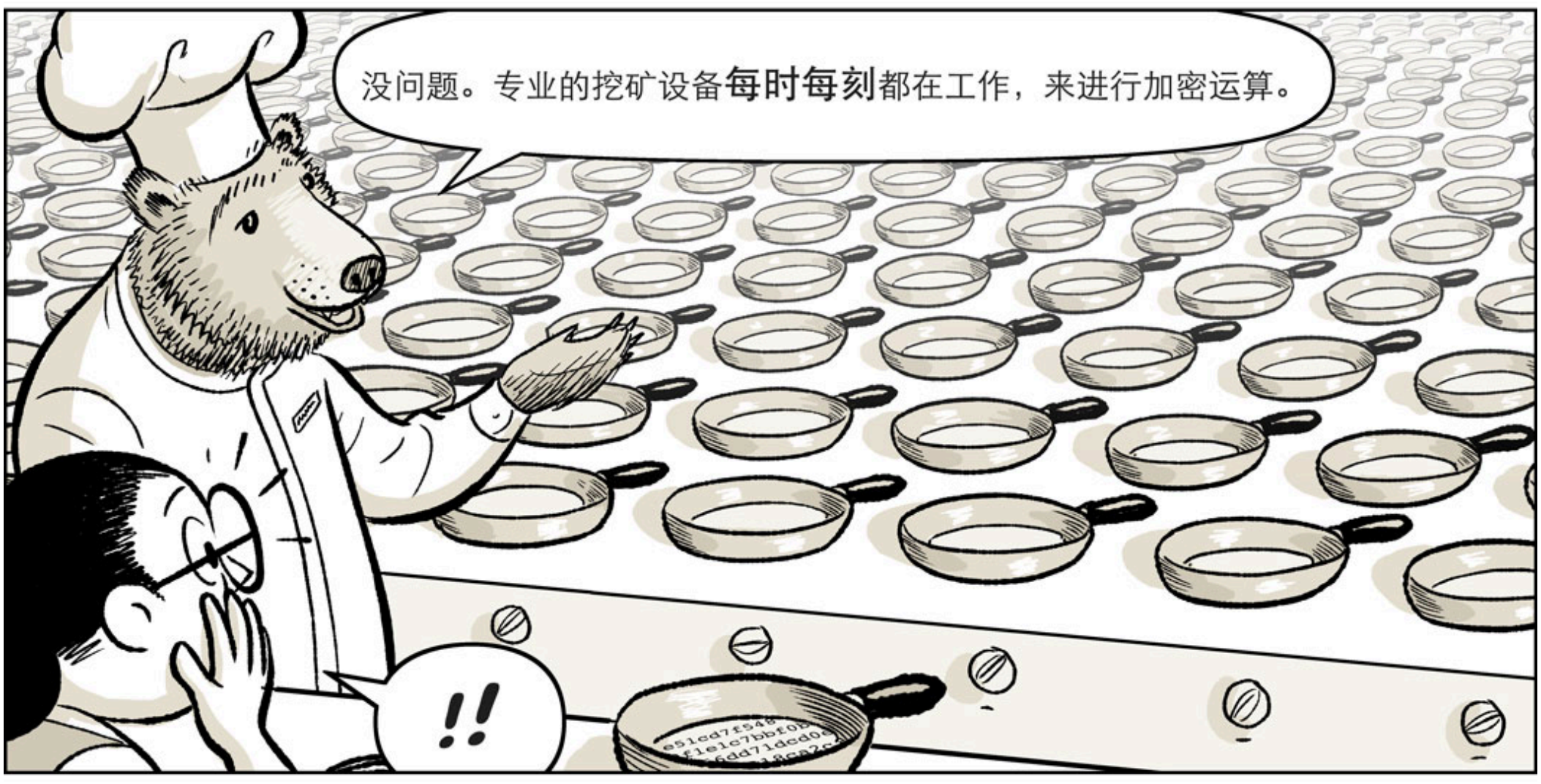

没啥。
你在找什么呢?


TICK
TICK
TICK
*NOT SALT


用个比喻，就是一个煎蛋，
用字面意思来说，
一个64位字节的字符串，
至少包含17个0。
e51cd7f548
780f1e1c7bbf0b
0da1156dd71dcd0e
56ead64218ca2c
67a62957da


这是不可能的
不是不可能，
而是
可能性很小。
再来尝试一次。


但是现在有了
一个新的时间戳，
一个新的随机数，
还有一个更好的结果。
不能够再让一个破碎的鸡蛋复合。


没问题。专业的挖矿设备每时每刻都在工作，来进行加密运算。
!!

现在你明白了为什么叫做**工作量证明**了吧

哎呦我去！**你**哪来的

初次见面，多多指教。我叫**中本聪**。

哦，好吧。

我早该猜到你是谁的。

如你所见，需要多个处理器“**工作**”来计算**加密难题**。

00000
000000000
0000e8fd1
0a42cf715
829f493fb
a37931ea2
32f479fe0
76ce6

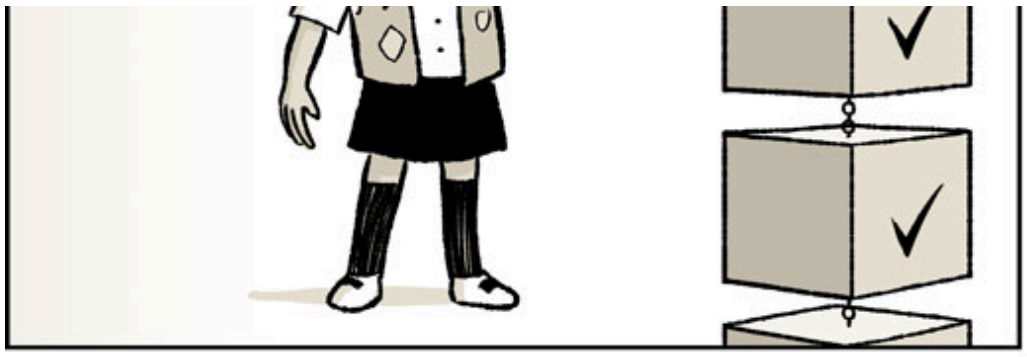
根据设计，每10**分钟**有**一个节**点可以获奖。如果加速或者减速，难度值会做出相应的调整。

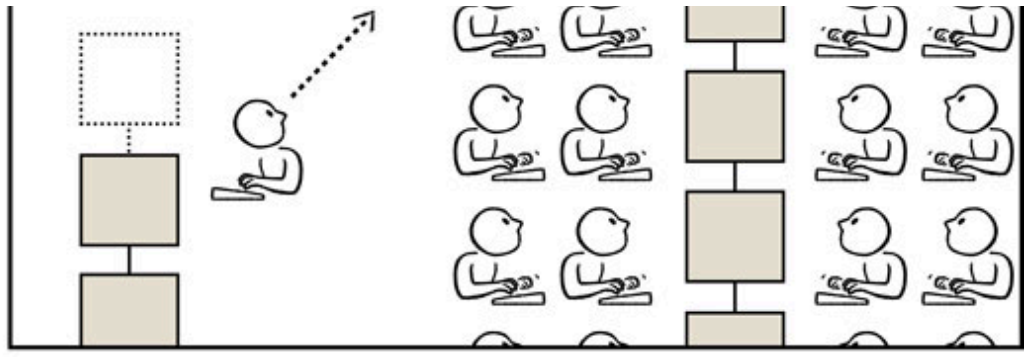
幸运的节点可以获得**新产出的比特币**（现在是12.5个，每四年减半。）其他矿工会检验结果。

数学检测出来后，他们就会开始争夺**下一个区块**的打包权，作为最新**被确认**区块的延伸。

节点通过贡献**电脑运算**来进行投票。

他们可以在任何一条链上搭建，但是跟其他人一样玩同一条链最符合他们自己的**经济利益**。





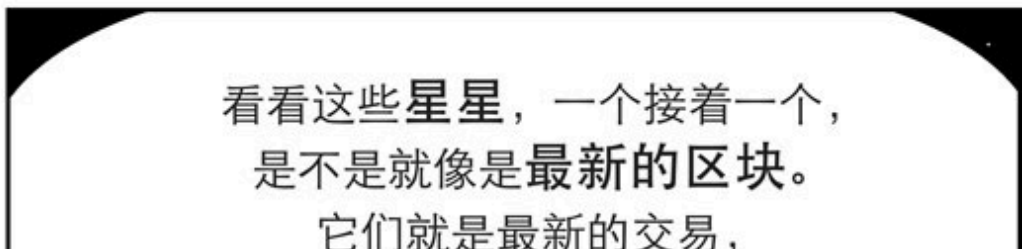

为什么呢?
因为这些新生成的币，即矿工奖励，

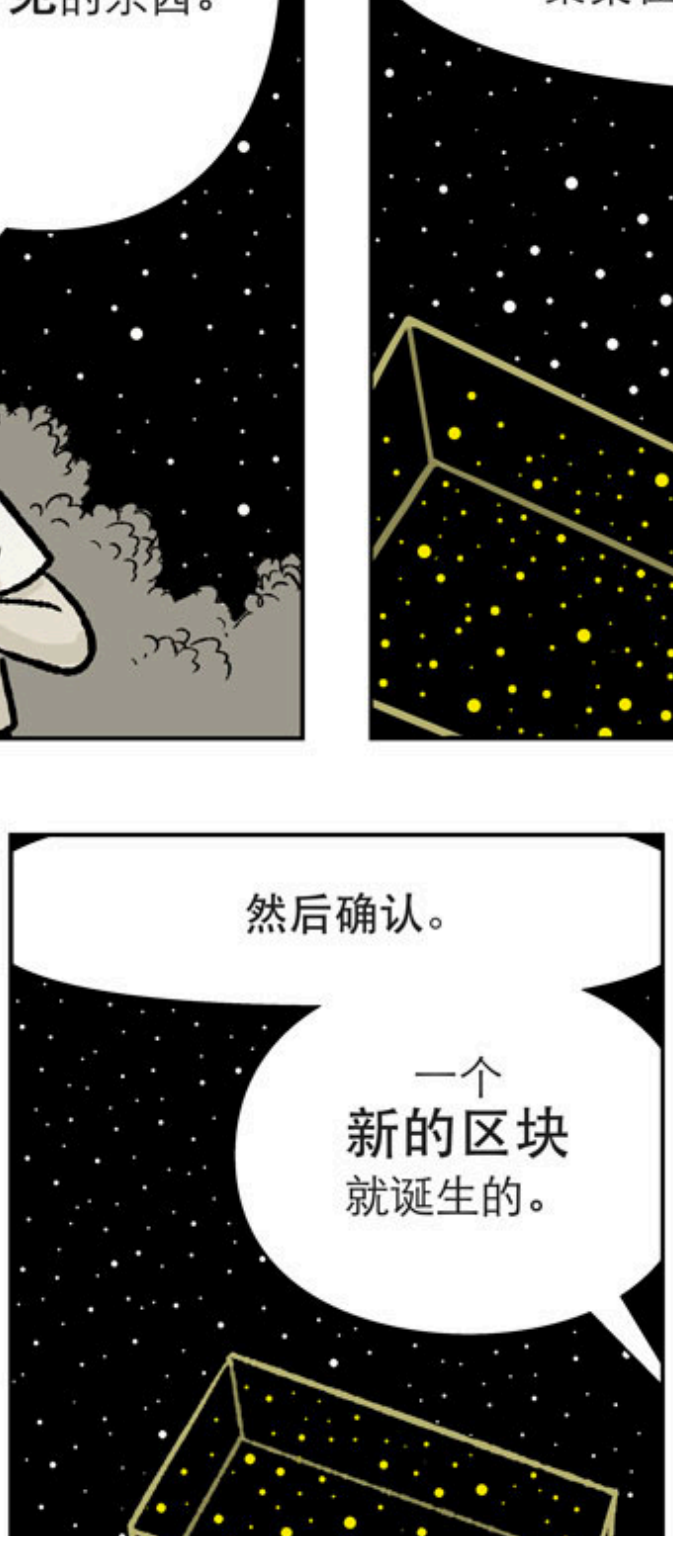

只有被共识链认可才有价值。
不然，

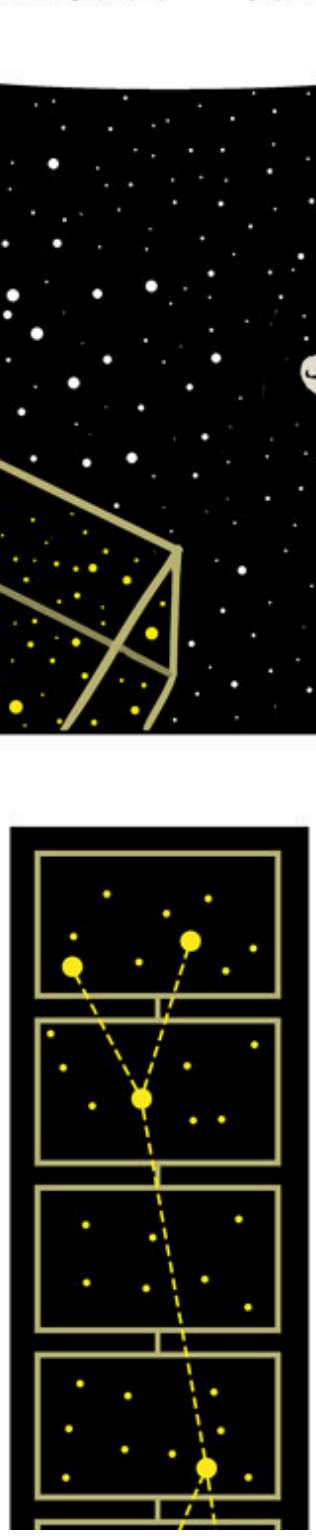

POOF
市场就不会认可他们。


即使贪婪的攻击者集中了大量CPU算力，那也是用来挖新的币比较划算，而不是攻击过去的交易历史。
个人利益，而不是信任，维持了整个系统。


想要信任任何人吗?
信任数学吧



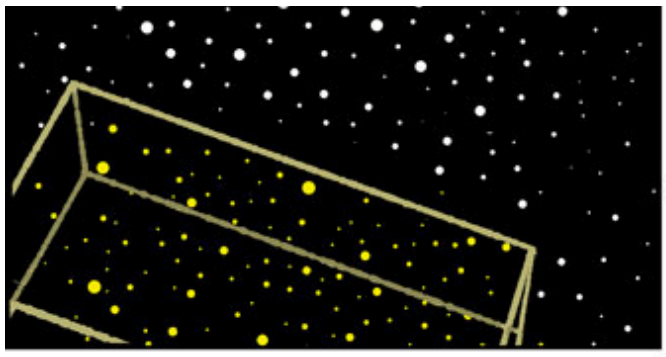


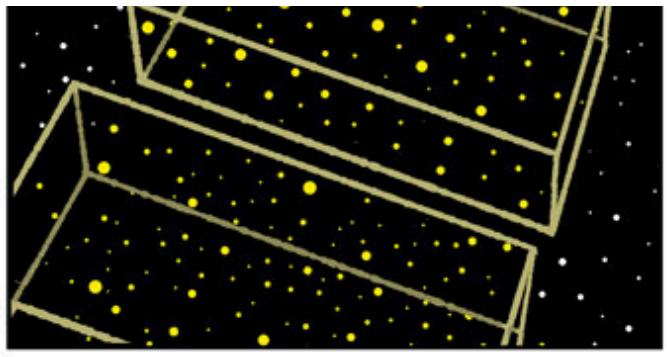


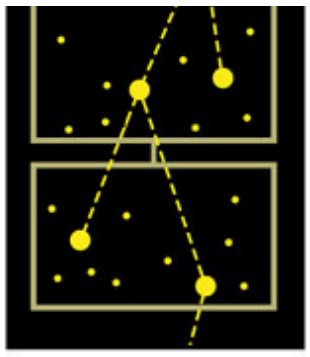
在这些区块里，
你会找到所有过
去钥匙的主人。

所有结合或者分
离的币从区块里
降级为区块奖励。

不管是9年前还
是最近的区块








最终：一个连贯的、透明的、点对点、只能添加新信息，任何人都可以添加新消息。但是任何人不可以进行更改。
试图更改任何小的价值，所有的哈希值都会更改，这就是蝴蝶效应。
但是如果真的有这么安全，怎么会有那个啥“mount”事件。


MTGOX是一家交易所，更准确的说是一家银行。大家把自己的比特币打到mtgox地址，这是个大错误。
啊

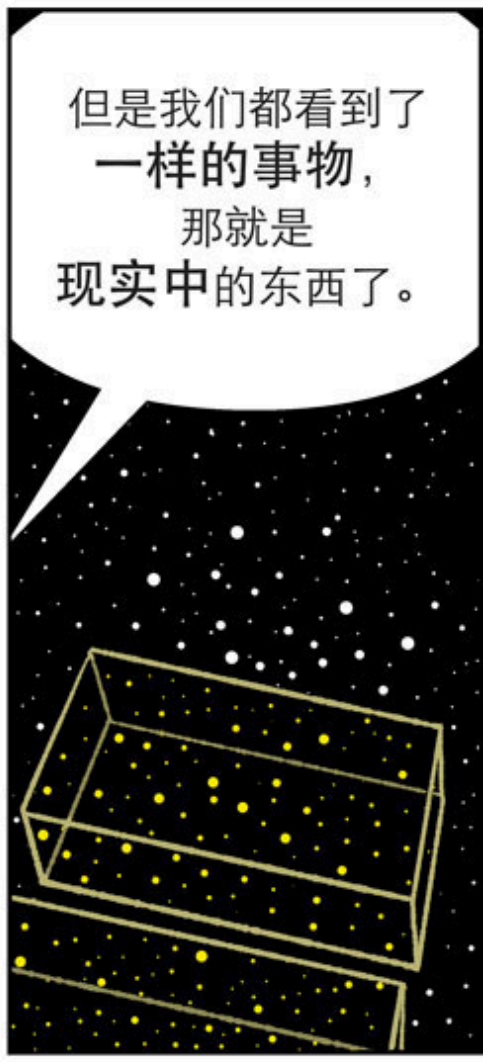

没有人攻击了这些钱。所以有人想要盗走它们。

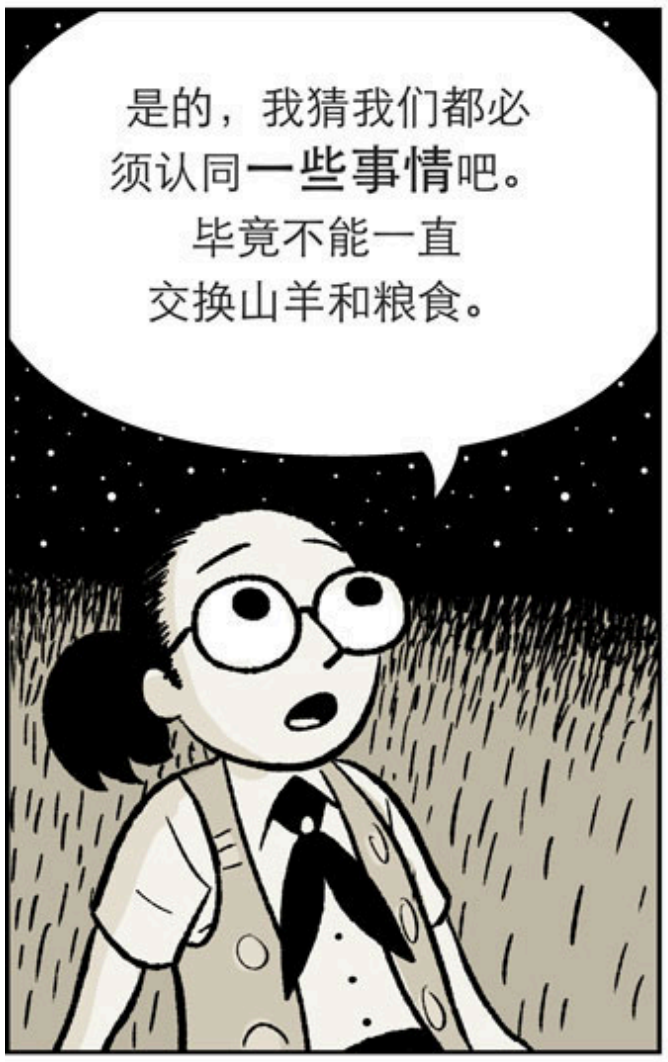

听说pow机制会消耗大量的电，是真的吗?
对的，
最近这个话题争议很大。


但是成本代价要衡量这个系统能提供的价值和功能。点对点的电子现金可以为世界各地的人带来福利。
使用。。价值。。。


钱真的
太奇怪了!
为什么所有的东西都有价值。好像大家都得了幻想症一样。


如果只是存在你的脑子中当然就是幻觉。

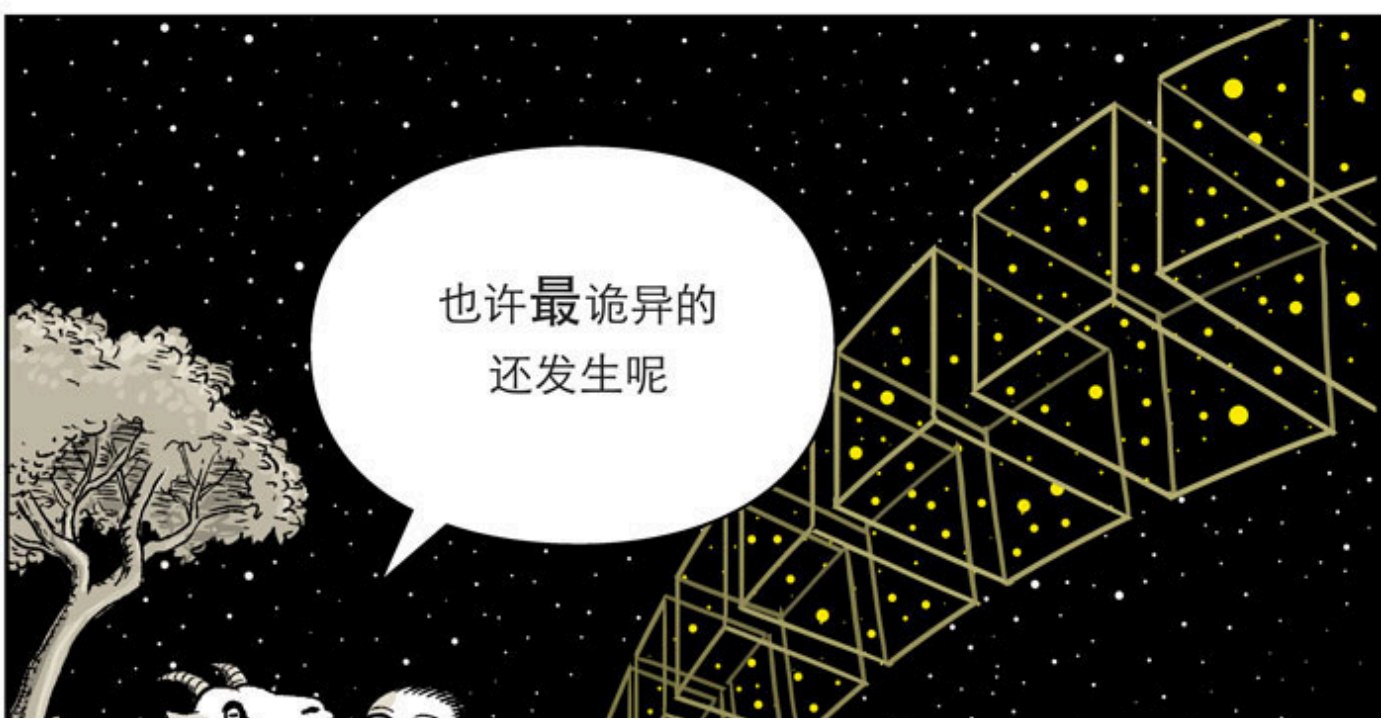

但是我们都看到了一样的事物，那就是现实中的东西了。


是的，我猜我们都必须认同一些事情吧。毕竟不能一直交换山羊和粮食。


我从来没想过世界居然能发生这么大变化。


金钱背后蕴藏着很多东西。


但，
确实，
金钱很奇怪


也许最诡异的还发生呢

了解更多

白皮书

下载比特币钱包

Reddit论坛

捐款

bitcoincash:pzycl4x2sc8z8rep6ex9x843qwucd7h3uvy0hrlmjc

Donate with Badger