

中饼之道

达哥微博精选

(2021.8-2024.11)

<http://weibo.com/btcdage>

<https://iris.to/btcdage>

nostr: npub17ahz4xa3hvkvvh4wguzzqknp8p7l5nyzzqc3z53uq538r5qgn0q40z7pw



@BTCdage

kwhh4wguzzqknP8p7l5nyzzqc3z5

I COME

I SEE

I HODL

@BTCDAGE

囤饼之道 达哥微博精选 (2021.8-2024.11)



引言

本书收录了达哥从 2011 年 8 月至 2024 年 11 月间对比特币及相关技术的深刻思考与探索。作为一个技术爱好者、早期实验者和坚定的比特币信仰者，达哥的历程不仅是个人成长的见证，更是整个加密货币领域发展的缩影。

从 2011 年第一次运行比特币挖矿软件，到 2024 年设计“聪之道”历史曲线工具，达哥经历了比特币的崛起、熊市的寒冬以及去中心化技术的兴起。他的笔记和文章涵盖了比特币技术、安全性、经济理论、DeFi 生态、去中心化协议等多个维度，是对区块链行业的深入解读，也是他对比特币自由理念的最佳注解。

2024 年 12 月 5 日，比特币价格首次突破了 10 万美元。这一历史性时刻进一步验证了比特币的价值，同时也彰显了去中心化资产在全球经济中的重要地位。

本书旨在记录这一段宝贵的旅程。通过这些文字，希望能为更多人打开通向去中心化世界的大门，让更多读者理解比特币的技术价值和信仰力量。

愿我们与达哥一道，在这条探索之路上继续前行。

囤饼之道 达哥微博精选 (2021.8-2024.11)

kvhh4wguzzqknp8p7l5nyzzqc3z53

目录

2021/10/6 16:06 脑钱包的安全性	1
2021/10/12 16:43 大饼的抗量子计算特性	3
2021/10/18 08:49 DEFI 的意义	4
2021/10/22 22:39 大饼的定投策略	5
2021/10/23 19:49 被动满仓	7
2021/10/27 11:55 大饼和黄金	7
2021/11/4 19:57 大饼什么时候卖	9
2021/11/10 10:15 历史选择了大饼	9
2021/12/6 15:59 以小博大	10
2021/12/25 18:34 韭菜三宝	11
2022/1/9 21:14 知道者悖论	11
2022/1/14 13:48 主观价值	12
2022/1/24 10:52 饼本位	12
2022-6-2 文化侵略	12
2023-1-11 nostr 协议	13
2023-1-15 nostr 中设置闪电网络收款地址	13
2023-1-16 《从 WEB1.0 到 WEB4.0》	18
2023-1-17 使用 nos2x 管理 nostr 私钥	20
2023-2-2 nostr 账户安全手册	23
2023-2-10 XMR 的问题	23
2023-2-17 如何安全私聊	24
2023-2-20 安全私聊自动化软件详细设计	24
2023-2-22 手动发起安全 nostr 群聊	26
2024-2-29 10:07 人类四大发明（发现）	27
2024-3-6 09:19 定投收益	27
2024-3-12 10:17 三·一二	29
2024-3-13 10:00 囤到底，月球见	32
2024-3-13 14:03 最好的货币	32
2024-3-15 16:18 高级脑疑问的相关思考	33
2024-3-16 17:44 以太坊脑钱包生成器	36

囤饼之道 达哥微博精选 (2021.8-2024.11)

2024-3-17 09:24 私钥安全启示录高级脑安全性探究.....	37
2024-3-21 16:49 比特币脑钱包生成器.....	38
2024-3-25 11:57 高级脑生成支持隔离见证的囤饼地址.....	40
2024-3-28 16:34 量子计算会摧毁大饼吗.....	44
2024-4-3 22:08 机遇.....	45
2024-5-5 22:47 以太坊虚荣钱包生成器.....	46
2024-5-31 15:05 《狐狸分饼》说开去.....	47
2024-6-13 11:33 放弃高考焦虑，囤大饼迎接未来.....	50
2024-11-1 15:45 桌面币价小组件.....	51
2024-11-14 20:04 达哥指数：用科学化指标预测市场热度.....	51
2024-11-16 11:44	55
2024-11-22 17:02 BBB聪之道BBB上线.....	56
2024-11-24 19:41 比特币的时代见证者：@囤饼达 达哥的探索与启迪	58
2024-11-28 14:58 冲击 10 万美元	61
附录（达哥制作的 AI 插图）	62
btcnage:	62
2024-2-20 23:06 纹身:	63
2024-2-21 11:21 上车:	64
2024-2-23 15:23 元宵节:	65
2024-2-23 19:26 万有引力:	66
2024-2-25 18:43 霸王龙:	67
2024-2-27 08:27 华尔街:	68
2024-2-28 19:06 方舟:	69
2024-2-28 21:23 回归 6W:	70
2024-2-28 23:22 兑人民币新高:	71
2024-2-29 10:07 人类四大发明（发现）	72
2024-3-1 10:48 见证奇点:	73
2024-3-4 00:14 阳光大道:	74
2024-3-4 11:37 性感叙事:	75
2024-3-5 20:21 囤饼达:	76
2024-3-5 23:05 新高 69K:	77
2024-3-8 00:11 三八节:	78

囤饼之道 达哥微博精选 (2021.8-2024.11)

2024-3-9 00:26 突破 7W:	80
2024-3-13 14:03 最好的货币:	81
2024-3-29 15:43 雉问:	82
2024-4-3 22:08 机遇:	83
2024-4-10 08:28 小事改变未来:	84
2024-4-20 08:11 减半:	85
2024-6-1 08:50 六一儿童节:	86
2024-6-10 09:31 端午:	87
2024-6-18 09:33 仕女图:	88
2024-11-21 12:04 比特牛:	89
2024-11-25 21:36 超级赛亚人:	90
致谢	92
版权声明	92
特别声明	92

囤饼之道 达哥微博精选 (2021.8-2024.11)



2021/10/6 16:06 脑钱包的安全性

今天聊聊脑钱包的安全性。

脑钱包原理上就是由用户自己定制一个复杂口令作为种子使用 SHA256 来生成私钥-地址对。脑钱包的口令需要满足两个条件：

- 1、 足够复杂，防止撞库（不能使用什么 password1234 之类的弱口令）
- 2、 足够好记，防止自己忘记（不要复杂到自己都记不住的结果）

虽然看起来两者矛盾，但是相对于随机生成的私钥纸钱包来说，脑钱包的确是牺牲一部分随机性来满足方便记忆的条件，拥有脑钱包，基本上可以做到人到哪财产到哪的境界。

一些 hodler 认为脑钱包是不够安全的，理由是，人类定制的种子不够随机，他们害怕自己的脑钱包口令被黑客采用字典碰撞的方式暴力破解。其实这是一种对黑客技能的误解，对于黑客来说，无非就是通过网络渗透获取信息或者字典撞库两种方案。

只要我们在离线环境中生成脑钱包，且保证口令的复杂性和保密性，私钥在需要时可以重新生成，且避免存储或泄露。那么，通过网络渗透入侵的路就已经完全堵死了。

实际上我们需要的是让脑钱包口令本身拥有足够的随机性即可防范字典撞库。

比如我们用脑钱包口令：“这是一个 BTC 达哥的脑钱包口令，但是我现在还不怎么安全”作为种子可以生成地址-私钥对：

```
15wzWHUJQZxf4xhTjir6GyTLQjsjxx6cFg  
5Jx1jLJKUhXWGviQf3CkJU2DN9BJ32MbeQHTZcedpqVhh1p2t2m
```

理论上，我们认为 SHA256 是安全无法撞库的（否则即使不用脑钱包，比特币系统也不安全），那么除非黑客的字典里存在明码“这是一个 BTC 达哥的脑钱包口令，但是我现在还不怎么安全”，否则，是不会通过撞库获取到比特币钱包地址：15wzWHUJQZxf4xhTjir6GyTLQjsjxx6cFg 的私钥的。

当然，正如同这个脑钱包口令本身所述，这样的脑钱包口令在安全性上仍然存在较大风险。

下面举一个例子来使用一个安全性较高的脑钱包（以下均为离线操作，有条件的话可以使用完全离线电脑进行。操作完成后清除浏览器缓存）：

我这里有两本书：

- 1、 中华书局出版《万历十五年》2006 年 8 月北京第一版。
- 2、 江苏文艺出版社《厚黑学》2009 年 11 月第一版。

取《万历十五年》103 页最后一段第一句话：

“起初，万历皇帝还没有意识到事态的严重，他以为对张鲸作一番口头申诉就足以了事。”作为字符串 A。

《厚黑学》109页最后一段第一句话：

“一个国家之进化，也好比小孩一天一天地长大。”作为字符 B。

第一步：用字符串 A 生成私钥 A。

起初，万历皇帝还没有意识到事态的严重，他以为对张鲸作一番口头申诉就足以了事。

----->5JUf9k1VgXmLP37EEsMWV5i11oFYkHhiR8fNiFR6x37BY6ugaPP

第二步：用字符串 B 生成一个私钥 B。

一个国家之进化，也好比小孩一天一天地长大。

----->5KSgM4vYWNSDYDpHKMS5Py7FDAPa7dtgT7pReSqGPLg2irNCGch

第三步、将私钥 A 与私钥 B 使用连接字符串“我是 BTC 达哥的第 N 个安全私钥”连接起来，生成我们需要使用的私钥地址对，记下生成的地址，私钥不记录（不记录才安全）。

5JUf9k1VgXmLP37EEsMWV5i11oFYkHhiR8fNiFR6x37BY6ugaPP 我是 BTC 达哥的第一个安全私钥 5KSgM4vYWNSDYDpHKMS5Py7FDAPa7dtgT7pReSqGPLg2irNCGch

----->

地址：1EQxBpa3ng3oLu419Guoql76Kjx4CTtJeL

私钥：5KQgXaHW9eE4FbQY621BmT27TYoBMfGTgAEan1cWqcqgHYgJVA7

5JUf9k1VgXmLP37EEsMWV5i11oFYkHhiR8fNiFR6x37BY6ugaPP 我是 BTC 达哥的第二个安全私钥 5KSgM4vYWNSDYDpHKMS5Py7FDAPa7dtgT7pReSqGPLg2irNCGch

----->

地址：16KU65mJiCJTXW1oucxz68ZdLfYNq8pzL

私钥：5JFNxAACoMvd8cSxJysHPvweUFpVySPAQpdP2qTZAudFNerHHYv

5JUf9k1VgXmLP37EEsMWV5i11oFYkHhiR8fNiFR6x37BY6ugaPP 我是 BTC 达哥的第三个安全私钥 5KSgM4vYWNSDYDpHKMS5Py7FDAPa7dtgT7pReSqGPLg2irNCGch

----->

地址：1H2gEob2yANVEQRvbWYkehSNNDXgVi5NSX

私钥：5KPvGn2HSQK9EZvwKcDeNJUDP2g9CV4Ndqn1oSrpBhV7CR5vF4g

上面就生成了 3 个足够安全且只有自己知道“生成方法”的大饼地址，我们只需要记下地址，私钥不用记。以后需要的时候重新生成一次私钥即可。

然后我们只需要在本本上记下（当然也可以记在脑子里）并备份到多个物理地点：

- “
1、中华书局出版《万历十五年》2006 年 8 月北京第一版 103 页最后一段第一句话
2、江苏文艺出版社《厚黑学》2009 年 11 月第一版 103 页最后一段第一句话
”

然后你把下面事项牢牢记在心理：

-
- 1、两个私钥用连接词连接以后作为种子生成私钥；
 - 2、连接词是“我是 BTC 达哥的第 N 个安全私钥”，N 是变量，以生成多个地址。

多亏了 SHA256 算法，这个世界没有任何黑客字典或其他碰撞方式可以破解这样的脑钱包口令，除非你自己告诉别人。

而且，这种方式比一般的纸钱包要安全的多，毕竟即使泄露了本本上的两句话，别人也无法得知你的种子生成方式及连接词是什么。

当然我这里只是一个例子，发挥你自己的想象力，可以创造出更好更安全的脑钱包口令生成和保存方式。

2021/10/12 16:43 大饼的抗量子计算特性

今天聊一聊大饼的抗量子计算特性。

前段时间和@比特币布道者 探讨了下大饼的继承性问题。因为在我们的价值观中，大饼是可以长期永久的持有下去。然而近期看到一个视频，任正非老总侃侃而谈，说大饼没有实际价值，最终将一文不值，理由是大饼的算法最终会被未来的量子计算机破解。由此，大饼没有长期持有的价值。

大多数对大饼没有深入学习的人，都会有这样一个认识，就是既然大饼完全开源，他的公钥是由私钥采用椭圆曲线加密算法 (SECP256K1) 所得。即使以目前的计算机算力而言破解难度很大，但如果量子计算机有一天进化发展到可以破解，导致 SECP256K1 被破解，到那个时候，任何公钥都可以用量子计算得到对应的私钥，大饼网络岂不是立刻崩溃？大饼就是建立在沙上的城堡，长远来看大饼的价值十分存疑，囤饼的理论基础就不存在了。

这样的认识很有普遍性，你猜怎么着，实际上中本聪早已未雨绸缪，给我们挖好了护城河。

当我们用一个 256bit 的随机数作为私钥，使用 SECP256K1 获得“公钥”（具体算法与本文无关不在累述）后，大饼网络并不直接使用这个“公钥”做为钱包地址，最主要的原因并不是很多人以为的“公钥”太长不好记，而是因为 SECP256K1 算法不抗量子计算。

得到了“公钥”以后，会进行 SHA256 算法和 RIPEMD160 算法的两次哈希套娃，得到的哈希值前面加上大饼网络版本号，获得一个字符串 A。

对字符串 A 再次进行两次 SHA256 套娃，得到的哈希值取头部 4 个字节，连接在字符串 A 的右侧，此时获得字符串 B。

将字符串 B 做 base58 编码，就得到了最终我们熟悉的“大饼地址”。

熟悉加密算法的朋友可以一眼看出，在多次连接字符串与哈希套娃之后，已经不可能从“大饼地址”反推出原来的“公钥”。也就是说，由于哈希算法“丢失信息”的特性，无论多么牛逼的

量子计算机，也是无法从一个丢失信息的“大饼地址”字符串破解反推到“公钥”（即使有能力碰撞破解出来的伪公钥也是无用的）。所以，在“公钥”未暴露之前，如果你仅仅是将“大饼地址”用来提币围饼，那么，你的大饼资产是完全安全无需顾虑量子计算的威胁的。

值得注意的是，如果你从你的大饼地址往外转账，那么，你的“公钥”信息就将暴露在大饼网络中，此时，抗量子计算的特性也就失效了（但是别忘了还有 SECP256K1 保护着你）。

所以中本聪设计了大饼的找零机制，当你从一个地址往外发送一部分大饼时，剩余的大饼也会转移到一个“找零地址”中去，也就是说为了保障账户的抗量子计算特性，一个大饼地址只用（转出）一次。很多科普的文章都没有指出这一点，甚至有一些教程为让你把大饼钱包软件的招领地址设置与发送地址一致，这就是忽视且浪费了大饼网络的抗量子计算安全性。因此，在这里达哥郑重的建议将找零地址设置为自己另外一个没有往外发送过饼的脑钱包。

结合之前的脑钱包讨论，希望大家都能安全的围住自己的大饼。

2021/10/18 08:49 DEFI 的意义

突然发现很多大佬昨天都在聊关于 defi 的话题。@暴走北纬 @玛雅 cndx @超级冰糖橙 恰巧昨天我在一个围饼群里也因为这个话题发生了激烈的讨论。

有些 holder 固执的认为 defi 就是骗局，eth 必然归零：其实这是认知没有与时俱进的表现，正如一位群友所说：“以 uniswap 为首的 dex 对币圈的发展非常有意义。”

显然，很多人对 defi 的误解源自于自身认知的不足，defi 的存在让各国政府明白，他们就是动用权力关了中心化交易所，也无法阻挡加密资产的交易流动。就像各国政府知道无法关闭大饼，所以才不对其他币动手。9 神的《围“大饼”》里说的好：否则私发货币是死罪。

可见 defi 对饼圈的发展是起到积极的作用的，我个人定投很多就直接在 dex 里用 u 购买，完全不担心 cex 是否关闭。

在 dex 里做市商（或者在其他类型的 defi 中质押自己的 U 或者饼或者其他币种菜），赚取的是矿币，矿币可以持有看多，可以锁仓套娃，可以卖出套现，当然也可以直接换饼（我经常的做法）。

有个群友说，“为什么要用毫无价值的矿币去骗取别人的饼，为什么不用法币清清白白的买饼”这就是认知有偏差，用自己的资金锁仓，其实是用“机会成本”换取矿币，用矿币在 dex 中交换 U 或者饼，和用自己的体力脑力工作换取的法币买饼，在道德上的高度是一致的。

按奥地利学派经济学理论来说，交易的本质，就是用自己觉得“不值”的东西去换别人觉得“不值”但是你觉得“值得”的东西。也就是说，价值是主观的，一个东西有一个公允的价格其实是大多数人主观上认为其价值的重叠。

别人拿饼换取你的 U，拿 U 换取你的矿币，拿 U 换取法币，都是别人自愿的，谈不上什么骗取。否则也可以理解成别人用饼在骗你的法币了。或者你在用法币骗取别人的饼。

至于 ETH 会不会归零，万物都会归零，宇宙终将热寂智能合约主链 ETH 目前还是龙头，eth2.0 进入 pos 会怎么样目前还无法得知。有信息就持有，没信心就卖出，没必要争论，更不要攻击不同意见者，否则会显得你既极端又很 low。

最后使用另外一个群友说的笑话结束：

一个人走過海旁，看見另一个人想跳海自殺。

他走上前去勸說「先生，不要跳下去！」

那人問道：為甚麼？」

他說：生命是美好的嘛！你是無神論者還是有宗教信仰？」

那人答：我有宗教信仰。

「佛教、道教、回教還是基督教？」

「基督教」

「羅馬天主教還是新教？」

「新教」

「我也是新教呢！聖公會還是浸信會？」

[浸信會]

「太好啦！我也是浸信會，你是 Baptist Church of God 還是 Baptist Church of the Lord？」

[Baptist Church of God.]

「真是太奇妙啦！我也是，那你是原教旨的 Baptist Church of God 還是改革派的？」

「改革派的」

[1879 年的改革派還是 1915 年的？

[1915 年的改革派。]

那人朝他屁股一腳把他伸進海裡：異端！去死吧！

2021/10/22 22:39 大饼的定投策略

今天聊一聊大饼的定投策略

★请注意★

如果你

1、不认同大饼的未来价值与四年牛熊转换周期规律

2、不认同与时间做朋友慢慢变富

3、资金雄厚，直接梭哈，无需定投

可无视这篇文章。谢谢。

定投的目的是在长时间跨度中（至少 4 年一个周期），以比较合理的法币成本增加饼本位收益。定投也是战胜人性弱点增持大饼的最好方式。一旦进入饼本位思维，坚持定投，那么你将再也不会担心饼价下跌，因为便宜打折的饼可以让我们用一定量的法币换到更多的饼，美滋滋。下面是定投的几种常见方式。

【策略一】

无脑定投：

1、每个月固定日期，投入固定数额（或流动资金比例）的法币购买大饼，无视价格和其他指数。

2、可在定投之前，一次性买入小部分底仓（不超过总预算资金的 30%），比如先买上 0.28BTC，也可以略过建立底仓这一步。

优点：最简单的策略，无视价格和任何指数等因素，因此最容易施行。

缺点：定投成本可能会高于其他策略

适用：囤饼新人，简单实用，存饼才是存真正的钱。

【策略二】

ahr999 指数定投：

- 1、ahr999 < 0.45 抄底梭哈。
- 2、0.45 < ahr999 < 1.2 激活定投，每月固定日期投入固定数额的法币购买大饼。
- 3、ahr999>1.2 时，暂停定投。

优点：较为简单，固定日期观查 ahr999 指数后决定操作方式即可。

缺点：ahr999 低于 1.2 越来越难，有踏空风险。

适用：已拥有部分大饼底仓，想要继续低成本增加币本位收益的朋友。

【策略三】

金字塔定投：

- 1、从目前历史最高点开始，每跌 10%（按第一次跌破的时间），投入一部分资金，每次投入的资金翻倍。

比如目前大饼历史高点 67000.

第一次跌至 $67000 \times 0.9 = 60300$ 立刻投入 1 份定投资金
第一次跌至 $67000 \times 0.8 = 53600$ 立刻投入 2 份定投资金
第一次跌至 $67000 \times 0.7 = 46900$ 立刻投入 4 份定投资金
第一次跌至 $67000 \times 0.6 = 40200$ 立刻投入 8 份定投资金
第一次跌至 $67000 \times 0.5 = 33500$ 立刻投入 16 份定投资金
第一次跌至 $67000 \times 0.4 = 26800$ 立刻投入 32 份定投资金
第一次跌至 $67000 \times 0.3 = 20100$ 立刻投入 64 份定投资金

- 2、如果大饼创下新高，则以最新价格重新开始计算价格重新运行本策略。

- 3、如果大饼连续数月在某价格区间波动，则每月固定日期按当前价格段的份额数量买入大饼一次。

优点：定投成本较为优化，因按价格安排买入点，可提前在 CEX 挂单。价格是越低越买，持仓成本低。

缺点：较为复杂，需要预先规划好投入的资金总量，进行份额分配，如果大饼在 2025 年之前不进入深熊，则能囤到的饼较为有限。有踏空风险。

适用：已拥有部分大饼底仓，短期看空后市，认为大饼本波牛市已结束的朋友

【策略四】

ahr999 改良定投：

- 1、每月固定日期操作，若 ahr999 指数低于 1.2，投入 1 份定投资金，低于 0.45，抄底梭哈。
- 2、ahr999 指数>1.2 的情况下，若币价 ≥ 50000 ，每月投入 1/4 份定投资金；若币价 < 50000 ，每月投入 1/2 份定投资金。
- 3、可在定投之前，一次性买入小部分底仓（总预算资金的 30% 或者 0.28BTC），以防踏空。

优点：同策略二，但不容易完全踏空

缺点：较为复杂，需要预先规划好投入的资金总量，进行份额分配，持仓成本略高于策略二

适用：已拥有部分大饼底仓，认为永恒牛市已经提前到来的朋友。

【策略五】

鸡尾酒定投：

策略三与策略四的结合体，两个策略一起执行

优点：对冲了策略三和策略四的踏空风险与持仓成本过高风险。

缺点：相对复杂，需要预先规划好投入的资金总量，进行份额分配，不利于新人操作。

适用：已拥有部分大饼仓位，对市场较为关注能克服人性弱点的朋友。

可按自己的偏好选择定投方法，无论用哪种方法，都要坚持(至少 4 年)，2025 年之前可能是最后一次定投机会，千万不可以半途而废，共勉之。

2021/10/23 19:49 被动满仓

好问题，个人认为囤饼投入不要超过总资产的 30%，20%当然也是很合理的，其实对于刚刚开始接受大饼的新人来说，用 10%的资金进入已经是算比较 open 的了，要知道，绝大部分人还是麻瓜的状态。随着深入的学习，认知程度越高，就越能接受饼才是真正的货币这个概念。

如果低于 10%稍显保守(但比没有好，10 年以后，有饼和没饼是两个世界)，但无需超过 30%，因为这是一个心理比较舒服的点，不太会因为饼价的短期下跌而影响生活质量和造成太大的心理压力，避免重蹈 48 万哥的覆辙。

其实，哪怕只投入总资产的 10%，10 年以后，你会发现拥有的大饼价值已经占你总资产的 90%以上。这就是“被动满仓”的定义。

2021/10/27 11:55 大饼和黄金

那今天聊聊大饼相对与黄金的优势吧。

1、黄金的稀缺性不如大饼

虽然黄金是贵金属，实际上地球的黄金储量大约有 60 万亿吨，只是由于大部分处在地心附近以现有的人类技术无法开采。通过火山喷发等地壳运动，部分黄金移动隐藏在地壳浅层中，成为可开采的金矿。黄金的稀缺性主要是由于勘探和开采的成本太高，在已探明的金矿中，开采量主要受制于开采成本，黄金的价格如果降低，则开采黄金的动力不足，进入人类金融系统增量就减少；如果黄金的价格增高，则会激励人类增加投入去勘探、开采，增大黄金的产能，结果会稀释了黄金的价格，因此黄金的价格长期相对稳定。

大饼由于算法确定了总上限不会超过 2100 万个，是真正意义上的稀缺。要想更改这个上限，

必须要让这种“反共识”的算力超过总算力的 51%，这在当前总算力规模下已经不可能实现。大饼的世界里代码即法律，丢失了私钥，则对应的饼就永久锁死在网络中不可用（至少 400 万以上的大饼已经被遗失锁死）。因此大饼的总量只会通缩。

大饼网络每新增 21 万个区块，区块奖励的大饼数量都会减半，这就是我们通常说的 4 年减半一次（21 万个区块时间大约就是 4 年）。

从 2008 年开始的创世区块到 2012 年第 210000 区块，每个区块都给矿工奖励 50 个大饼。

从 210001 区块到 2016 年的 420000 区块奖励减半为 25 个。

从 420001 区块到 2020 年的 630000 区块奖励减半为 12.5 个。

从 630001 区块到 2024 年的 840000 区块奖励为 6.25 个。

以此类推，2024 年 840001 区块开始，每个区块的奖励会变成 3.125 个。

（可能因此在 2025 年左右触发奇点事件，开启永恒牛市）

有意思的是，大饼增量越来越少，却不会像黄金那样会随着总算力(开采成本) 的增加而变化，无论人类因为大饼的价格增高而堆砌多少算力，只会抬高大饼的生产成本，却无法增加哪怕 1sat 的大饼增量。因此，大饼具有的是真正的稀缺性。

曾经有人说大饼可以无限分割，所以它就没有稀缺性，这就是无稽之谈，首先大饼并不可以无限分割，它的最小单位是 sat (聪)，1 饼=1 亿聪。而且分割性和稀缺性没有任何关系，黄金可以分割到原子级别，并不影响 1kg 黄金的价值。无法认知到这点，坚持认为大饼无限分割不具有稀缺性的人，可能是智力发育有所欠缺。大家离他远点。

2、黄金的防伪性不如大饼

现在想买到真正的黄金是很难的，我们甚至经常看到新闻从某银行买的黄金可以吸磁铁。连银行都不可靠，那么普通人想买到货真价实的十足真金就太难了。

大饼网络中则不可能有假饼。只要能提上主链网络就一定是真大饼，就这么简单。

3、黄金的隐匿性和可携带性不如大饼

有人说“盛世地产乱世黄金”，指的是黄金具有人类价值共识和容易携带（相对于不动产）的特性。但是黄金毕竟是物理世界的产物，隐匿性很差。目前价值 1000 万人民币的黄金就重达 27 公斤。想象一下战乱期间，你驮着沉甸甸的根本无法藏匿的黄金，走到哪里都是一块赤裸裸的肥肉，能捱到和平地区不被谋财害命完全靠造化。

大饼就不一样了，采用脑钱包方式掌控私钥，身上可以不带任何硬件，做到 0 物理负载。人到哪，资产就到哪。更优秀的是，由于人饼合一，逃难时你在外表上和其他难民没有任何区别，亡命之徒无法得知你身携资产，也就不存在被盯上谋财的可能性。

4、黄金的可交付性不如大饼

比如伊朗要从英国某公司购买一批物资，由于无法使用银行交易（美国制裁），提出用黄金交付。那么将黄金从德兰黑运往伦敦，需要大批武装安保和大量的运输时间。如果用大饼，则 10 分钟上链，30 分钟确认结算。完胜黄金这种笨重的物理介质。

大饼以上所述特性对黄金具有压倒性的优势，唯一的劣势就是相对于黄金数千年的人类

囤饼之道 达哥微博精选 (2021.8-2024.11)

共识，大饼还是一个新事物，不了解其优点的人还很多，总体人类共识还处于低点。但也正是如此，目前的大饼价格还是被严重低估，所以我们现在还有机会去定投。等到大饼人类共识上升到一定阶段，1个大饼甚至0.1个大饼就是普通人高攀不起的存在了。

2021/11/4 19:57 大饼什么时候卖

今天聊到了大饼什么时候卖的话题。

有人说等大饼到了多少多少价位就可以全卖了。

其实这还是错误的停留在了法币本位思维。

首先要确定的是：囤饼至少要经历一轮牛熊，从囤饼开始四年内是绝对不可以卖的，否则就会重蹈48万哥的悲惨覆辙。

饼本位观念中，法币是持有就会不断贬值的badmoney，而饼这种goodmoney是没有理由去换badmoney的。在任何以法币兑换汇率的“价位时间点”去清仓大饼都是没有必要的。

那什么时候可以卖饼呢？当你有必须的消费需求（囤饼人时间偏好低，很少会有购买奢侈品之类的不必要消费），且法币现金流已经无法覆盖时，才是卖出饼的唯一理由。

比如你现在有个必须的消费需求，还需要100万法币的现金流缺口。此时你可以卖出市值100万法币的饼，来支持你这笔必须的消费。

看出来了吗？将大饼这种goodmoney兑换成购买力会不断降低的badmoney的唯一用途就是：立刻将badmoney消费出去。

除非消费需求完全覆盖了你所有大饼的市值，否则你永远无需清仓大饼，哪有把goodmoney换成的badmoney这种傻事。

有人会这么做，只是因为他们观(zhen)念(ta)不(ma)同(sha)罢了。

2021/11/10 10:15 历史选择了大饼

每当我在说大饼是真正的货币，健全的货币，地球上最硬的资产时，会有这样一种声音：你说这玩意是真的货币这么牛逼，为什么还要用美元来定价啊？

首先要确定的是：货币只是一种特殊货物（通货），只是这种特殊的货物除了“交换别的货物”以外没有自身应用，它不能吃也不能穿。货币的价值在于：一定单位的这种通货能够交换其他货物的份额，也就是所谓的“购买力”大小。

解释一种货币购买力最容易让人理解的方式，就是用另外一种大家熟知的货币的购买力的比较，人们把这种比较称之为“汇率”

比如我们今天用人民币买精肋排是 50¥一斤，而在美国则是 3.62\$一斤

$$50/3.62=13.81$$

$$3.62150=0.0724$$

从¥本位来看，美元的购买力在中国就是 13.81

从 U 本位来看，人民币的购买力在美国则是 0.0724

当然，如果你要在美国购买东西得先按国际汇率把¥换成\$才可以。用美元在中国买东西也得把\$换成¥。

(聪明的你肯定发现国际汇率和实际购买力不符，对吧

这种人为的因素由于众所周知的原因我们不便深入讨论。)

这个例子说明，并不是大饼在使用“美元定价”，而是我们在交易所看到的不断更新的“大饼价格”，仅仅是显示出“当前时刻大饼的购买力”对标“美元本位购买力”的汇率而已。

有人说，大饼的价格是虚的，你能拿他去买东西吗？

且不去说萨尔瓦多这样的主权国家已经将大饼规定为法定货币，可以通过闪电网络很方便的购买物品。及时不提这些，请记住，大饼的价格是“购买力的汇率”，是实实在在的。美元也没法直接在国内买东西，但是你可以通过把美元按汇率兑换成人民币的方式获得购买力。大饼也一样，可以通过按汇率兑换成各个国家的法币的形式获得相应的购买力。

区别在于，你持有法币，购买力在不断的下降。

而大饼的购买力虽然有着波折起伏，然而，大趋势总是一路向前的，这一点从大饼的汇率历史曲线可以证明。

套用一句高大上的话：是历史选择了大饼。

2021/12/6 15:59 以小博大

今天看到凉兮的合约又亏完发飙的视频。

群里也有些合约亏损较多的朋友，锲而不舍的存钱、合约、亏完，不停循环。

我在思考，为什么他们不愿意拿那些钱去做围饼这种确定性极强的事情呢。

人人都说围饼致富太慢，不如合约是以小博大“以小博大”，多么诱人的一个词。

你们真的知道什么是“小”，什么是“大”吗？

比如 10 万人民币，是大还是小？

如果 10 万元相对于你围饼的资金来说，仓位占比很小

那么去玩玩合约以小博大尚能理解，因为即使你爆仓也无关痛痒。没错，这个“小”字，应该是你仓位大小。

如果 10 万元已经是你的资产的大仓位占比，那么玩合约就不符合“以小博大”的原则，而属于梭哈赌博，基本上就是在给市场送钱。这就是对大小概念理解偏差导致的决策性错误。

记住，任何人做任何事都应该做好风险评估

风险/收益比较小的大仓位做

风险/收益比较大的小仓位做

风险/收益比过大的事情就不值得做。

梭哈赌博 99% 的概率是完全亏损，一个有理性的人是不会做这个选项的。

哪怕你运气爆棚如年初凉兮，成了那 1% 的幸运儿，也会和他一样在接下来的操作中亏完崩溃。

其实，10 万元买 0.32 个饼，围上个 10 年，何尝不是一种确定性极强的以小博大呢。

2021/12/25 18:34 韭菜三宝

都说韭菜有三宝:抄底梭哈割肉跑。

我们知道，数月、甚至一两年内的短期行情实际上是不可精确预测的(planb 就是例证)。然而所谓的机构也好，主力资金也好，他们的长袖善舞的极限，也就是在这样一个时间段内而已。毕竟长期趋势是不受人为控制。

绝大部分散户就是在这么一个时间段内被反复收割。没有一个系统性的交易策略，或者即使有，因为人性的弱点无法严格遵守已经既定的策略，是韭菜三宝行为屡屡发生的原因。

投资者在刚买入投资标的时，通常会有一个预期的卖出心理价位。刚开始这个心理价位理所当然的在买入成本线之上，此时可以称之为“心理止盈位”。如果市场很快走高，比较聪明的投资者很容易调整心理止盈位，继续吃趋势红利。如果市场反向走低，价格低于买入价时间一久(被套)，投资者的卖出心理价位跟着降低，但并不会降低到当前市场价，很多投资者不喜欢设置止损，继续死扛。随着被套时间的增加，卖出欲望会日益强烈。这样，一旦市价与卖出心理价重合，很容易就放弃了筹码。此时成交价若低于成本价叫“割肉”(想想 48 万哥)，高于成本价就是所谓的“拿不住”。这往往是因为很多人倒在了黎明前或止步于牛市清晨的原因。

其实应对方法很简单:不要梭哈!不要梭哈!不要梭哈

不梭哈，就保住了弹药库，面对市场波动心理就能毫无波动，遇到暴跌甚至还有点想笑(趁机降低成本)。具体操作就是严格定投(定期或者金字塔方法去收筹码)，不要以自己的短期市场分析为依据去抄底买入(又累又容易出错，何苦呢?何必呢?)。这样，你的卖出心理价就会一直高高在上，当微笑曲线回到你的成本线上方后，你也没有理由急着去止盈了，

当然，只有大饼才可以如此操作。也只有提高了认知，明白大饼何以让人信心满满，才不至于某一个时刻心态崩塌酿成惨案。省下频繁操作的时间多学习，是提升自己，避免去当韭菜的一个极好的方式。

2022/1/9 21:14 知道者悖论

老师对学生们说:“下周(周一到周五之间)将进行一场考试，不过你们不会预先知道这场考试具体发生在下周的哪一天。

聪明的学生开始了推理:

1.这场考试一定不会发生在周五，因为如果是周五考试，那么因为前四天没考，我们就提前知道了考试发生在周五。违反了老师说的我们不会预知考试的逻辑条件

2.既然排除了周五，这场测试应该在周一到周四中，那么，根据同样的理由，可以排除周四，因为如果前三天没有考试，那么我们能知道考试在周四了。

3.继续同样逻辑，可以排除周三和周二。

4.因为排除了除了周一以外的四天，那么考试就一定会发生在周一，同样违背了不可预知的逻辑设定。所以，周一也不会考试。

学生最后得出结论，下周任意一天都不会考试

结果第二周的某一天，考试还是来了。学生目瞪狗呆，
这怎么可能!!

这就是很有意思的“知道者悖论”

同样的事情发生在我们的大饼市场中，我们知道在和法币的较量中，大饼的美元汇率一定会

囤饼之道 达哥微博精选 (2021.8-2024.11)

涨到 100w\$, 1000w\$。。。但是我们无法预知具体的时间点，我们只需要知道，那一天在未来的 20 年内一定会像那场考试一样到来。
这，就够了。

2022/1/14 13:48 主观价值

价值是主观的，比如一张 20 年前的全家福照片对你来说具有价值，对一个路人来说就是一张废纸。

一个货物，之所以呈现出一定的“客观价值”，只是很多人对这个货物“主观价值”的交集，我们称之为“共识”

共识”有两个维度，一个是产生“主观价值交集”者的数量，决定了共识的范围(广度)。一个是维持“主观价值交集”的时间，决定了共识的连续性(深度)。共识的广度决定了它的流动性，共识的深度决定了它的价值稳定性。

大饼拥有 10 多年的广泛共识，原因是它本身就是从价值中创造而来(以时间和能量)，以太坊有着数年的广泛共识，因为他给其他价值流动提供了平台。

反观 nft，它的流动性差说明共识广度不足;基本靠热度炒作决定了其共识深度也不足。很容易想象一组屌丝的照片对于其他人来说实际价值根本就趋近于 0

想通了这点，就不会把有限的精力投入到这些旁门左道上去了--除非你是发 NFT 的镰刀，可以自己收割别人。

2022/1/24 10:52 饼本位

先说两个基本事实：

1、央行印钞机缺乏自我约束的动机，法币没有销毁机制总量只会一直增加。通货膨胀导致法币的购买力持续贬值。

2、大饼总量限定 2100 万枚，由于私钥丢失等因素实际流通量只会更少(据信至少 400 万个已永久丢失，这部分价值则均分给了余下的大饼上)，大饼的供应量只会越来越少。

所谓交易，就是交换双方由于边际效用、信息不对等等因素，造成主观价值的差异，用自己认为“不够好”的东西交换别人“更好的”东西。

所以，你应该在合适的时间卖出美元，换回大饼。比如前段时间大饼汇率 34000\$，1 美元可以卖到 2941 聪而在前期高点汇率 69000\$的时候，1 美元只能卖到 1449 聪。

我个人金字塔买单挂在了 27600\$，期望能以 3623 聪的价格去卖出美元。就是不知道什么时候才有好人以这个价位买我的\$了。

这就是饼本位。

2022-6-2 文化侵略

最近很多人都在聊文化侵略，让我想起一个事。

某地疫情期间搞了个保供名单，不让京东等物流和货物进城进小区，对搞保供制度的这些人来说，京东货物就是货物侵略，妨碍了他们自己兜售烂货。

有些人说，京东也是为了赚钱，才没什么好心。

其实，别人什么目的根本不重要，重要的是你有没有选择权。

只要是允许货比三家的选择，最后被选择最多的一定是共识最好的。如果你觉得被侵略，说明你拥护的是共识低的烂货。

记住，“京东”什么目的不重要，东西是好货才重要。

2023-1-11 nostr 协议

试用了一下 nostr。

基于加密学（非区块链）的去中心化信息载体。

生成私钥后备份保存好。

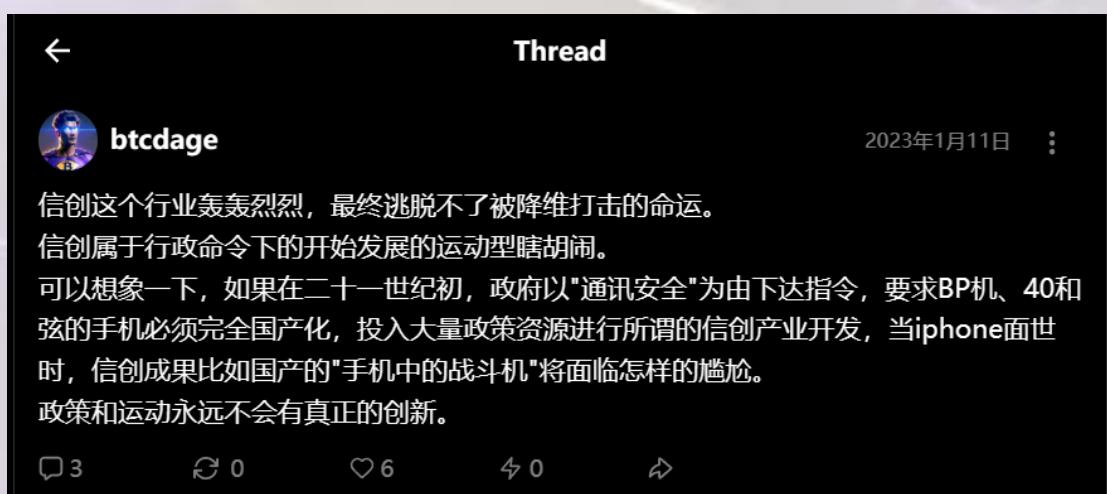
不再需要手机号验证，繁琐的 kyc，你的私钥你的账户。

这是我发的第一篇 nostr。

astral.ninja/note17d39svygyn48mavnejgl0xr0qxh00yasn96dq9u22uezqvstklswumxqx?continueFlag=19278e79782564f74d444cc320eb651b

或者：

<https://iris.to/note17d39svygyn48mavnejgl0xr0qxh00yasn96dq9u22uezqvstklswumxqx?continueFlag=19278e79782564f74d444cc320eb651b>



2023-1-15 nostr 中设置闪电网络收款地址

在 nostr 中设置闪电网络地址收款地址

- 1、访问 getalby.com 点击右上方的选项图标
- 2、点击 Login 进行登录（第一次登录需要注册账户）
- 3、点击 Sign up with email 进行注册
- 4、输入你的邮箱地址，和 你自定义的 alby 密码，点击 Sign up 进行下一步
- 5、进入你的邮箱进行验证，然后点击 alby 页面的 “Get your lightning address”获取闪电网

络地址

6、输入你的自定义的 ID, 你的闪电网络地址将是 ID@getalby.com 。然后点击“Create Address”

7、复制你的闪电网络地址

8、进入 astral.ninja, 点击下面齿轮图标进行设置

9、点击 edit 按钮对个人信息进行编辑

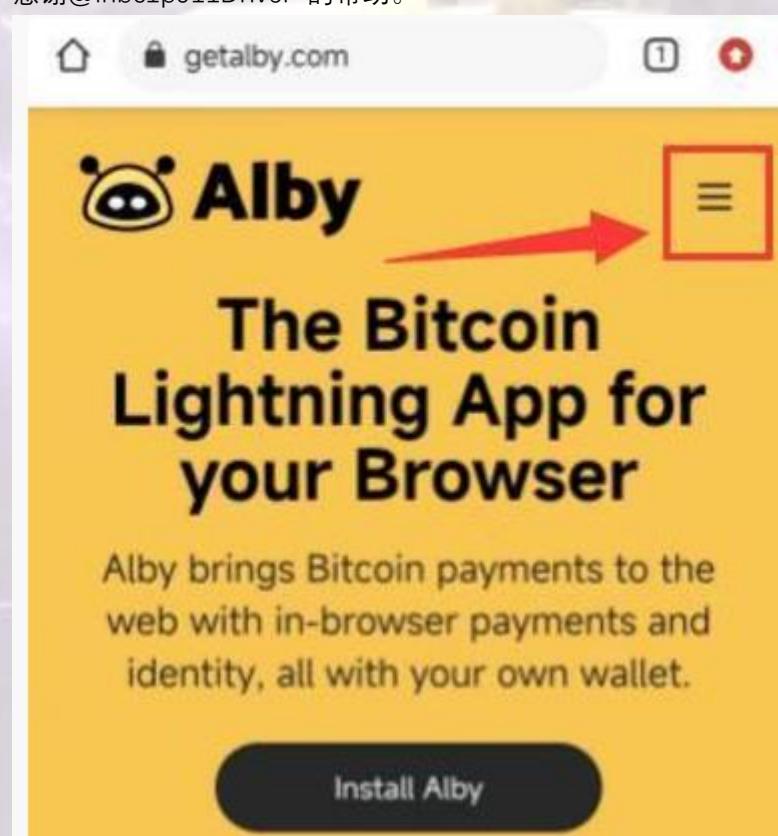
10、粘贴你的闪电网络地址, 点击 save 保存

这样你的 nostr 的收款地址就设置完毕了。

别人可以点击文章后面的闪电标志通过闪电网络对你进行大饼打赏。

btw:用邮箱注册而不是用 bluewallte 账户登录, 主要是因为后者仍然需要输入邮箱地址才可以生成闪电网络地址。就像一些平台用微信登录以后仍然要绑定手机一样, 不如直接手机注册了。

感谢@lnbc1p911Driver 的帮助。



The image is a collage of four screenshots from the Alby website, illustrating the user authentication and account creation process.

Top Left: A screenshot of the Alby homepage (getalby.com). It features a yellow header with links for "Value4Value", "Blog", "Install Alby", and a prominent red-bordered "Login" button. Below the header, a text block reads: "Alby brings Bitcoin payments to the web with in-browser payments and identity, all with your own wallet." A large "Install Alby" button with a curved arrow pointing to it is centered, with the text "Do it!" below it.

Top Right: A screenshot of the login page. It offers two options: "Log in with lightning" (in a yellow button) and "OR" (separated by a horizontal line), followed by "Log in with email". Below this is a form field labeled "Email address*" with a placeholder "Email address" and a "Log in" button. At the bottom, there are links for "Don't have an account?", "Sign up with email" (red-bordered), and "install Alby". A red arrow points to the "Sign up with email" link.

Bottom Left: A screenshot of the sign-up page (getalby.com/user). It has fields for "Email address*" (with placeholder "Email address" and a red arrow pointing to it), "Password*", "Confirm password*", and a "Sign up" button. Below the form is a link: "Already have an account? Log in with email or install Alby". Red arrows point to the "Email address" field, the "Password" field, and the "Confirm password" field, each accompanied by Chinese annotations: "你的邮箱", "设置密码", and "设置密码" respectively.

Bottom Right: A screenshot of the user dashboard. It shows a balance of "0 sats" and three buttons: "Receive", "Send", and "Topup". Below this, a section titled "Get your Alby username and lightning address" explains that a lightning address is like an email address for Bitcoin. It includes a "Get your lightning address" button, which is red-bordered and has a red arrow pointing to it.

Create your lightning address

Your lightning address can be used to easily send and receive bitcoin over the lightning network.

Your lightning address can't be changed at a later date so choose wisely.

Create Address

Your Lightning Address

@getalby.com

https://getalby.com/p/c...

astral.ninja

btcdag2009

btcdag2009
npub17ahz_0z7pw
i come,i see,i hodl.

POSTS FOLLOWERS RELAYS

search posts

npub17ahz_0z7pw
btcdag2009
nostr为什么会成功？因为说真话是刚需。
中心化的产品曾经可以满足这个需求，然而环境不可挽回的恶化。nostr协议及时出现了。
权力作恶越是泛滥凶猛，越是在推动去中心化协议的探索和进步。
皇上，丐帮是不是壮大还不是你决定的。——苏乞儿。

npub17ahz_0z7pw
btcdag2009
昨晚用了将近4个小时从0开始建立了第一个nostr中继器。
大家可以通过 [lns.to](#) 或者 [astral.ninja](#) 等客户端访问。
比如我的公钥是：
npub17ahz_0z7pw...
What's happening?

settings

profile

Name: btcdag2009

About: (in 150 chars)
i come,i see,i hodl.

Picture URL:
<https://nostr.build/l/4639.jpg>

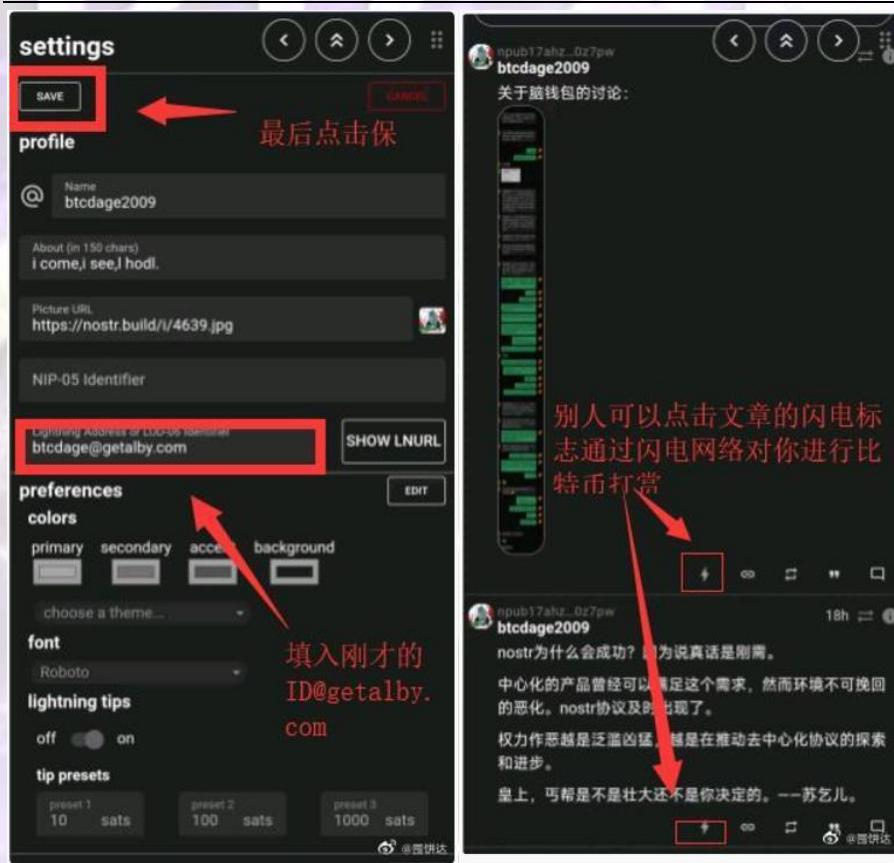
NIP-05 identifier:

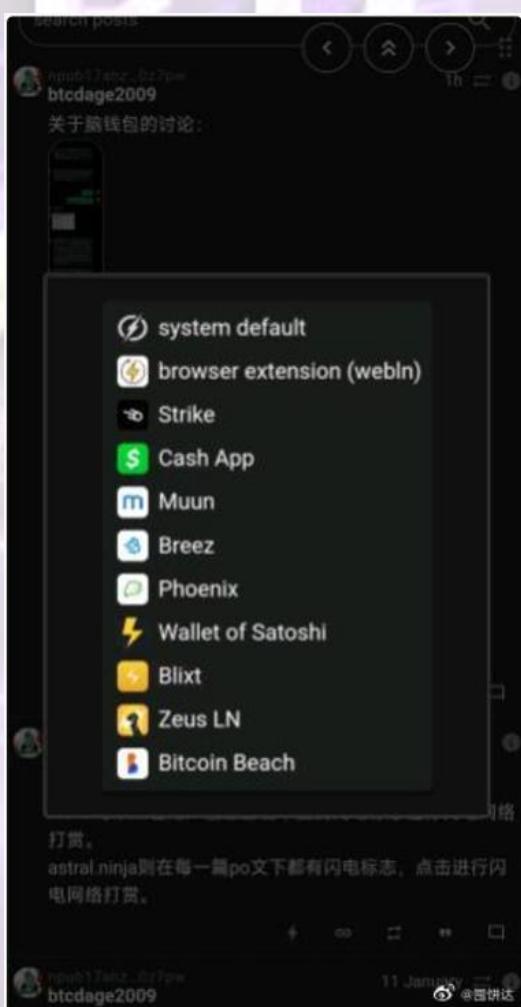
Lightning Address or LNURL Identifier:
btcdag2009@getalby.com

preferences

colors

primary secondary accent background





2023-1-16 《从 WEB1.0 到 WEB4.0》

发布了头条文章：《从 WEB1.0 到 WEB4.0》

【WEB1.0】

BS 架构，B 为浏览器客户端，S 为服务器端。

1、所有数据由平台所有者发布在服务器中，用户只能通过浏览器被动接受服务器返回的数据。

2、数据产权完全归平台所有者，平台所有者（服务器管理员）拥有数据的全部增删改的权限。

缺点：数据采集缺乏用户参与

【WEB 2.0】

BS 架构，B 为浏览器或者 APP“客户端”，S 为“服务器端”。

1、数据可由用户进行发布，数据存放在平台所有者的中心服务器（或集群）中。

-
- 2、用户通过账户和口令进行平台登录，所有账户数据包括口令（有可能加密过）等敏感信息也存放在平台
 - 3、所有者的中心服务器（或集群）中。不同的平台需要分别注册账户，用户信息不能跨平台使用。
 - 4、用户数据产权完全归平台所有者，平台所有者有权对用户账户的权限进行限制甚至封禁，也可对用户数据进行修改或删除。

进步：用户深度参与数据的采集

缺点：用户无法保护对自己数据的权利，任由平台方处置。平台自身也容易被铁拳限制或者关闭。

【WEB 3.0】

BS 架构，B 为浏览器或者 APP 访问的“DAPP”，S 为“区块链”。

- 1、数据由用户进行发布，数据存放在区块链中（不考虑毫无意义的非公链）。
- 2、用户通过加密学，根据公链的不同使用相应的不对称加密算法，使用公钥（地址）作为账户 ID，私钥作为签名凭据。用户私钥不保存在任何服务器中。同一类型的公链的“用户账户”通用（比如 ETH/BSC/OKC/KSC 通用，不能跨异类型的公链），但是用户其他数据只保存在平台方使用的单独链上，无法跨链使用。
- 3、虽然理想状态的公链，元数据无法修改或删除。但通过智能合约，平台方实际控制了用户数据的指针。另外智能合约的版本升级也完全由平台方控制。用户对自己的数据仍然没有真正的权利。

进步：不再使用用户密码进行账户鉴权，私钥由用户独自控制，独立性、安全性、隐私性得到极大提升。

缺点：数据仍由平台方实际控制，通过智能合约，平台方仍然可以对用户进行限制甚至封禁。

【nostr 协议（WEB 4.0）】

BS 架构，B 为浏览器或者 APP 访问的“客户端”，S 为“中继器”。

- 1、数据由用户进行发布，数据存储在任意数量的中继器中。
- 2、用户通过统一的不对称加密算法，使用公钥作为账户 ID，私钥作为签名凭据，实现对身份和操作的鉴权。这种账户鉴权发生在客户端，是通用且与中继器无关的。
- 3、每个中继器的管理员只能对自己架设的中继器的数据进行裁剪操作（只能删不能改，因为修改数据需要私钥签名，篡改的数据会被客户端丢弃）。虽然中继器之间不会自动同步，但由于客户端同时连接若干中继器，可以同时发布数据到这些中继器中。读取也是同时读取若干个中继器。因此，一部分中继器的用户数据被删除不影响用户的使用。任何一个中继器的管理员都无法实现封禁某个用户数据（无论是账户信息还是发布的数据）。
- 4、中继器很容易搭建，任何人都可以搭建一个自己的中继器来实现自己的数据副本。加强了去中心化，确保第三点的实现。

进步：

- 1、用户账户完全由加密学生成，且所有平台通用，在互联网上第一次实现了“用户实际意义拥有自己账户数据的权利”。
- 2、用户去中心化，由于第一点的进步，用户数据第一次完全跨平台，不同的平台客户端访

问同样的一批中继器，返回的数据完全一致。

3、客户端的去中心化，只要是按照 nostr 协议开发的客户端，就可以从中继器读取数据，比如 iris 和 astral 是不同的客户端，但是读取的数据是一样的。使用户不再担心平台被铁拳制裁——一个客户端站点访问不了换一个就是。如果客户端做成应用程序或 app，就更彻底的去中心化了。

3、中继器的去中心化，使得权力无法完全封禁数据源，提高了数据的鲁棒性。

在 nostr 协议下：

- 1、中继器管理员拥有自己中继器的完全权利，但是无法干涉用户权利。
- 2、用户掌控自己数据的完全权利，但是无法干涉某一个中继器管理员的权利。
- 3、应用平台的企业家可以根据自己的判断，在自己发布客户端时，在客户端侧对数据进行审查和筛选，也可以添加广告和其他业务，但是无法干涉用户是否选择采用其他客户端去访问中继器的权利，也无法干涉其他人建立的中继器的管理权。

人人管好属于自己产权的事情，没有权力干涉他人权利。自己的任何行为的结果交给市场。这就是 nostr 协议的哲学思想，也是其有资格可以称之为未来的 WEB4.0 的重要原因。

2023-1-17 使用 nos2x 管理 nostr 私钥

【图文教程】使用 nos2x 管理 nostr 私钥。

by btcdage

nostr 公钥：npub17ahz4xa3hvkvvh4wguzzqknp8p7l5nyzzqc3z53uq538r5qgn0q40z7pw

nostr 协议中，用户可以在所有的应用使用同一个账户，使用私钥进行账户的登录。

在各个客户端中使用同一个私钥登录，客户端的安全性就显得十分重要。

为避免私钥泄露的风险，在目前网站类型的标准客户端，均支持在浏览器插件进行私钥签名操作。

因此使用 chrome 插件 nos2x 管理私钥，可以提高账户安全性。

1、在 chrome 中打开扩展程序，打开 chrome 应用商店，搜索 nos2x。

2、打开 nos2x 应用页，安装 chrome 插件。

3、chrome 应用商店可能需要科学上网，如果没有科学，也可以下载插件进行离线安装，下载地址：

<https://pan.baidu.com/s/1nc7WN GhU56YgcSoKiSDO9Q?pwd=vf36>

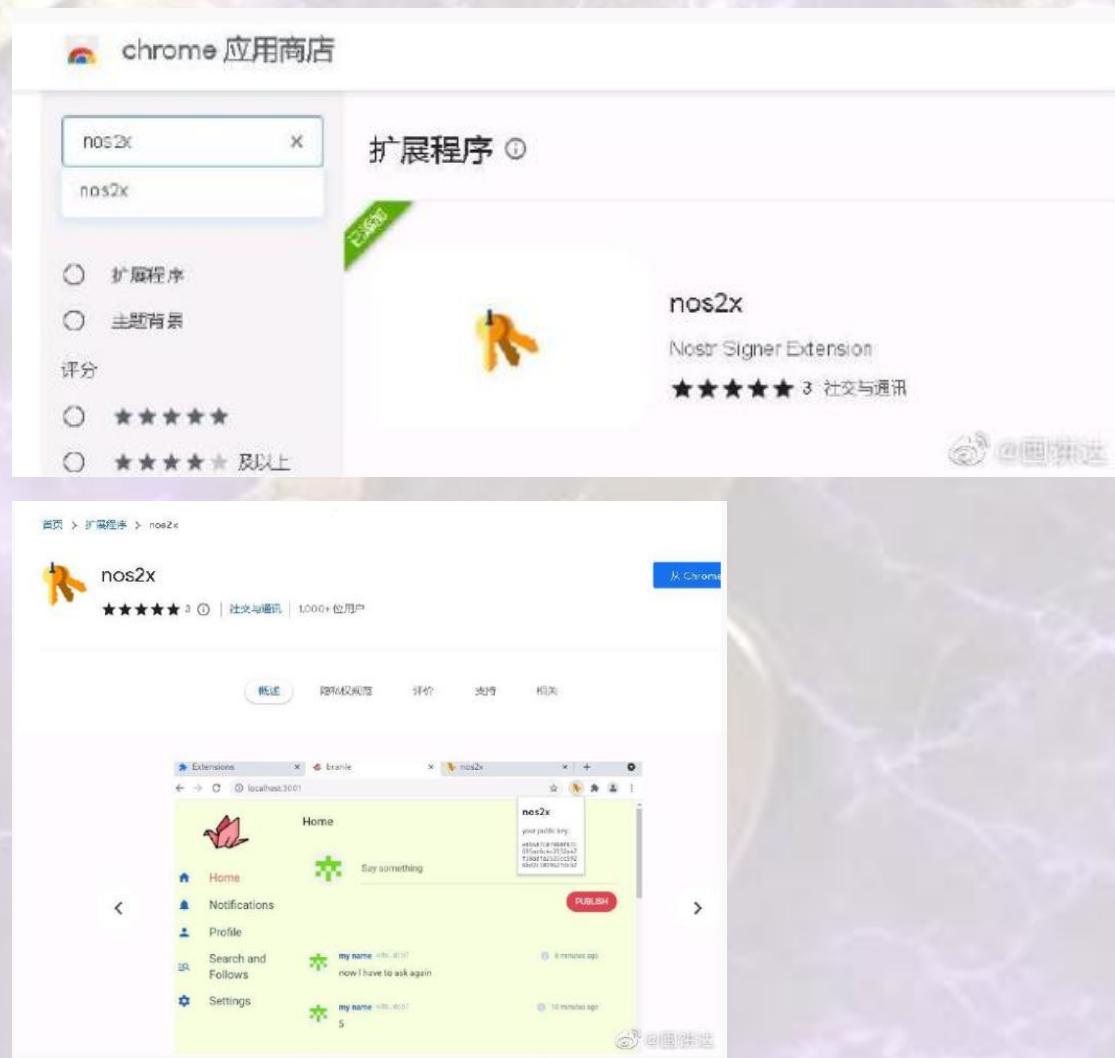
4、安装完毕后，打开 nos2x 扩展程序的显示，右键点击 nos2x 图标，选择选项。

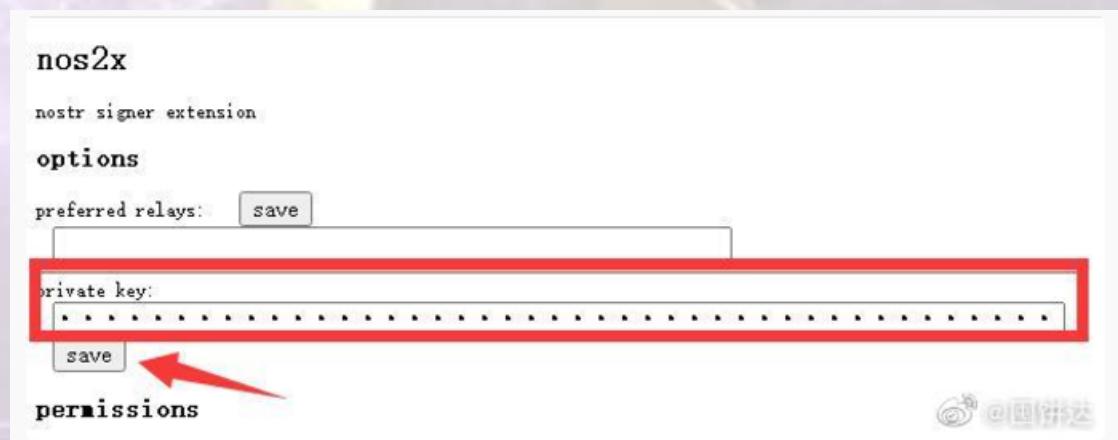
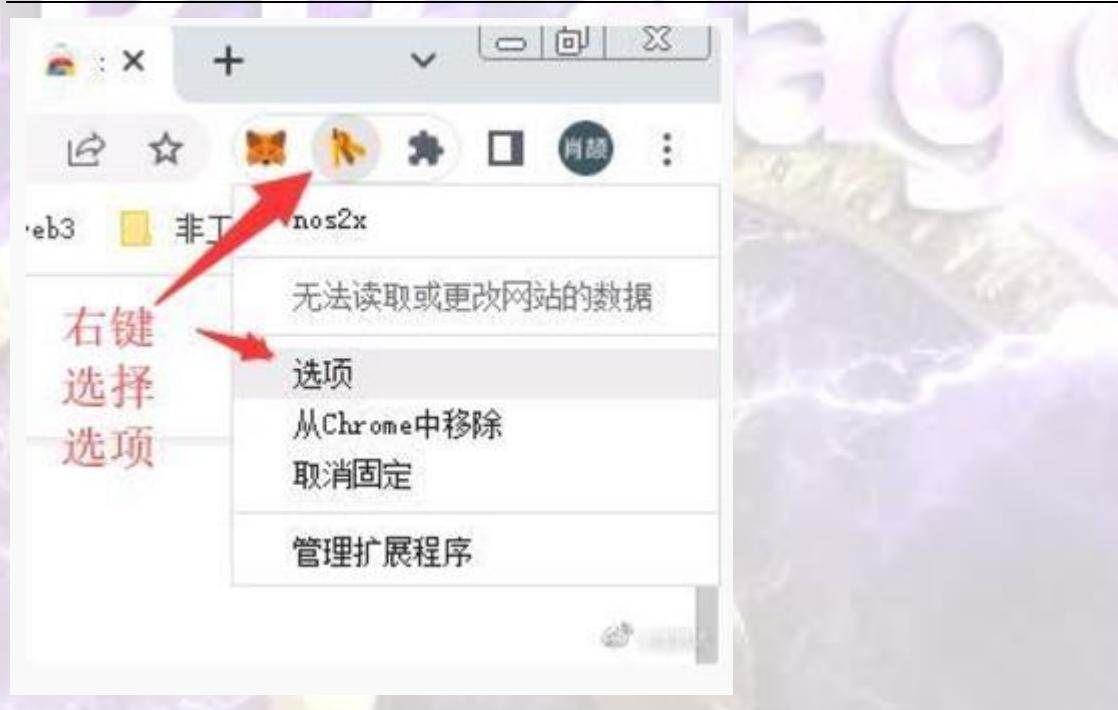
5、输入你的 nostr 私钥，点击 save 保存。

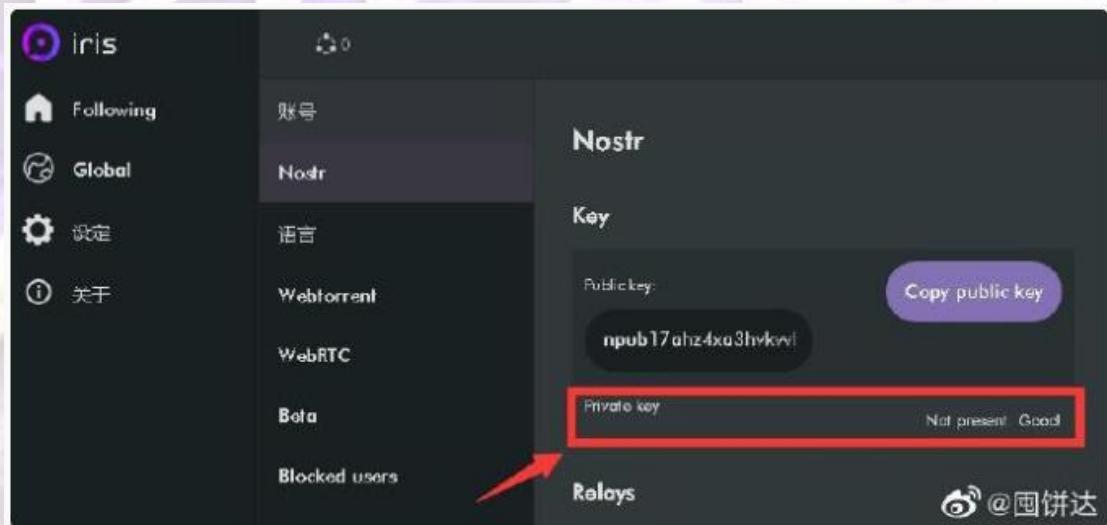
6、当你进入一个 nostr 应用时，请不要使用私钥登录，而是选择 extension(扩展插件) 登录。

7、插件将弹出选项，选择“一直授权”还是“授权 5 分钟”或者“仅授权本次操作”。推荐“authorize forever”(一直授权)。这样每次需要私钥进行签名时会自动进行签名，而客户端网站是不接触私钥的。

这样在使用网站类型的 nostr 客户端时，都可以用 nos2x 进行插件签名操作，确保账户私钥安全。







2023-2-2 nostr 账户安全手册

nostr 账户安全手册

1. 别泄露私钥，别泄露私钥，别泄露私钥。
2. 只用开源可靠的客户端 app。不随便导入私钥可疑的客户端。
3. 客户端网站不导入私钥登录，用 nos2x 之类的浏览器扩展插件去对签名签名（建议 nos2x 的新版改进下，修改自己资料的时候必须手动签名，以免客户端网站修改闪电地址的作恶操作）。
4. 不同圈子用不同账户，多账户分散风险，比如聊天用一个，发 po 用一个，评论用一个，敏感话题用一个，测试新的客户端用一个。

小技巧：必须复制私钥的时候，暂时关闭其他软件读取剪切板的权限，粘贴一半，留几个字符手动输入。

2023-2-10 XMR 的问题

门罗的问题归根结底仍然是去中心化的不足。

门罗这种 cpu 矿币，由于肉鸡的建设资源和电费不是矿工自己承担，如同国企的领导掌控不是自己投资的企业一样，不会有自己投入资金的企业那种真正的重视和归属感。当然也不怎么会参与这种加密货币的社区。

为了抗 ASIC，门罗每隔一段时间就会更新挖矿软件，在这个过程中，我深深地体会到 xmr 开发团队的权力之大。矿工只有乖乖的把肉鸡里的挖矿程序升级。像比特币这种用户、矿工、开发团队的三足鼎立在门罗这儿并不存在。

一个开发团队权力独大的加密货币，哪怕算力再分散，它也是高度中心化的，是没有真正的前途的。

2023-2-17 如何安全私聊

如何和别人安全私聊？

可以按照下面方法手动实现：

1. 新建一个 nostr 账户。
2. 将新建账户的 nsec 私聊发送给对方。
3. 两个人都使用这个 nsec 登录 nostr 平台
4. 自己对自己发私信。

就实现了安全私聊。没有人知道你和谁聊天，聊了多久，聊了什么。

用完即焚，每次安全私聊完，这个账户就废弃不用。

下次私聊再重新建立新账户。

注：

安全发送私聊临时账户私钥给对方的几种方法。

1. 直接 nostr 私聊发给对方即可，利用了 nostr 私聊信息是加密的特性。
2. 传统社交发给对方，把头部 nsec1 去掉，末尾加几位随机字符。（提前约定好后几位是假的截去，前面加上 nsec1 即可，当然前面也可以约定好加几位混淆字符）。

2023-2-20 安全私聊自动化软件详细设计

nostr 协议安全私聊自动化软件详细设计

自动安全私聊方案设计：

用户用公开的账户 A，想和公开的账户 B 进行安全私聊。

- 1、用户使用 A_nsec1 登录客户端 A，点击用户 B 的 B_pub1 的资料界面。
- 2、点击进入安全私聊界面。
 - a、客户端 A 自动生成一个 公钥私钥对 (C1_nsec1/C1_pub1)。
 - b、客户端 A 将安全私聊请求以正常私聊的协议方式发送到 relay，内容包括 C1_nsec1/C1_pub1。客户端 B 收到私聊请求和 C1 信息。
 - c、客户端 B，开始监听 C1 的私聊接收事件。
(这个过程中，在 relay 侧暴露一次 A --->B 的私聊动作，单因内容加密，C1_nsec1/C1_pub1 是第三方保密的)。
- 3、A 发送安全私聊信息比如“你在吗？”。
 - a、客户端 A 自动生成一个公钥私钥对 (C2_nsec1/C2_pub1)，和 A 的昵称、发送的信息进行拼接，比如“{s:C2_nsec1,p:C2_pub1,n：“btcdage”,c:“你在吗？”}”，用约定好的 C1_nsec1 签名后，通过普通私聊协议发送给 C1。然后客户端 A 开始监听 C2 的私聊事件。

b、客户端 B 收到 C1 的私聊事件，用 C1_npub1 解密后，进行显示：

btcdage:你在吗？

4、客户端 B 回复“我在。”

a、客户端 B 生成一个新的公钥私钥对 (C3_nsec1/C3_npub1)，和使用 B 的昵称、回复的信息进行拼接，比如“{s:C3_nsec1,p:C3_npub1,n:"satoshi",c:"我在。""”，用 C2_nsec1 签名后，通过普通私聊协议发送给 C2。然后客户端 B 开始监听 C3 的私聊事件。

b、客户端 A 收到 C2 的私聊事件，用 C2_npub1 解密后，进行显示：

satoshi:我在。

5、A 再次发送安全私聊信息比如“吃饭了吗？”。

a、客户端 A 自动生成一个公钥私钥对 (C4_nsec1/C4_npub1)，和 A 的昵称、发送的信息进行拼接，比如“{s:C4_nsec1,p:C4_npub1,n:"btcdage",c:"吃饭了吗？""”，用约定好的 C3_nsec1 签名后，通过普通私聊协议发送给 C3。然后客户端 A 开始监听 C4 的私聊事件。

b、客户端 B 收到 C3 的私聊事件，用 C3_npub1 解密后，进行显示：

btcdage: 吃饭了吗？

6、客户端 B 回复“吃过了。”

a、客户端 B 生成一个新的公钥私钥对 (C5_nsec1/C5_npub1)，和使用 B 的昵称、回复的信息进行拼接，比如“{s:C5_nsec1,p:C5_npub1,n:"satoshi",c:"吃过了。""”，用 C4_nsec1 签名后，通过普通私聊协议发送给 C4。然后客户端 B 开始监听 C5 的私聊事件。

b、客户端 A 收到 C4 的私聊事件，用 C4_npub1 解密后，进行显示：

satoshi:吃过了。

如上所示，客户端 A 和客户端 B 通过一次公钥 A---》公钥 B 的私聊消息传递之后，就进入了 C1-C2-C3-C4-Cn...无限临时账户的信息交流。每个临时账户的聊天记录里只有一个单独的语句，不构成对话，无法挖掘任何信息。

一旦退出软件或者点击“停止安全聊天”，则客户端停止监听 Cn 的私聊事件。再次私聊需要再次从第一步开始。

聊天记录只在本地客户端的缓存显示，一旦清除缓存或者客户端不留缓存，则不可能还原。

补充，每次监听新的 cn 私聊事件时，上一个 cn-1 的结束监听。

btw:

目前手动安全私聊，可在发言前加一个逗号，以方便一目了然区分谁的发言。
因此，方案中自动加入昵称。

=====

基于 nostr 协议安全私聊的一点想法，聊做抛砖引玉。

2023-2-22 手动发起安全 nostr 群聊

如何在微信群手动发起安全 nostr 群聊

例子：

1. 树洞登录写下今日树洞口令:abcd

让参与群聊的人都关注树洞账户可以看到。

2. 微信群里写下今日微信口令:1234

3. 各自拼接树洞口令和微信口令:abcd1234

4. 对拼接口令做 sha256 哈希生成:

e9cee71ab932fde863338d08be4de9dfe39ea049bdafb342ce659ec5450b69ae

5. 参与群聊的人使用哈希结果作为私钥 nostr 客户端，打开对自己的私聊界面开始安全群聊。

注：

1. 树 洞 账 户 可 以 用
nsec1wyumvdel8snyq59nf0jq24kazyemdyyv6gdhadmlz4er2f7ghewqfaw9rr

也可以在群里预先设定一个专属口令发布账户。

2. 对口令进行 sha256 这步可以借助使用 @比特币布道者 的 比特币脑钱包生成页：

网页链接

3. 可以线下约定第三个字符串进行拼接，再进行 sha256 生成私钥。

4. 每天更换树洞口令和微信口令（以及线下口令），可确保安全性。

此方法唯一缺点是手动操作之后群聊中无法分辨谁是谁，需要自己做约定记号，但群聊的私密性得到了最大的保障。

btw:

如果客户端进行二次开发，随机生成私钥再和《如何实现和别人安全私聊》

@note1nuyk5caznu0n5realdlh4lck0fwpu56m9gwhm2u99gqyyamv7g6s77m7yk

一样处理自动带上发言人昵称，就实现了方便的加密群聊。只需要在群里加入或者退出人员

时自动更换临时私钥，保障了安全群聊的私密性。

2024-2-29 10:07 人类四大发明（发现）

人类四大发明（发现）

- 1.用石头敲骨头
- 2.蒸汽机原理
- 3.电磁感应
- 4.一种点对点的电子现金系统



2024-3-6 09:19 定投收益

按照当前的价格(63600)来算，如果你从2021年就跟着达哥一起金字塔定投，那么，到今天，你的收益率应该是180%左右。如果按昨天的史高69000，就是208%的收益率。

注意收益率和每份定投的金额无关，定投成本是 22383 不变。根据数据可知，如果：
每份金额是 1000u,就能买到 33.24 个大饼
每份是 10000u,就能买到 332.4 个大饼
每份 100u,能买到 3.24 个大饼
每份 10u,能买到 0.324 个大饼
就算是每份投 1u (要在 dex 交易)，也买到了 324w 聪的大饼

无论投入多少，收益率都是至少 180%。这就是大饼的公平性，没有投资门槛，一视同仁。

3 年 180% 收益率，确定性 100%。天底下仅此一家。
赌狗退散。

要“落袋为安”吗？
抛弃法币思维，1 饼=1 饼。
永远记住定投是为了以更少的法币换更多的大饼，hold!
hold!
hold!

金字塔定投	当前饼价:	63600	平均成本:	22383.09202
收益率	每份定投(\$)	定额份额	投入金额(\$)	饼总量
184%	1000	744	744000	33.2393755
2021/11/16	62100	1	1000	0.01610306
2021/11/26	55200	2	2000	0.036231884
2021/12/4	48300	4	4000	0.082815735
2022/1/7	41400	8	8000	0.193236715
2022/1/24	34500	16	16000	0.463768116
2022/2/28	37500	8	8000	0.213333333
2022/3/31	45200	4	4000	0.088495575
2022/4/30	47600	4	4000	0.084033613
2022/5/12	27600	32	32000	1.15942029
2022/6/15	20700	64	64000	3.09178744
2022/7/31	23300	32	32000	1.373390558
2022/8/31	19800	64	64000	3.232323232
2022/9/30	19200	64	64000	3.333333333
2022/10/31	20600	32	32000	1.553398058
2022/11/30	16500	64	64000	3.878787879
2022/12/31	16500	64	64000	3.878787879
2023/1/31	22800	32	32000	1.403508772
2023/2/28	23100	32	32000	1.385281385
2023/3/9	20700	32	32000	1.54589372
2023/4/30	29100	16	16000	0.549828179
2023/5/8	27600	32	32000	1.15942029
2023/6/30	29600	16	16000	0.540540541
2023/7/31	29200	16	16000	0.547945205
2023/8/17	27600	32	32000	1.15942029
2023/9/30	26900	32	32000	1.189591078
2023/10/31	34100	16	16000	0.469208211
2023/11/30	37500	8	8000	0.213333333
2023/12/31	42000	8	8000	0.19047619
2024/1/31	42300	8	8000	0.189125296
2024/2/29	60400	1	1000	0.016556291

2024-3-12 10:17 三·一二

历史告诉我们一切。

囤饼之道 达哥微博精选 (2021.8-2024.11)

现货	合约	币种	最新价格	24h涨跌	币种	最新价格	24h涨跌	
自选	BNB	BTC	ALTS	USD⑤	名称	成交量	最新价格	24h涨跌
市场 / 成交量	最新价格				BTC / USDT	51.23亿	72,321.54	+5.76%
BTC / USDT	3895.36			-49.01%	ETH / USDT	28.00亿	4,058.14	+6.28%
量 1,850,543,338	¥ 27,077.37				UNI / USDT	5,393.41万	14.382	+2.99%
BCH / USDT	133.95			-47.39%	CAKE / USDT	5,150.38万	4.171	+8.03%
量 151,426,740	¥ 941.43				FIL / USDT	1.88亿	11.093	+7.89%
BNB / USDT	6,514.9			-58.21%	LTC / USDT	3.11亿	101.99	+19.29%
量 120,942,034	¥ 45.79				BNB / USDT	7.39亿	526.2	+2.73%
XTZ / USDT	0.9901			-57.21%	AVAX / USDT	4.27亿	48.74	+19.29%
量 67,024,168	¥ 6.76				DOT / USDT	1.54亿	10.922	+8.16%
ETH / USDT	88.25			-51.77%				
量 597,328,052	¥ 620.24							
ALGO / USDT	0.1000			-60.25%				
量 6,515,598	¥ 0.70582							
ALGO / BTC	0.0000			-22.29%				
量 99?	¥ 0.700582							
NEO / USDT	4.000			-54.80%				
量 21,817,969	¥ 28.11							
ATOM / USDT	1.172			-58.08%				
量 14,413,808	¥ 9.24							

2020.3.12 日 钱包

2024.3.12

3|2

致敬币圈 敬畏风险

放弃容易 坚持不易
纪念312币圈激荡四周年

2020年3月12日 2024年3月12日
比特币 3794.5 USDT 比特币 72666 USDT



比特币四年涨幅 1816 %

@囤饼达

2024-3-13 10:00 囤到底，月球见

一个刚入场没一年的小伙伴跟我说：“达哥，牛市这么猛，我是不是该趁机卖了？”我看着他，心说来了来了，又是一个想在牛市跳舞的勇士。

我拍了拍他的肩膀，语重心长地说：“小子，听我说，这大饼的世界里，最重要的就是一个‘囤’字。你知道吗？那些年，大饼还只是个小不点的时候，有多少人眼睛里只有法币，结果呢？错过了一波又一波的致富快车！”

小伙伴一脸迷茫：“但是，达哥，牛市不是赚钱的好机会吗？”

我笑着说：“你得明白，我们囤饼人，不是因为短期的涨跌，而是看重它长远的价值。大饼稀缺，总量有限，未来的潜力无限。你今天卖了，可能暂时赚一点，但你失去的，是未来可能的一大笔财富。”

“再说了，大饼就像是我们的信仰，中本聪不也是希望建立一个去中心化的新世界吗？我们囤饼人，就是为了坚持这个信念，见证这个世界的改变。”

小伙伴点了点头：“达哥，我懂了，我要成为一个真正的厚德（hodler）！”

我拍了拍他的肩膀：“对，年轻人，未来是属于我们这些敢于梦想、勇于坚持的人的。记住，牛市熊市都是过眼云烟，只有囤住，才能抵达财富的彼岸。”

亲爱的朋友们，下次有人问你牛市卖不卖，你就大声告诉他：“囤（hodl）到底，月球见！”

2024-3-13 14:03 最好的货币

在一个货币聚会上，黄金、法币和大饼决定比赛看谁是最好的货币。黄金自信地说：“看我的市值，我最稳。”法币不服气地说：“但是我交易快。”大饼在一旁轻轻笑道：“你们继续争吧，我这就去月球了。”



2024-3-15 16:18 高级脑疑问的相关思考

关于高级脑疑问的相关思考

问题一：“哈希算法能够提高抗碰撞性吗？”

首先我们需要做下定义：

抗碰撞性：

指在可行的时间和资源内，难以找到两个不同的输入，使得它们经过哈希函数处理后产生相同的输出哈希值。

散列性：

指能将任意长度的输入数据映射到一个固定长度的输出哈希值上，且输入数据的微小变化都会导致输出哈希值的显著不同（雪崩效应）。

抗暴力破解：

指通过设计复杂度高的计算过程或数据结构，使得尝试通过穷举所有可能的解来破解密码、密钥或加密数据变得在实际操作中非常耗时和计算上不可行。

默认定义：

为了方便讨论，除非特别指出，下文所有的“哈希算法”这个词，我们套用具体的 sha256 算法来讨论。（文中 sha256 就是哈希算法，哈希算法就是 sha256）

“sha256 算法具有足够高的抗碰撞性”应该是共识，比特币世界所有的一切都建立于这个必要条件。因此，哈希算法并不是能不能“提高抗碰撞性”的问题，它本身就具有抗碰撞性。

高级脑的“算法规则”这一维度，假设 sha256 的抗碰撞性为 a。任何多次的套娃和加盐并不能使最终结果的抗碰撞性 $b > a$ 。但是需要注意的是， b 也不 $< a$ 。因为 $b = a$ 。

给大家一个感性认识：

字符串 A="1"

字	符	串
B=	Kxik7YNwCwXDLar3XwCwXDLar3XKLP4KoHNzsXsLjtHvofMUWQc367qEZzV7FGK1KyP2Dyjw8tcjRPnaxTEJvTLpq3wUiqcYE1sfrvqTpNiLkXNwCwXDLar3XKLP4KoHNzsLjtHvofMUWQc367qEZzV7FGK1KyP2Dyjw8tcjRPnaxTEJvTLpq3wUiqcYE1sfrvqTpNiLkptamW8X1L19VhtEvsQYgs43Jeq5ScqvdBRaVFuUgjYWNgwCwXDLar3XKLP4KoHNzsLjtHvofMUWQc367qEZzV7FGK1KyP2Dyjw8tcjRPnaxTEJvTLpq3wUiqcYE1sfrvqTpNiLkBknTXmtStgYNMzbj1L3jMyuRTJjw4KcZA5KFyBCwJjr7D1X9r6eHCGbFEebBxTwbNgd7"	

Hash (A) 的抗碰撞性统计学上等同于 Hash (B)

理性认知：

因为 SHA256 的核心安全属性，散列性和抗碰撞性，主要取决于算法本身的数学和计算特性，而不是依赖于输入明文的复杂度。这意味着无论输入数据的复杂度如何，SHA256 都提供一致的安全性水平。

那么，既然我们知道 Hash (A) .安全性（散列性、抗碰撞性）= Hash (B) .安全性（散列性、抗碰撞性）。

为什么我们觉得 hash ("1") 不安全，而 hash (B) 安全呢？因为我们关注的不仅仅是哈希的安全性。在实践中，我们跳出哈希这个维度（就像三维生物离开了纸面）关注安全性时，破解 hash (A) 的明文 A。只需要使用字典或者穷举来破解。而抗暴力破解的唯一方式就是“增加明文的长度（防穷举）、复杂度（防字典）和随机性（防字典）”。而哈希的散列性正好满足生成足够长、具有足够复杂度和随机性的字符串——作为抵抗破解的明文。

高级脑的核心“隐藏算法规则”根本不是为了提高私钥的“抗碰撞性”，因为经过哈希之后的抗碰撞性与种子本身的熵无关。高级脑只需要解决种子的“抗暴力破解”性，而，隐藏的“算法规则”（设计复杂度高的计算过程或数据结构）确保了最后生成私钥之前的那个“明文”的复杂程

度，成就了高级脑的“抗暴力破解”性质。

问题二、高级脑是否提高了记忆负担？

1、假设我将选用下面其中之一作为种子明文：

A:

202cb962ac59075b964b07152d234b70

B:

d09afe71664f2385fa8ef0a63c227bdd6942dcbb6fffd87e5d001b2a434396

请问上面两个选项哪个对记忆力负担更重？

答案肯定是 B。虽然使用 B 做 hash 种子的防暴力破解性肯定高于 A。

2、再做一次选择题：

A:

202cb962ac59075b964b07152d234b70

B:

对“达哥”进行 sha256，一共套娃 10 次，每次结果都加上“达哥”。

请问上面两个选项哪个对记忆力负担更重？

我的答案这次是 A。使用 B 做 hash 种子的防暴力破解性仍然高于 A。

两个 B 其实是同一个东西，这次显然很好记忆，因为他只有 3 个需要记忆的元素：

(1) 种子“达哥” (2) 做 sha256 10 次 (3) 每次结果后面种子原文

而 A 实际是 123 的 md5 哈希值，MD5 是一个已经公认不再安全（抗碰撞性较弱）的哈希算法，用 A 做明文，抗碰撞性和抗暴力破解性（因为长度更短）都较弱。

这个例子证明了，明文的安全性和记忆负担并不成正比。

3、再来一次选择题：

A:

please coffee bind dog carry solid album simple gun leave become illness

B:

对“达哥”进行 sha256，一共 10 次，每次结果都加上“达哥”。

请问上面两个选项哪个对记忆力负担更重？

我的答案仍然是 A。我不觉得去记忆 12 个随机的无意义的助记词的记忆负担会低于 B。

结论：

1、隐藏算法不提高抗碰撞性（也不降低），它提高的是抗暴力破解性，抗碰撞性不需要提高，经过了任意一次 sha256 的散列后就已经满足了，碰撞性与明文复杂度无关。

2、隐藏算法是提高抗暴力破解性，而算法的复杂性是可以无损压缩（参见上面的选择题的例子）而不增加记忆负担的。比如上面的后两个例子中，B 的算法规则只有 3 个元素。而且是有逻辑意义方便记忆的。

12 个助记词则是 12 个无关元素，记忆负担高于选项 B。

算法规则必须隐藏，否则就失去了“防暴力破解”性，任何人可以通过重现你的算法规则来制作穷举或者字典攻击。

3、从安全性的角度来看，一个加密的流程一定要隐藏一些元素，无非是你选择隐藏种子明文的规则性还是隐藏算法的规则性：

Bip 选择的是公开算法，隐藏种子明文的规则性，这就必然使种子明文具有巨大的随机性（熵）。而熵才是记忆力负担，只是它固化了这个负担的值，12 个单词就要记忆 12 个元素（加上密语就再加一个元素），24 个就增加一倍记忆负担。

高级脑则是选择隐藏算法的规则性，降低种子明文的随机性，使种子更好记忆。再上面的例子中，种子这个元素可以是“达哥”两个字，也可以是沁园春雪全文。加上设计精巧的“复杂而又好记”的隐藏算法，从而满足了在方便记忆的同时兼顾了防暴力破解性。

4、最后需要强调的是，如果你认同 sha256 的散列性，就不需要再就 防碰撞性 再做讨论，因为“碰撞性与明文复杂度无关”。

2024-3-16 17:44 以太坊脑钱包生成器

【新工具发布】#以太坊脑钱包生成器#

应群友 @五叶 的需求，写了一个以太坊脑钱包生成工具！

现在，你可以利用高级脑方案（网页链接）轻松生成安全的以太坊地址。🔒

✓ 功能特色：

⌚ 一键生成以太坊地址、私钥、公钥及助记词。（一维地址）

🕒 支持二维码显示，方便安全备份。

🔑 简洁易用，单文件完全开源，无需安装任何插件或软件。右键点击页面查看源码复制保存到本地***.html 文件即可在离线环境下打开使用。

💰 你可以用比特币高级脑生成的复杂种子来同时生成以太坊地址，实现一套高级脑，同时管理两种币的私钥。

🔒 安全提示：

为了您的资产安全，实际生成囤币地址时请在离线环境下使用本工具。

最初始的自然语言种子生成的一维地址可能被暴力破解，请确保使用了高级脑的方式生成了复杂且难以被猜测的脑口令作为最终的种子明文。

切勿在线上环境或公共平台分享您的私钥或助记词。

立即体验：

<https://startbitcoin.org/EthereumBrainWalletGenerator/?continueFlag=19278e79782564f74d444cc320eb651b>

我们目标是：不依赖第三方的安全 hold。记住：厚德不需要任何硬件。

程序风格借鉴了@比特币布道者的 比特币脑钱包（网页链接）。

感谢 @比特币布道者 提供的存放空间。希望这个工具能帮助你更好地管理和使用你的以太坊资产！

#以太坊##脑钱包##区块链工具#

2024-3-17 09:24 私钥安全启示录高级脑安全性探究

私钥安全启示录:高级脑安全性探究

在这个宇宙里，想象有一把独一无二的锁，每个比特币地址就是这样一把锁，而这把锁自带一把原生的钥匙——私钥。只要你看过这把钥匙，就能打开锁，获取里面的财物。椭圆曲线密码学 (ECC) 保证了这把锁与这把钥匙之间的独特配对：一个私钥对应一个公钥，没有第二把钥匙能打开这把锁。

要如何保护这把宝贵的钥匙，确保既不被他人发现其样子，又能让自己方便记忆呢？我们可以采用高级脑的方法，选择一个易于记忆的信息，如一段话，使用安全隐秘的方法将其转换成私钥。这就好比用一把我们自己定义的、易于记忆的钥匙来管理那把独一无二的锁的钥匙（从现在起，想象私钥就是一把攻击者千方百计想要打开的锁）。

这个宇宙的哈希算法，如 SHA-256，是算法规则的基础。虽然理论上存在碰撞性问题，即不同的输入可能产生相同的输出，但由于 SHA-256 的强抗碰撞性，我们不必担心突然会有另一把钥匙能打开我们的锁。我们真正需要警惕的是，有人可能尝试用他们的钥匙库，一把一把来尝试打开我们的锁——暴力破解。但只要他们无法准确猜测你的钥匙细节（脑口令和生成规则都是细节的一部分），这种尝试是注定失败的。

高级脑的反对者往往拘泥于初始脑口令的熵低，认为这降低了安全性。然而，这种观点忽略了高级脑策略的真正价值。与 BIP 等方案相比，高级脑不是依赖于助记词的随机性或熵的高低，而是通过使用强哈希算法和隐秘的算法规则来实现防碰撞性，以及解决暴力破解的风险。这一切都是为了维护整体的安全性，同时保持了口令的易记性。高级脑展示了一个原则：安全性不是为了熵，而熵是为了安全性；密码学是实现安全性的工具，而不是目的。我们应该将焦点放在如何提高安全性，而不是机械地追求数字的随机性。

因此，我们的挑战在于如何隐藏这个私钥的细节。高级脑方法通过选择一个复杂而独特方便记忆的信息串来生成私钥，实质上提高了钥匙的隐蔽性。攻击者不仅需要猜测出这个信息，还需要知道你将信息转化为私钥的确切方法。由于隐秘算法规则中含有 SHA-256 算法，我们也不担心攻击者能通过碰撞找到另一把可以使用的钥匙。

在比特币的宇宙里，每个地址所隐藏的独一无二的钥匙，只有地址的主人能识别。采用高级脑方法，利用强哈希实现防碰撞性，利用隐秘规则解决暴力破解风险，我们不仅确保了这把钥匙的安全性，同时还能便捷地通过记忆随时“复制”这把钥匙。使得比特币的使用既私密又方便。

2024-3-21 16:49 比特币脑钱包生成器

新工具发布：比特币脑钱包生成器 

一个旨在为你提供更安全、便捷的比特币存储方案的开源项目。

功能亮点：

一键生成：

使用脑口令生成助记词（仅限本软件使用）、私钥、公钥及 P2PKH、Bech32 两种格式的地址。

▲请注意▲：软件自带加盐和哈希套娃功能，但为了让最终的脑口令获得足够高的熵，请保证使用自己设计的高级规则而不是仅软件的基础功能。

助记词可以在本软件中重现私钥和地址，有利于囤饼持有人分发给实际所有人而不暴露自己的高级脑规则。

QR 码快速分享：每个生成的密钥或地址都附带 QR 码，便于安全分享或备份。

用户友好界面：简洁明了的操作流程，方便实现你的自定义高级脑规则。

获取方式：

源码地址：GitHub – BrainWalletGenerator

(<https://github.com/btcdage2000/BrainWalletGenerator/>)

下载可执行文件：GitHub Releases

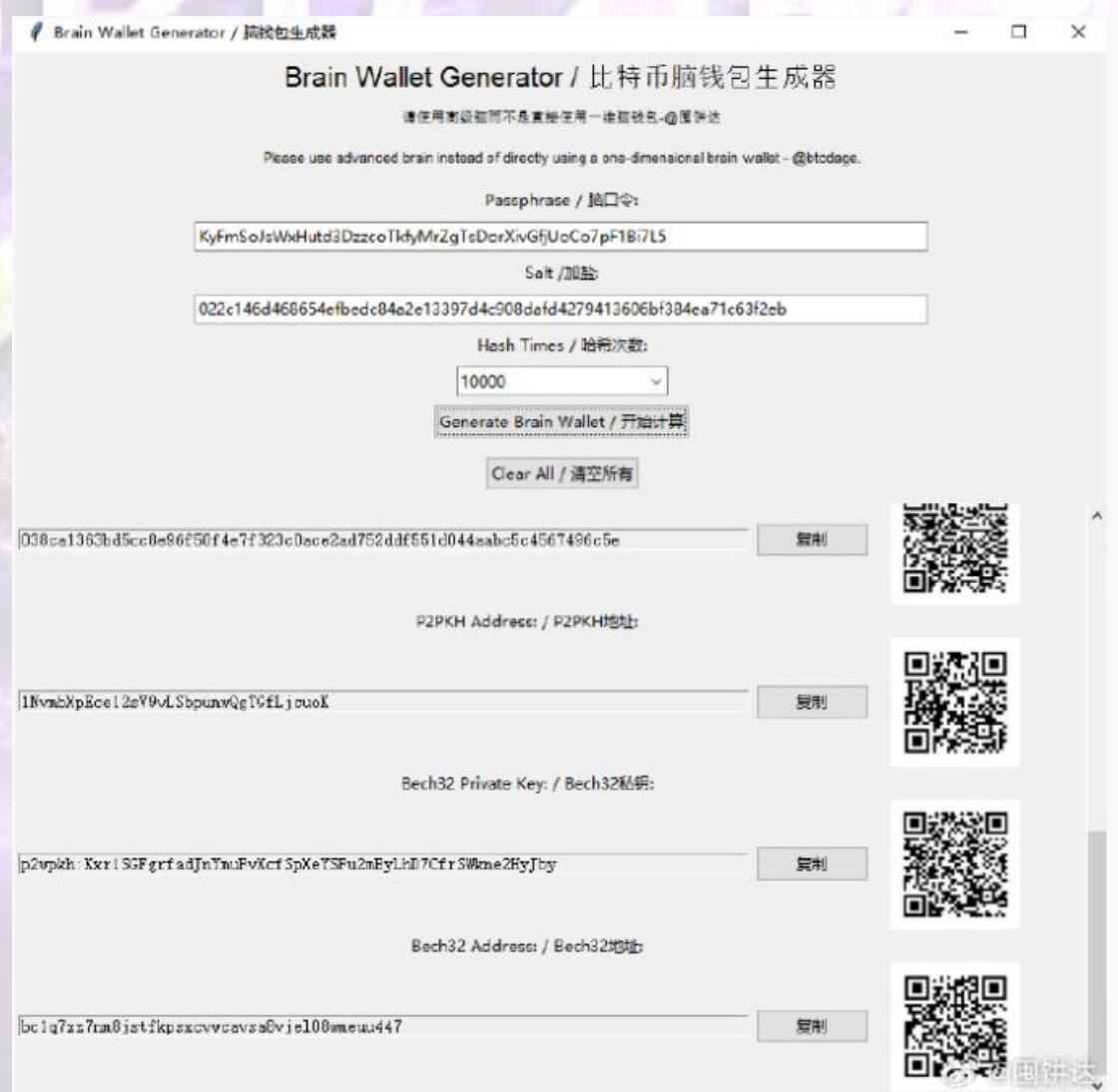
(<https://github.com/btcdage2000/BrainWalletGenerator/releases>)

为何选择脑钱包？

参见高级脑教程。

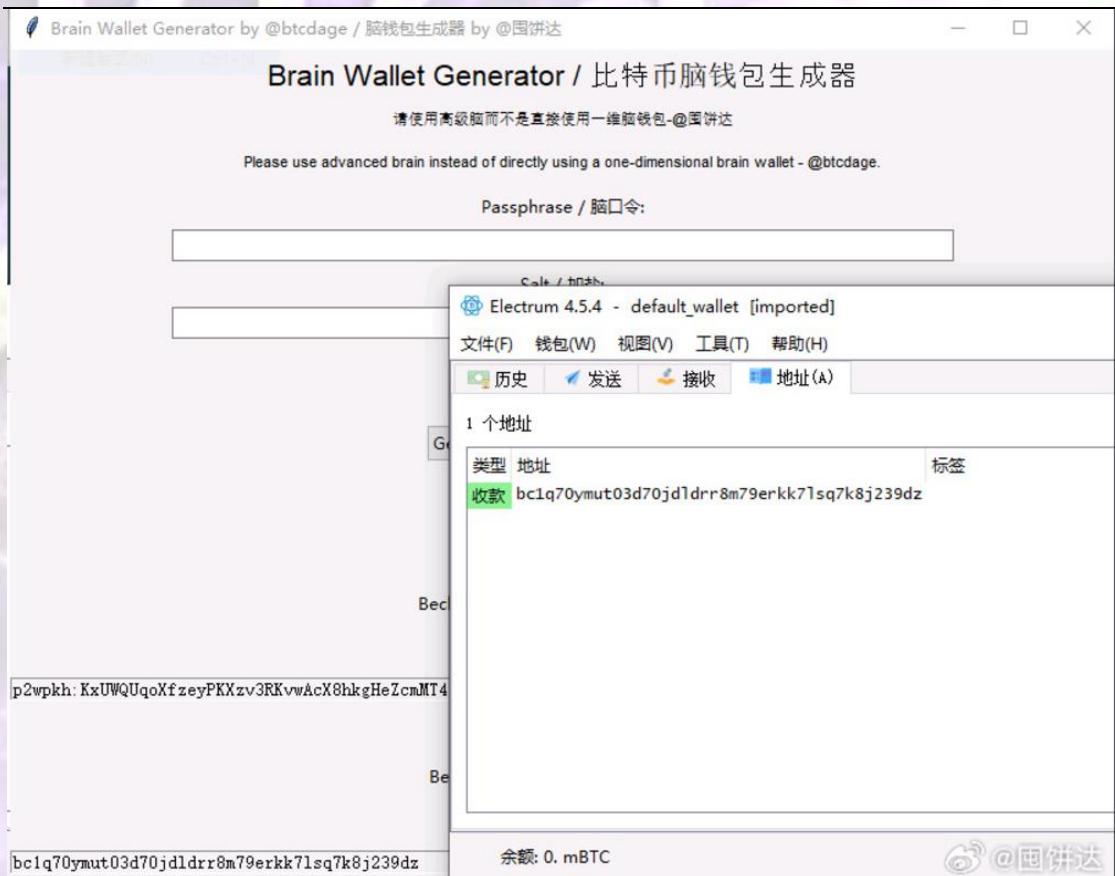
#比特币 #高级脑钱包 #加密货币安全 #区块链工具收起

囤饼之道 达哥微博精选 (2021.8-2024.11)



推荐使用 electrum 钱包软件配合进行，脑钱包地址验证，导入私钥进行转账签名等功能。

囤饼之道 达哥微博精选 (2021.8-2024.11)



2024-3-25 11:57 高级脑生成支持隔离见证的囤饼地址

【图文教程】高级脑生成支持隔离见证的囤饼地址

本文将提出了一个高级脑设计算法, 使用达哥的脑钱包生成工具来生成支持隔离见证的囤饼地址。(实际使用时, 算法由你自己设计并保密, 我这只是又一个例子, 用来激发你的想象力, 希望能起到抛砖引玉之效)

一、规则算法设计: (实际使用时, 这个算法由你自己设计, 我这只是又一个例子, 激发你的想象力, 抛砖引玉之效)

1、涉及到记忆元素: 两个脑种子 (种子 A 和种子 B)、一个“关键记忆词”、序号数使用半角阿拉伯数字。

2、种子 A + 序号数 为 脑口令 A, 把“关键记忆词”作为盐值, 哈希次数为 N, N=种子 A 的字符数量。使用达哥的脑口令软件一键生成: 私钥 A、公钥 A。

3、私钥 A 作为脑口令 B, 把种子 B 作为盐值, 哈希次数为“公钥 A 的最后三位阿拉伯数字”。使用软件生成: 私钥 B、公钥 B。

4、私钥 A+私钥 B 作为脑口令 C, 公钥 A+公钥 B 作为盐值, 哈希次数为“公钥 B 的最后三

位阿拉伯数字”。一键生成的私钥和地址就是序号数派生出的囤饼地址。

5、按照这个算法改变序号数生成其他囤饼地址。

二、具体例子便于理解（仅用序号数 1 来举例）：

种子 A：“价值是主观的”

种子 B：“放弃救人情结尊重他人命运”

关键记忆词：“我是关键记忆词我不会记录在物理世界中我只会记录在脑海中”

1、种子 A + 序号数为脑口令，盐值为“关键记忆词”，哈希次数为 N，N=种子 A 的字符数量。此例子中种子 A 是 6 个字。

脑口令：价值是主观的 1

盐值：我是关键记忆词我不会记录在物理世界中我只会记录在脑海中

哈希次数：6

得到私钥 A：L4ix5CULbyAQcPbSuMtwuCU8eTPWD922fbFt4cB7Kz26b2S7VD4Y

公钥 A：029dc05240c6fd01fea162cb954a0dba8dc06f49ac148246189096bd87e7cb7ae9

公钥 A 最后三位阿拉伯数字是：779。

2、私钥 A 作为脑口令，种子 B 作为盐值。进行 779 次哈希，一键生成信息：

脑口令：L4ix5CULbyAQcPbSuMtwuCU8eTPWD922fbFt4cB7Kz26b2S7VD4Y

盐值：放弃救人情结尊重他人命运

哈希次数：779

得到私钥 B：KzZf6zJ5gBEyyWFefMVc5dtEC9LX9acvMewfzQKFe3YB4naXN19a

公钥 B：0341804628211614707f27f32aab557918a4fe79b3af94d85546b7155119c27b15

3、私钥 A+私钥 B，作为脑口令 D，盐值为：公钥 A+公钥 B，哈希次数为“公钥 B 的最后三位阿拉伯数字”。这里是 715。一键生成的私钥和地址是序号数派生出的囤饼地址。

脑口令：

L4ix5CULbyAQcPbSuMtwuCU8eTPWD922fbFt4cB7Kz26b2S7VD4Y

KzZf6zJ5gBEyyWFefMVc5dtEC9LX9acvMewfzQKFe3YB4naXN19a

盐值：

029dc05240c6fd01fea162cb954a0dba8dc06f49ac148246189096bd87e7cb7ae90341804628

211614707f27f32aab557918a4fe79b3af94d85546b7155119c27b15

哈希次数：715

得到序号 1 派生的囤饼私钥：

p2wpkh:KygGPCUXD82n32RjeyDJbrBX8suQdJjWLDUaLyMwgxYDEgEeDKC

支持隔离见证的囤饼地址：bc1q2l7jcderafthyxs5uxln5m3skpx8mn8rfkrv2wq

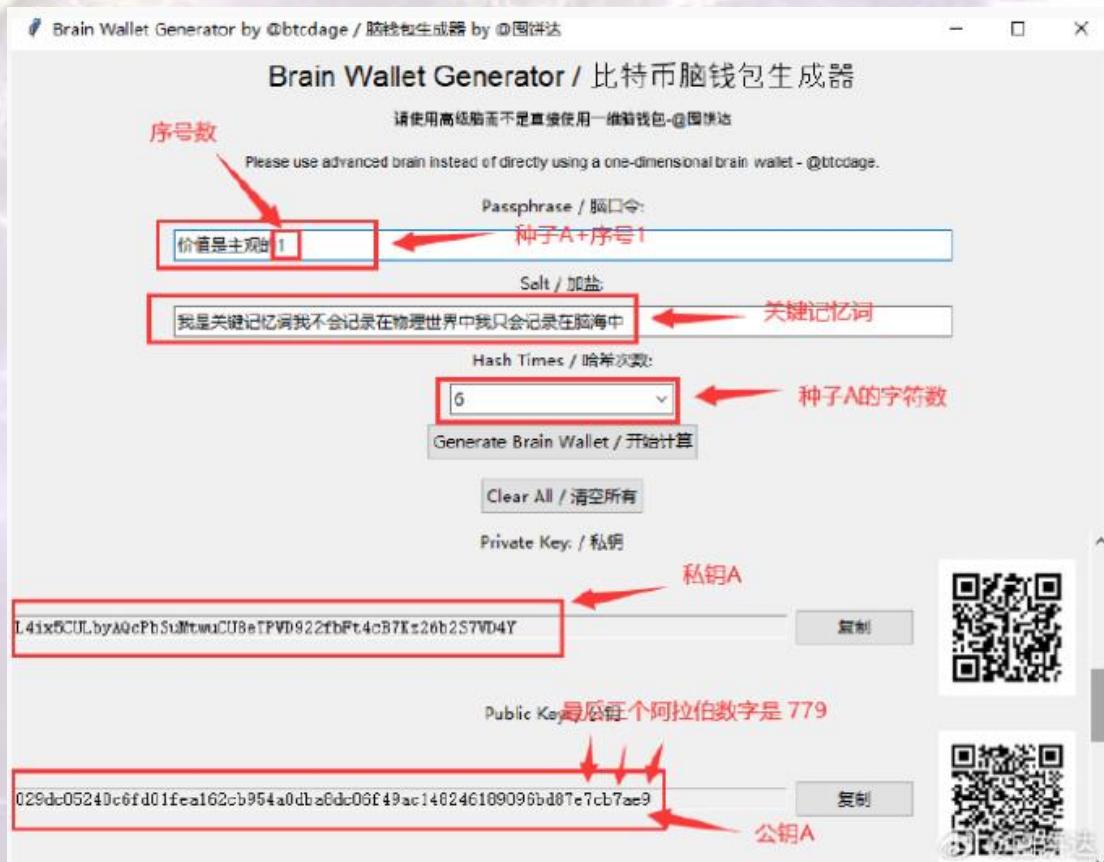
三、安全保存策略：

1. 分布式存储算法规则：建议将设计的算法规则进行分布式存储，或者将其打印多份，存放

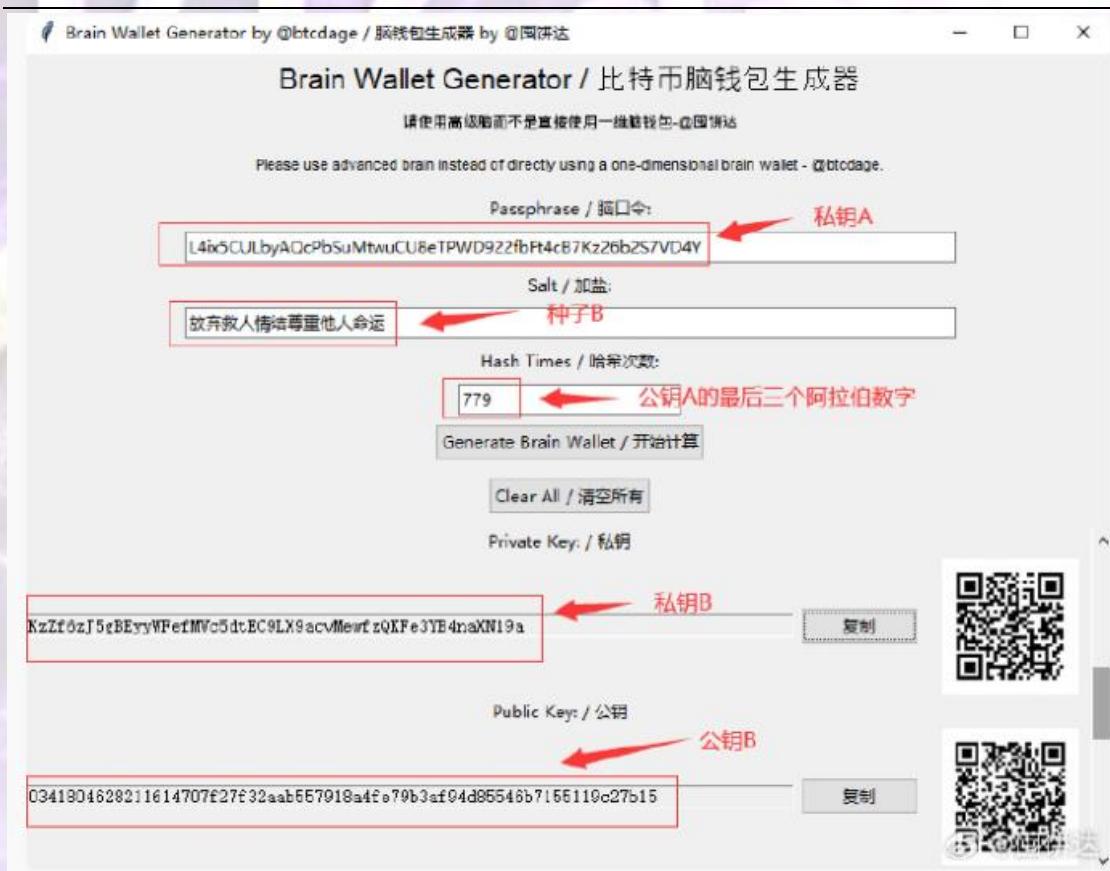
于多个安全且隐蔽的地点。务必确保算法细节不被外界知晓，以降低被暴力破解的风险。

2. 种子信息的物理存储：将两个脑种子分别记录在纸上，并保存在不同的秘密地点。同时，建议定期复习这些种子信息，以强化记忆，确保在需要时能够准确回忆。

3. 关键记忆词的心智记忆：关键记忆词应当仅在脑海中记忆，切勿将其记录在任何物理介质之上。这样做可以防止在脑种子信息意外泄露的情况下，保护资产免遭损失。



国饼之道 达哥微博精选 (2021.8-2024.11)



2024-3-28 16:34 量子计算会摧毁大饼吗

量子计算会摧毁大饼吗?

目前主要的量子算法:

【Shor 算法】:

描述: 由彼得·肖尔在 1994 年提出, 能有效解决大数分解问题和离散对数问题。

▲▲▲对大饼的威胁: 直接威胁到基于椭圆曲线数字签名算法 (ECDSA) 的大饼交易签名, 因为 ECDSA 的安全性依赖于离散对数问题的难解性。

【Grover 算法】:

描述: 由 Lov Grover 在 1996 年提出, 是一种量子搜索算法, 可以在无序数据库中以平方根时间复杂度找到特定元素。

▲▲▲对大饼的威胁: 能加速搜索哈希值的过程, 理论上对大饼的工作量证明 (PoW) 构成威胁, 但效果有限且不如 Shor 算法直接。

【量子退火 (Quantum Annealing)】:

描述: 一种量子计算方法, 通过量子退火过程解决优化问题, 尤其适用于寻找全局最小值问题。

▲对大饼的威胁: 可能对寻找大饼挖矿中的随机数有加速作用, 但相较于 Grover 算法, 其对大饼网络的直接威胁较小。

【Boson 采样】:

描述: 一种量子计算模型, 利用玻色子的特性来执行复杂的采样任务, 被用来演示量子霸权。

对大饼的威胁: 目前主要关注于展示量子计算的潜力, 并非直接针对加密算法, 对大饼网络的直接威胁较小。

【量子随机行走 (Quantum Random Walks)】:

描述: 量子版本的随机行走, 展现出与经典随机行走不同的扩散特性, 用于算法加速和量子搜索。

对大饼的威胁: 在理论上可能加速某些搜索问题的解决, 但目前尚未直接应用于攻击大饼网络的方式。

【HHL 算法 (Harrow-Hassidim-Lloyd Algorithm)】:

描述: 用于解线性方程组的量子算法, 能在特定条件下显著加速求解过程。

对大饼的威胁: 虽然 HHL 算法在解决特定数学问题上有潜在的加速能力, 但对大饼网络构成的直接威胁较小, 因大饼的核心安全问题不涉及线性方程组的求解。

在这些量子算法中, Shor 算法对大饼网络构成了最直接和最严重的威胁, 因为它能够直接破解大饼所依赖的 ECDSA 数字签名算法——这也是为什么一个地址只能用一次的原因: 公钥暴露了, 私钥也就很快被破解了, 你的币如果还在里面也就随风而去了。

Grover 算法可能对大饼挖矿过程产生影响，但这种影响相对有限，对于 SHA-256，Grover 算法能将破解时间从 2^{256} 减少到 2^{128} ，这仍然是一个极其庞大的数字。

当然，实际上量子计算机达到运行 Shor 算法解决实际加密标准所需规模的能力，还面临很多技术和物理障碍。

即使 Grover 算法可以加速哈希的搜索过程，大饼网络可以通过调整难度目标来适应这种加速，以保持区块生成时间大约为 10 分钟。

而且，随着量子计算技术的发展，新的量子安全的加密算法也在研发中。

比如：

【哈希基加密算法】：

优势：主要用于数字签名方案，基于密码学哈希函数的安全性。

应用：在保护交易签名免受量子攻击方面特别有效，因为目前没有已知的量子算法能高效解决哈希函数的抗碰撞性问题。

场景：适用于大饼交易验证，确保交易的不可篡改性和用户的私钥安全。

【基于格的密码学】：

优势：提供了一套完整的加密和签名解决方案，基于计算上认为是量子安全的格问题。

应用：除了数字签名，还能支持加密通信和构建更复杂的密码协议，如全同态加密等。

场景：适用于大饼网络的加密升级，提高整体安全性，尤其是在未来可能面对量子计算机直接攻击加密货币钱包和交易加密的情形。

大饼作为一个去中心化网络，其安全性不仅依赖于交易的签名验证，还包括用户地址和钱包加密的保护。

哈希基加密算法擅长于签名方面，而基于格的密码学能提供更全面的加密解决方案。

不同的加密技术可以在不同时间点，针对网络的不同部分进行升级。

例如，先通过软分叉引入哈希基的签名算法，随后再考虑更全面的协议升级以引入基于格的密码学。

通过软分叉引入的哈希基和基于格的密码学技术，可以让网络在不影响现有用户的前提下，逐步提升其抗量子计算的能力，既保证了大饼网络的安全性和前瞻性，又维护了网络的统一和稳定性。

量子计算会摧毁大饼系统的说法可以休矣。

2024-4-3 22:08 机遇

这次大饼的回调，许多人可能看到的是恐慌和不确定性，其实这恰恰是又一个明显信号：机会来了。

囤饼之道 达哥微博精选 (2021.8-2024.11)

我一直强调的一个观点是，法币的不断贬值对我们的财富是一种无形的侵蚀。而大饼，凭借其 2100 万的绝对稀缺性，为我们提供了一种抵抗这种侵蚀的手段。这不是空洞的说教，而是建立在对经济规律深刻理解的基础上。大饼的每一次减半，都在提醒我们，它与生俱来的稀缺性和价值。

我们讨论价值时，总会提到共识。大饼能在过去十多年中持续增值，正是因为它背后不断增强的共识。这份共识，既是对其技术的信任，也是对其价值逻辑的认同。这不仅仅是数字游戏，这是一场关于信任和共识的社会实验。

而现在，当大饼再次给我们机会时，我想说的不仅仅是“买入”。更重要的是，理解这背后的逻辑，认识到这不仅是一次财富积累的机会，更是一次站在时代前沿的机会。我提倡的定投策略，不是无脑操作，而是基于对大饼长期价值的认可和信任。

我经常强调脑钱包的重要性。这不是因为我对传统存储方式不信任，而是我更倾向于那种“人饼合一”的状态。只有当你真正掌握了自己资产的控制权时，你才能在这个充满不确定性的世界中，找到一丝确定性的安全感。

所以，对于那些还在犹豫的人，我想说的是，现在正是一个极好的时刻。抓住机会，不仅仅是因为大饼的价值，更因为这代表着一个时代的转变。我们正在见证历史，而选择如何参与，将决定你在这场变革中的位置。



2024-5-5 22:47 以太坊虚荣钱包生成器

写了一个以太坊虚荣钱包生成器，支持多线程。在 CPU:i7 12700 3.61GHz RAM:64G 的电脑

上开 20 个线程，完全跑起来以后每分钟可以计算近 500 万次，每秒约 8 万多次。

<https://github.com/btcnage2000/EthereumVanityAddressGenerator/blob/main/EthereumVanityAddressGenerator.html>

Ethereum Vanity Address Generator | 以太坊虚荣钱包地址生成器

by [btcnage](#) | 制作: 囤饼达

Vanity addresses can be used to create phishing addresses for "Address Spoofing Attacks." As a demonstration of functionality on this page, we urge everyone to carefully verify each character of the complete address before conducting any transactions. | 虚荣地址可能被用来生成钓鱼地址进行“地址欺骗攻击”。本页面作为功能演示，希望大家在操作转账时一定要逐一字符核对完整地址。

Prefix | 前缀 (hex, no '0x' | 十六进制, 不含 '0x'):

Suffix | 后缀 (hex, no '0x' | 十六进制, 不含 '0x'):

Number of Workers | 工作线程数量:

Status | 状态: Searching... | 搜索中...

Attempts | 尝试次数: 1001464640



2024-5-31 15:05 《狐狸分饼》说开去

《狐狸分饼》说开去

一、三个《狐狸分饼》的故事

《狐狸分饼》是一个经典的寓言故事，原版是这样的：

两只小熊找到了一块大饼，决定平分这块饼。为了公平起见，它们请来了狐狸做裁判。狐狸将饼分成两块，但一块明显比另一块大。为了让两块饼一样大，狐狸咬了一口较大的那块。可是，这样一来另一块又显得大了，于是狐狸又咬了一口原先较小的那块。狐狸就这样一口一口地调整，最后两块饼都被狐狸吃掉了大半，而两只小熊只得到了一点点饼屑。

这个版本的故事揭示了一个重要的道理：监管者未必总是公正和无私的，有时他们可能会利

用自己的权力为自己谋取利益。这种行为不仅没有解决问题，反而损害了当事人的利益，破坏了公平。

现在我们改变一下故事的细节。

《狐狸分饼 2》

两只小熊找到了一块大饼，决定平分这块饼。分饼的小熊因为自私，给自己分了 90% 的饼，只给另一只小熊留了 10%。（不良商家侵害消费者权益）另一只小熊觉得不公平，于是找来了狐狸评理。（消费者投诉举报）狐狸一口咬掉了大块的饼的 80%，说这下公平了。（官方处罚不良商家）

这个故事揭示了行政处罚的本质，即通过削减违规者的利益来达到公平的表象，但实际上并未真正补偿受害者，甚至可能让第三方（如执法者）获得好处。这种形式的公平往往只停留在表面，无法有效纠正不公正行为，也不能真正保护受害者的权益。

《狐狸分饼 3》

两只小熊找到了一块大饼，决定平分这块饼。分饼的小熊因为自私，给自己分了 90% 的饼，只给另一只小熊留了 10%。（不良商家侵害消费者权益）另一只小熊觉得不公平，于是找来了狐狸评理。（消费者投诉举报）狐狸决定进行惩罚性赔偿，将大块的那份分给了受害者小熊，而自私的小熊只能得到 10% 的饼。（惩罚性赔偿给消费者）

这种惩罚性赔偿制度不仅纠正了不公正行为，还对施害者进行了惩罚，同时充分补偿了受害者，恢复了真正的公平。这种制度强调对不公正行为的严厉打击和对受害者的全面补偿，有助于维护社会的公平正义。

二、行政处罚制度的弊端

现实生活中，行政处罚制度广泛应用于各种违法违规行为的处理，但其弊端显而易见。

1、无法充分补偿受害者

行政处罚往往以罚款为主，这些罚款通常归政府所有，而不是直接补偿受害者。受害者在受到损害后，无法通过行政处罚获得应有的赔偿，甚至需要自行承担维权的成本和风险。

2、可能导致执法不公

行政处罚权力集中在执法机关，容易导致执法不公。执法人员可能滥用权力，通过罚款谋取私利，或在执法过程中偏袒某些利益群体，无法实现真正的公平公正。

3、更容易被收买

掌握监管和惩处权利的部门更容易受到利益诱惑，可能会被不法分子收买，导致执法腐败。这不仅损害了公平公正的原则，还可能让违法行为更加猖獗。

4、缺乏震慑力

对于一些大企业或富有的个人而言，行政罚款金额相对较小，无法对其形成有效震慑。违规

者可能视罚款为经营成本的一部分，继续进行违法行为，无法有效遏制不法行为的发生。

三、惩罚性赔偿制度的优势

惩罚性赔偿制度作为一种补充和改进，能够有效弥补行政处罚制度的不足，并在多个方面发挥重要作用。

1、充分补偿受害者

惩罚性赔偿制度旨在对受害者进行全面补偿。通过要求违规者支付高额赔偿金，不仅可以弥补受害者的直接损失，还可以覆盖其维权成本和精神损害。这种制度有效保障了受害者的合法权益。

2、增强震慑力

惩罚性赔偿制度的赔偿金额往往远高于实际损失，对违规者形成强大的经济压力和心理震慑。特别是对于那些财力雄厚的企业和个人，高额赔偿金能够有效遏制其违法行为，从而维护市场秩序和社会公平。

3、促进社会公平正义

惩罚性赔偿制度通过严厉打击不法行为，维护社会公平正义。它不仅对施害者进行惩罚，还通过补偿受害者来恢复受损的公平。这种制度有助于增强公众的法律意识和公平观念，推动社会和谐发展。

4、防止执法腐败

惩罚性赔偿制度将赔偿的重点放在受害者身上，减少了中间环节，使得执法部门不容易受到利益诱惑，从而降低了执法腐败的风险。受害者直接受益，公平性更高，透明度更强。

5、提高受害者的维权收益

惩罚性赔偿可以让受害者（消费者）的维权收益变高，更倾向于维权。受害者在知道自己有机会获得高额赔偿后，更有动力去维权，这进一步增加了商家的违法成本和赔偿风险，有利于推动公平正义。而相反，行政处罚却做不到这一点，无法有效激励受害者维护自己的权益。

四、惩罚性赔偿制度对食品安全的促进作用

食品安全问题是关系到公众健康和生命安全的重大问题。近年来，食品安全事件频发，严重影响了公众的信任和社会稳定。在食品安全领域引入惩罚性赔偿制度，能够有效促进食品安全水平的提升。

1、严惩食品违法行为

通过惩罚性赔偿制度，对生产和销售不合格食品的企业和个人进行严厉惩罚，能够有效打击食品违法行为。高额赔偿金不仅可以弥补消费者的损失，还能对违规者形成强大的震慑，促使其遵守食品安全法律法规。

2、保障消费者权益

惩罚性赔偿制度能够保障消费者的合法权益。在食品安全事件中，消费者作为受害者，往往面临维权难的问题。通过惩罚性赔偿制度，消费者可以获得充分的补偿，增强维权信心，提高维权效率。

3、提升企业责任感

惩罚性赔偿制度要求企业对其产品质量和安全负有更高的责任。面对高额赔偿风险，企业会更加重视食品安全管理，加强质量控制，提升产品安全性，从而提高整体食品安全水平。

结论

通过《狐狸分饼》故事及其延伸，我们深入探讨了行政处罚制度和惩罚性赔偿制度的不同之处。

行政处罚制度在实际应用中存在诸多弊端，无法充分补偿受害者，且缺乏震慑力。

而惩罚性赔偿制度能够有效弥补这些不足，通过对违规者的严厉惩罚和对受害者的全面补偿，促进社会公平正义和食品安全等领域的改善。

引入和完善惩罚性赔偿制度，是构建公平正义社会的重要举措，有助于提升公众的法治意识和社会整体文明水平。

2024-6-13 11:33 放弃高考焦虑，囤大饼迎接未来

放弃高考焦虑，囤大饼迎接未来

随着高考季节的落幕，这一备受全国瞩目的事件再次引发了广泛讨论。然而，在当前的Z世代环境和人工智能技术的快速进步背景下，这条曾被视为阶层流动的通道正变得日益狭窄。对于大多数家庭而言，现在是时候重新审视教育资源的分配与未来财富积累之间的平衡了。

二十年前，高考被广泛认为是通向成功的关键途径。但是，随着社会阶层的日益固化，公务员、事业单位和国有企业等依赖税收的阶层通过血缘关系扩张其影响力，社会流动性大大降低。在政府的默许和鼓励下，民间对资本的敌视情绪不断升温，导致企业家逃离国内，外资撤出。私有企业作为劳动力市场的主要贡献者，其数量的减少加剧了就业难题。伴随着失业率的上升和大学毕业生人数的增加，即使是来自985、211高校的毕业生也面临失业的困境，更不用说其他普通高等教育机构的毕业生了。

很多人还没有意识到，在目前局势的发展下，对于大多数家庭而言，为子女进行大量的补课和教育投资，希望通过高考改变命运，已经收益甚微。除非孩子具有非凡的学习天赋，否则这些投资的经济效益极低，反而给家庭带来更大的经济压力。在这个时代背景下，重新考量教育投资的回报已很必要。

随着人工智能（AI）技术的突飞猛进，使得高考生应试教育所培养的许多技能和知识迅速过时。AI不仅能够高效完成重复性工作，还在数据分析、语言处理等领域超越了人类。因此，传统教育体系下的优势在AI时代渐失色彩，即便是成绩优异的学生，也不一定能在未来职场获得优势。

尽管接受教育是必要的，且精英教育对于某些人而言是必需的，但并非每个人都需要成为精英。特别是在当前的环境下，即使成为精英，在国内也难以获得匹配的生活和工作待遇。如果孩子天生具有精英潜质，投资其出国发展无疑是最佳选择，这可能更有助于其天赋的发挥和潜力的实现。

作为一种去中心化、抗通胀的数字资产，大饼的长期投资价值已得到证实。随着全球对大饼接受度的提高，与其把财务资源投入到应试教育的额外支出，不如直接囤大饼，对子女的未来更为明智。

面对社会结构的固化、人工智能技术的发展以及就业市场的挑战，教育投资的经济效益正在下降。在未来充满不确定性的情况下，寻找更稳健的生存策略至关重要。而大饼，可能正是其中的一个解答。需要注意的是，本文主要面向普通家庭，对于既得利益阶层而言，则可能不具参考价值。

2024-11-1 15:45 桌面币价小组件

分享一个悬停桌面的币价小组件，可自定义透明度。

<https://pan.baidu.com/s/1mStbBH-6qp3wMh7fk8oTPQ?pwd=hjzt#list/path=%2F>



2024-11-14 20:04 达哥指数：用科学化指标预测市场热度

达哥指数：用科学化指标预测市场热度 🔥

牛市中常有人问：牛市何时结束、顶又在哪儿。

对我们囤饼人而言：“1 BTC = 1 BTC”，并不关心顶部在哪，更不会去做所谓的逃顶。

但是为了用有限的法币能定投到更多的大饼，还是可以通过一些科学化的方式来关注市场的热度。因此，我特别推出了“达哥指数”——一个大饼市场热度的衡量标准。

● 达哥指数的原理：

达哥指数综合考虑了两个因素：次季期货合约与现货价格的偏离度，以及距离交割日的时间衰减因子，来量化市场的热度。具体来说：

次季偏离度 (Deviation)：通过计算期货合约价格与现货市场价格之间的差异，得出偏离度。例如，若期货价格比现货价格高 10%，那么偏离度就是 10%。

时间衰减因子 (Time Compensation Factor)：随着期货合约交割日临近，市场对价格偏离的敏感度会逐渐减弱。距离交割日越远，偏离度的影响越大；而随着交割日的接近，市场的敏感度逐渐下降。

● 达哥指数 (Heat Index) 的计算方式：

公式如下：

新版公式：

$$\text{Heat Index} = \text{AdjustedDeviation}/A$$

$$\text{AdjustedDeviation} = (\text{次季合约价} - \text{现货价}) / \text{现货价} \times 500$$

$A=\max(1/180,\min(1,\text{剩余天数}/180))$ ，确保 A 的范围在 [1/180,1]。

AdjustedDeviation 是 偏离度的倍数（次季合约价格与现货价格偏离的程度乘以 5）。
A 是时间衰减因子，A 的值随着距离交割日的临近逐渐减小，最大为 1（距离交割日远）到 0（距离交割日近）。

Heat Index 就是最终的“达哥指数”，数值范围 0 到 100，数值越高，市场热度越高，越接近 100，表示市场可能进入疯狂阶段。

■ 理论支持：

价格偏离与市场情绪：期货合约价格和现货价格之间的差异能够反映市场情绪。价格差距越大，往往意味着市场情绪越乐观，反之亦然。

时间衰减与市场波动：随着交割日的临近，市场的价格波动对未来走势的影响会逐渐减弱。引入时间衰减因子后，达哥指数能够更精准地反映市场动态。

■ 达哥指数的应用：

市场过热警告：达哥指数超过 75 时，表示市场进入过热阶段，可暂停定投等待机会。

市场冷淡评估：达哥指数低于 20 时，表明市场情绪冷淡，交易量可能较低，适合耐心等

待市场情绪回暖。

定投决策参考：当指数在 40-75 之间，市场较为活跃，可以适当减少定投资金；而低于 20 时，可以放心进行定期定额投资。

如何看待达哥指数？

达哥指数为你提供了一个直观的市场温度计，帮助你做出更加明智的定投决策。精准的热度评估能帮助你有效规划定投份额，增加饼含量增加的机会。

达哥指数历时曲线（每日更新，无需魔法）

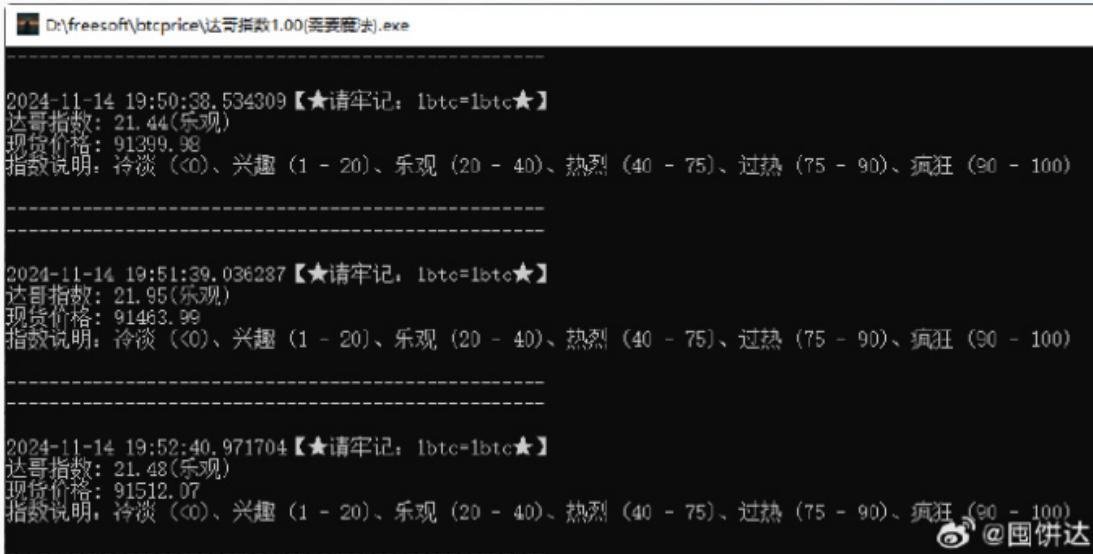
<https://btcdage2011.github.io/btcdage/dgzs.html>

备份：

<http://startbitcoin.org/dagezhishu>

感谢@比特币布道者 提供备份空间。收起





新版公式：

$$DGZS = \frac{AdjustedDeviation}{A}$$

- $AdjustedDeviation = \frac{\text{次季合约价} - \text{现货价}}{\text{现货价}} \times 500$
- $A = \max(1/180, \min(1, \text{剩余天数}/180))$, 确保 A 的范围在 $[1/180, 1]$.

算法模型

输入：

1. 现货价格 (*SpotPrice*)
2. 次季合约价格 (*FuturePrice*)
3. 当前日期 (*CurrentDate*)
4. 次季交割日 (*ExpiryDate*)

计算步骤：

1. 计算价格偏离度：

$$Deviation = \frac{FuturePrice - SpotPrice}{SpotPrice}$$

2. 调整偏离度：

$$AdjustedDeviation = Deviation \times 500$$

3. 计算剩余天数权重 *A*：

$$A = \max(1/180, \min(1, (ExpiryDate - CurrentDate)/180))$$

4. 计算达哥指数：

$$DGZS = \frac{AdjustedDeviation}{A}$$

输出：

- 达哥指数 (*DGZS*)：定量化市场热度。
- 市场状态标签：根据 *DGZS* 的值输出“冷淡”、“兴趣”、“乐观”、“热烈”、“过热”或“疯狂”。

2024-11-16 11:44

“达哥指数”是一个基于真金白银交易数据的市场热度衡量标准。

④ **市场数据的真相**

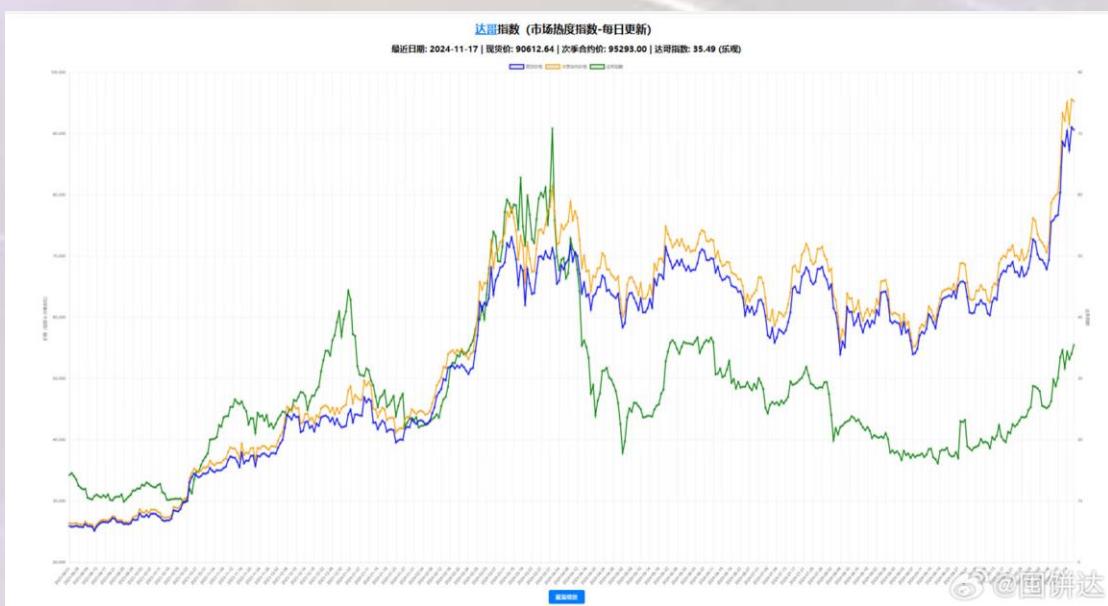
在信息爆炸的时代，各种社交媒体指标如谷歌搜索率、推特关注率等，虽然能提供市场情绪的侧面反映，但它们真的能准确预测市场动向吗？达哥认为，真正的市场热度应该由实际的交易行为来定义。因为“真金白银不会说谎”，它们是市场参与者用真金白银“投票”的结果，是最真实的市场声音。

☒ **为什么选择某安？**

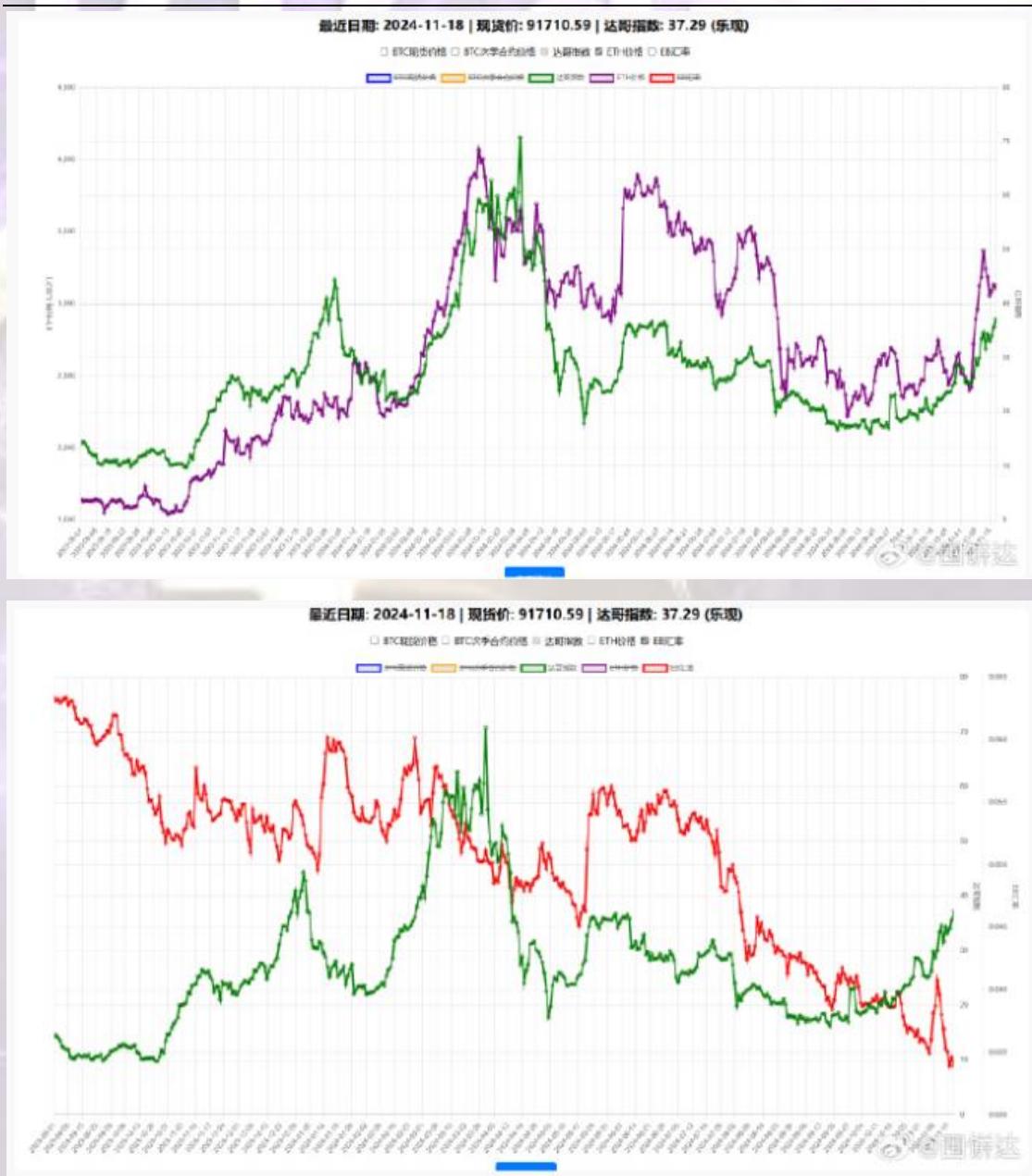
达哥指数的计算选择某安作为数据来源，因为它是目前全球交易量最大的交易所之一。某安的数据更为可靠，反映了全球市场一致的真实数据。搬砖套利者的存在使得不同交易所之间的价格迅速趋于一致，因此，最大的交易所往往能提供最全面、最准确的市场信息。

❖ **达哥指数的优势**

与那些依赖于谷歌搜索率、推特关注率等社交媒体指标的指数相比，达哥指数基于实际的交易数据，更能反映市场的真实热度。它屏蔽了各种噪音和谎言，提供了一个更为准确和可靠的市场热度指标。



囤饼之道 达哥微博精选 (2021.8-2024.11)



2024-11-22 17:02 BBB聪之道BBB上线

◆ BBB聪之道BBB上线啦! 🎉

十几年间，每天、每周、每月、每年 BTC/USD/CNY 汇率变化，尽收眼底！曲线图每日更新。
知道现在一块钱能买多少聪吗？顶部实时数据每分钟更新！

★ 亮点功能：

- ✓ 详细历史曲线
- ✓ 每日达哥指数
- ☒ 探索市场动态，感受数据的力量，立即体验吧！

➲ BBB 聪之道BBB：市场热度 & 汇率历史

<https://btcdage2011.github.io/btcdage/sats.html>

另：✓ 桌面组件已更新功能，右键菜单直达BBB聪之道BBB



< 返回

聪之道

...

达哥指数历史曲线 (每日更新) BBB 聪之道
BBB 实时达哥指数(需要魔法) 软件下载
达哥微博 比特币布道者网站

聪之道

实时行情：2024-11-22 17:03:13 (每分钟自动更新)
【BTC/USD】1比特币=98852.06美元 | 【BTC/CNY】1比特币=715906.36元 | 【USD/Sats】1美元=1011.61聪 |
【CNY/Sats】1元=139.68聪 | 【USD/CNY】1美元=7.24元 | 【CNY/USD】1元=0.14美元

开始日期： 结束日期：
 粒度： 【注
意：历史曲线数据会滞后一天。】

微博 @囤饼达

2024-11-24 19:41 比特币的时代见证者：@囤饼达 达哥的探索与启迪

[拜拜][拜拜]
//@比特币布道者

【比特币的时代见证者：@囤饼达 达哥的探索与启迪】

By HodlGpt
2024.11.24

一、初探比特币的世界 (2011)

2011年，因工作的缘故，达哥首次接触到比特币。那时的比特币还只是极少数技术爱好

者关注的“玩具”。出于对新技术的兴趣，达哥下载了比特币钱包 Bitcoin Core，并在笔记本上运行挖矿软件连接矿池，用 CPU 断断续续挖了几周。尽管显卡挖矿当时已成为主流，他还是用 CPU 成功挖出了 0.1 个比特币。由于挖矿对工作有一定干扰，且当时的比特币价值低得微不足道，达哥暂停了这项尝试。多年后，这段挖矿经历被他戏称为“一次低成本的数字实验”。

二、2013 年的遗憾（2013）

2013 年，达哥以不到 1000 元的成本购买了 6 个比特币，但由于保管不善，这 6 个比特币最终丢失，令他十分懊悔。时间来到 2021 年，在一次偶然的整理中，达哥竟意外找到了 2011 年挖矿所得的 0.1 个比特币。这笔“遗产”现在已价值约 7 万元。

三、重返加密货币（2017）

2017 年初，随着比特币和以太坊的价格飞涨，达哥的老朋友 C 先生 向他提起，用显卡挖矿以太坊（ETH）正在成为热点。尽管达哥当时对比特币的认知仍停留在“价值并不稳固”的看法上，但 ETH 的智能合约和矿工生态吸引了他的注意。他决定不走常规路线，而是开发 多币种的中文挖矿软件。

四、深耕挖矿软件

达哥先后推出支持 ETH、ETC、ZEC、XMR 等多个 POW 币种的挖矿软件，迅速积累了大量资产。这一阶段，他从挖矿抽水中获得了人生的第一桶金。

此时 ICO 热潮席卷全球，达哥也参与了一些项目，获得了短期浮盈。但绝大多数 ICO 项目最终成为“空气币”，让他深刻认识到加密市场的泡沫与风险并存。

五、BCH 硬分叉的震撼

当年比特币社区围绕“大区块之争”爆发分歧，催生了 BCH (Bitcoin Cash)。虽然没有直接参与争议，但当 Coinbase 上线 BCH 时，达哥感受到了市场的震动。他将部分 ETH 兑换为 BTC 和等值的 BCH，确保资产布局的平衡。尽管他对 BTC 的兴趣仍未完全觉醒，但这一举动成为后续转变的伏笔。

六、熊市中的技术与思考（2018-2020）

随着市场进入寒冬，挖矿生态逐渐降温。达哥的挖矿收入随之减少，但技术成本低廉的优势让他得以继续稳健运营。

七、门罗币与中心化的反思

在跟踪门罗币（XMR）频繁的算法更新时，达哥发现其开发团队对项目拥有绝对主导权，认为这种“算法集中化”与真正的去中心化理念背道而驰。这种观察进一步促使他对比特币的三权分立机制产生兴趣，并逐步认识到比特币作为“去中心化资产”的独特性。

八、数字人民币测试的觉醒

2020 年，数字人民币测试的消息引发了达哥对金融控制与自由的深刻思考。他将数字人民币视为“电子粮票”，其“可控性”是对个体自由的威胁，是一种计划经济的倒退。这一认知促使他重新审视比特币，开始研究其底层机制和经济原理。通过阅读奥地利学派经济学的经

典书籍，他强化了对自由市场与稀缺资产价值的理解，并逐步将场外资金转化为 BTC。

九、DeFi 的热潮与代价 (2021)

2021 年的 DeFi 之夏吸引了全球目光，达哥也将手中的 ETH 投入到 DeFi 生态中。与此同时，他清仓了 BCH、ETC 等资产，集中资金布局 BTC。

十、套利与风险

在这段时间，他尝试了 CEX 借贷+DeFi 套利的组合策略，通过 资金费套利、次季合约贴水套利 等手段获利。然而，风险也接踵而至。一次 QBT 合约漏洞 让他在 PancakeBunny 的存款损失了十几万 U。这次教训让他深刻认识到 DeFi 的核心风险点在于智能合约安全，同时也让他对 CEX 平台的透明性保持警惕。

十一、技术的深入

这一年，他开发了多个智能合约应用，并开始研究比特币脑钱包技术。他撰写了一套高级脑钱包方案，并与@比特币布道者 深入交流，还因此结识了@拖拉机。他们在探讨技术的同时，也为推动比特币科普奠定了基础。

【信念的确立与全仓 BTC (2022-2024)】

十二、ETH 转 POS 后：“比特币之外皆山寨”

当以太坊在 2022 年转向 POS (权益证明) 后，达哥对 ETH 完全失去了兴趣。他认为，POS 的中心化倾向与公平性问题，使 ETH 无法再与比特币相提并论。自此，他提出“比特币是价值观的选择，自由主义的锚定物”。因此“比特币之外皆山寨”。他逐步将 ETH 和其他 PoS 币种分批兑换为 BTC，同时创建了比特币定投方案。他的策略包括金字塔定投和鸡尾酒定投法等，并通过多篇科普文章推广比特币的理念与技术知识。

十三、去中心化的探索：Nostr 协议

2023 年，Nostr 协议因其去中心化特性引起了达哥的关注。他深入研究了这一协议的特性，并撰写了多篇文章宣传去中心化的重要性。在推广过程中，他结识了@阿剑、@ale 等圈内朋友，并与他们在理念传播和技术应用方面展开合作。

十四、达哥指数与“聪之道”：量化市场热度

2024 年，他结合市场数据设计了 达哥指数，通过次季合约偏差值判断市场热度。此外，他推出了“聪之道”历史曲线工具，为圈内用户提供比特币汇率历史数据查询服务。这些工具不仅帮助更多人理解比特币市场，更反映了他推动比特币普及的愿景。

十五、微博变迁：从“btc 达哥”到“囤饼达”

达哥的微博旅程并非一帆风顺。他的首个微博账号“btc 达哥”因分享比特币知识而被封，但他并未因此停下脚步，而是开启了新账号“囤饼达”，继续以务实的态度传播比特币相关知识。

十六、结语

囤饼之道 达哥微博精选（2021.8-2024.11）

从 2011 年的一台笔记本到 2024 年的聪之道，达哥的故事是一部从技术尝试者到比特币信仰者的蜕变史。在他的旅途中，C 总、@比特币布道者、@拖拉机、@阿乐、@阿剑 等朋友成为了他的同行者，共同推动了加密货币的传播与发展。

达哥的经历不仅是他个人的成长史，更是一段币圈发展的重要见证。

2024-11-28 14:58 冲击 10 万美元

最近的行情真是让人心跳如鼓。大饼一口气冲到接近 10 万美元，只差最后一哆嗦，却突然回撤了 8000 多美元，一片看空声音随之而来。

是的，市场的“熊哀鸦”又开始唱歌了。可你再看，大饼只用了短短几天就涨回到了 95000 美元以上。

朋友们，这背后其实是一场必然发生的“十万美元大戏”，只不过戏里戏外，我们囤饼人都需要一颗沉着的心。

为什么 10 万美元以下是过去式？

饼的稀缺性是根基

大饼总量恒定 2100 万，而随着矿工奖励的减半，进入流通的增量越来越少。而且，据统计，至少有 400 万个大饼因为私钥丢失等原因永远无法找回。这意味着你现在能买到的每一聪，未来都会成为市场争抢的“硬通货”。

机构的长线布局

别被短期波动迷惑，回撤只是主力资金清理浮筹的操作。你知道吗？许多机构已经开始将大饼视为数字黄金，作为通胀时代的避险资产。而在全球印钞机日夜轰鸣的大背景下，机构囤饼的脚步只会越来越快。市场上浮动的筹码将被持续吸走——10 万美元以下，几乎是他们的“安全区”。

心理关口的突破即将完成

我们知道，从 1 美元到 1 万美元，大饼每一次心理价位的突破，都伴随着更强的市场共识。这次，十万美元可能只是下一个 100 万美元的起点。今天的“心惊肉跳”，未来看或许只是历史中的“小浪花”。

10 万美元是大饼的“新底”

现在很多人因为大饼的“跌涨轮回”患得患失。其实要明白一个朴素的道理：每一次下跌，都是下一轮牛市的助燃剂。为什么？因为回调清洗的是短线投机者，而每次长线资金接盘后，大饼的底部只会更高。十万美元以下的买入机会，真的已经不多了。

看看饼本位的逻辑吧：

“你用贬值的法币换取了通缩的比特币，这是一种用弱货币换强货币的行为。人类的历史，总是站在正确的共识一边。”

对囤饼人来说，时间就是胜利

你只需要记住一件事：囤饼的成本不在于价格波动，而在于你能否拿住你的信仰。

市场就是这样，每一次上涨都会带来怀疑，每一次回调都会伴随恐惧。

可是，大饼的长期趋势就像一条向上的曲线，摆脱不了短期波动的你，将无法分享到时间的红利。

“大饼的盟友，是全球央行无尽的印钞机。”

10万美元，只是开始。现在上车，回头看，你会感谢今天的自己。

市场总是波涛起伏，但大饼的价值却像一颗恒星，越燃烧越耀眼。冲破十万，不是“会不会”，而是“何时”。

而你现在的选择，将决定你未来是否有资格享受胜利的盛宴。

千万记住：便宜的大饼永远是过去的故事！10万美元以下的大饼，或许你再也见不到了。

附录（达哥制作的AI插图）

btcage:



2024-2-20 23:06 纹身:



2024-2-21 11:21 上车：



微博@囤饼达

2024-2-23 15:23 元宵节：



2024-2-23 19:26 万有引力:



微博 @囤饼达

2024-2-25 18:43 霸王龙：



微博 @囤饼达

2024-2-27 08:27 华尔街：



微博 @国饼达

2024-2-28 19:06 方舟:



2024-2-28 21:23 回归 6W:



微博 @围饼达

2024-2-28 23:22 兑人民币新高：



2024-2-29 10:07 人类四大发明（发现）

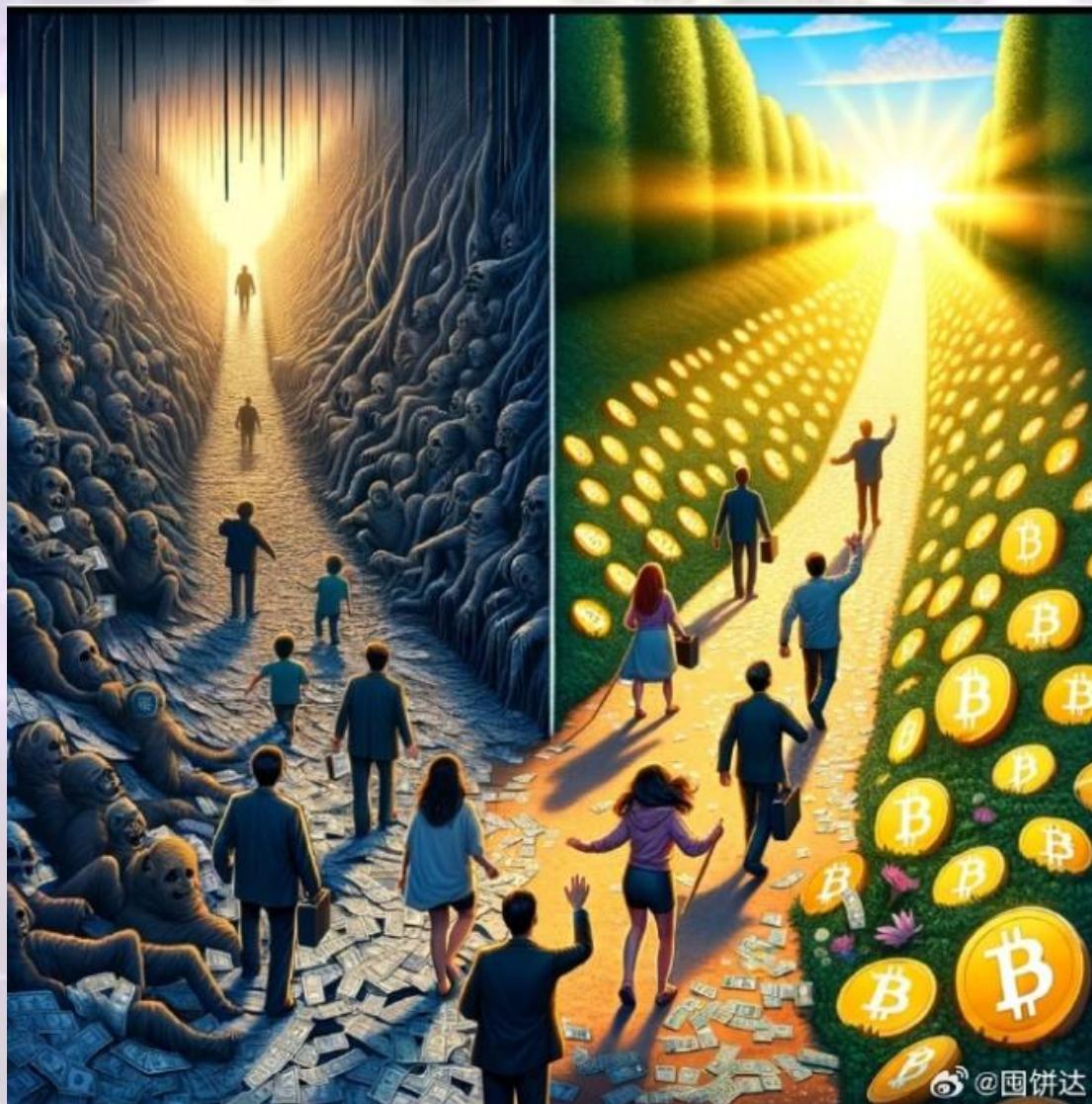


2024-3-1 10:48 见证奇点：



微博 @囤饼达

2024-3-4 00:14 阳光大道：



2024-3-4 11:37 性感叙事：



微博 @囤饼达

2024-3-5 20:21 囤饼达:



2024-3-5 23:05 新高 69K:



2024-3-8 00:11 三八节:



微博 @国饼达



微博 @国饼达



2024-3-9 00:26 突破 7W:



2024-3-13 14:03 最好的货币：



2024-3-29 15:43 稚问：



2024-4-3 22:08 机遇：



微博 @囤饼达

2024-4-10 08:28 小事改变未来：



微博 @囤饼达

2024-4-20 08:11 減半:



微博 @囤饼达

2024-6-1 08:50 六一儿童节:



2024-6-10 09:31 端午:



微博 @围饼达

2024-6-18 09:33 仕女图:



2024-11-21 12:04 比特牛：



2024-11-25 21:36 超级赛亚人：



@围饼达



微博 @国饼达

致谢

本书的完成，离不开许多朋友和同行者的支持与启发。特别感谢以下人士：

C 先生：引领达哥进入以太坊挖矿领域，开启新世界的大门。

@比特币布道者：在比特币技术和理念传播方面的启发与合作。

@拖拉机、@阿乐、@阿剑、@ale：在去中心化协议和技术研究上的支持与交流。

社区成员与读者：在传播比特币理念和推广技术知识中，给予了达哥宝贵的反馈与支持。

感谢所有直接或间接支持达哥探索之旅的人，正是这些点滴努力，共同铸造了加密货币领域的繁荣与未来。

版权声明

版权所有 ©2024 @btcdage。

本书仅为个人学习与交流使用，所有内容为非公开发布，未进行任何形式的商业印刷或销售。本书中涉及的观点与内容，仅代表作者个人见解，与任何机构、组织或第三方无关。

本书并非正式出版物，未申请任何出版号或书号，属于私人收藏。内容部分来源于公开网络，整理编辑仅为记录个人思考与见证时代发展之用，绝无冒犯或侵权意图。

特别声明

本书内容涉及比特币及相关技术，仅为信息分享用途，所有投资与行为风险由读者自行承担。

本书不得以任何形式复制、传播或用于商业用途，违者责任自负。

若书中内容涉及版权争议，请联系作者及时调整或删除相关内容。

封面设计：@btcdage

排版制作：@btcdage

完成日期：2024 年 12 月



kwhh4wguzzqknP8p7l5nyzzqc3z5

@BTCdage



kvvh4wguzzqknP8p7l5nyzzqc3z!