

- 現職
 - 帳聯網路科技股份有限公司-資深軟體工程師
- 工作經歷
 - 宏達國際電子股份有限公司-資深軟體工程師
 - 仁寶電腦工業股份有限公司-軟體工程師
- 學歷
 - 長庚大學-資工所
 - 長庚大學-資工系





도라에몽

©1970-2008 Fujiko Pro



回到4年前...

3000美金







中國信託銀行
CTBC BANK

 台新銀行



凱基銀行
KGI BANK



臺灣銀行
BANK OF TAIWAN



Fubon Bank
富邦銀行



獲利檢視...



BENZ e250價值300萬元新台幣

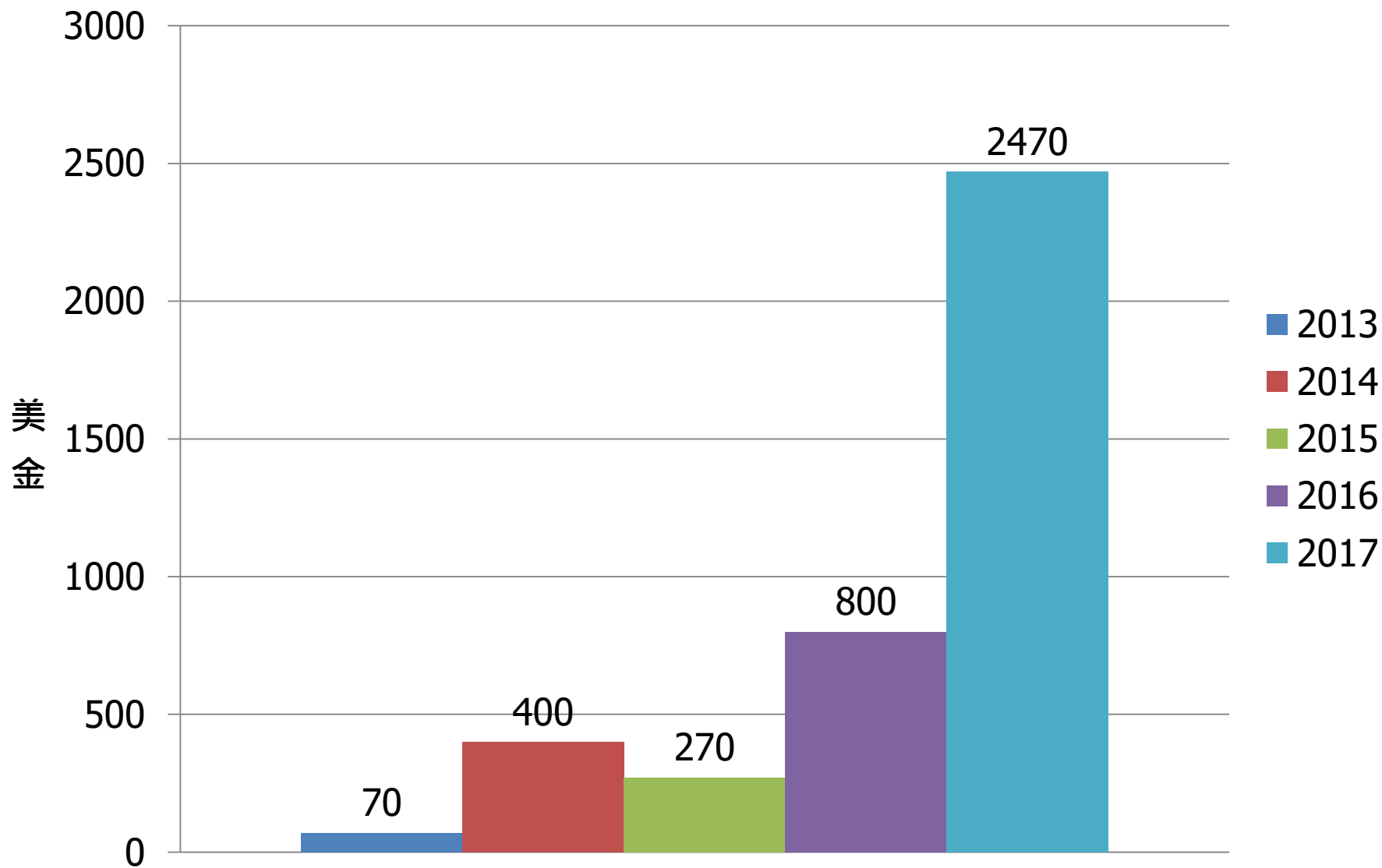


Ubike價值1萬元新台幣

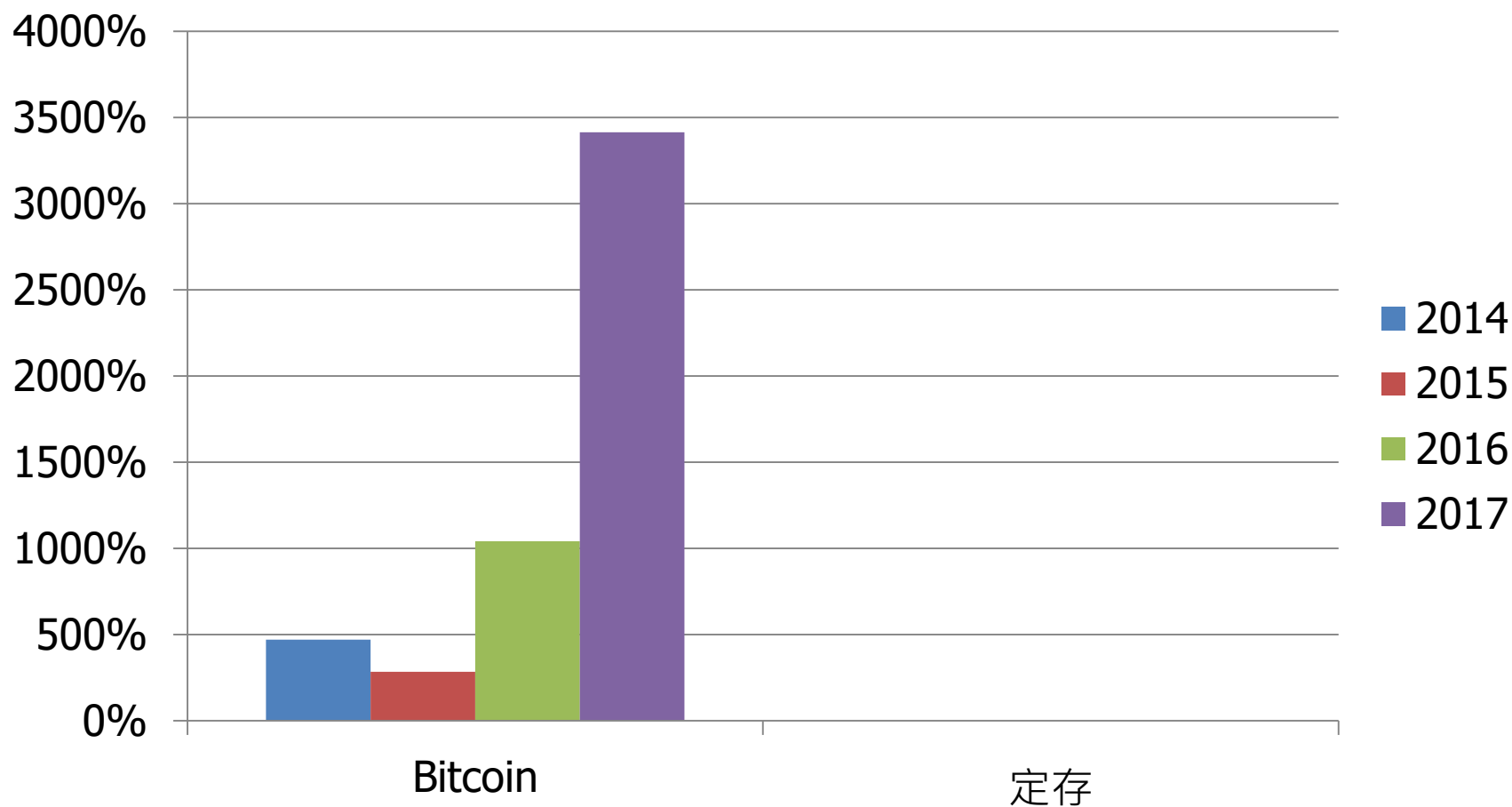
近三年走勢，週線



2013->2017，成長25倍!!



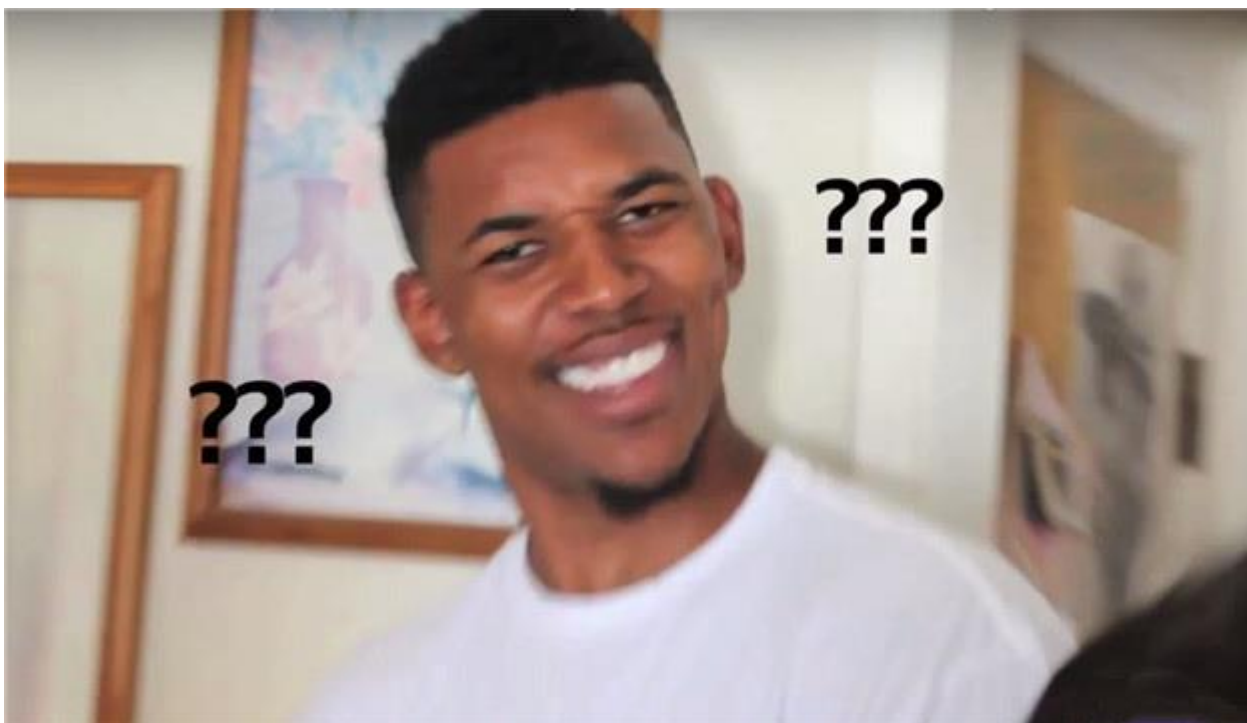
Bitcoin 與定存獲利比較



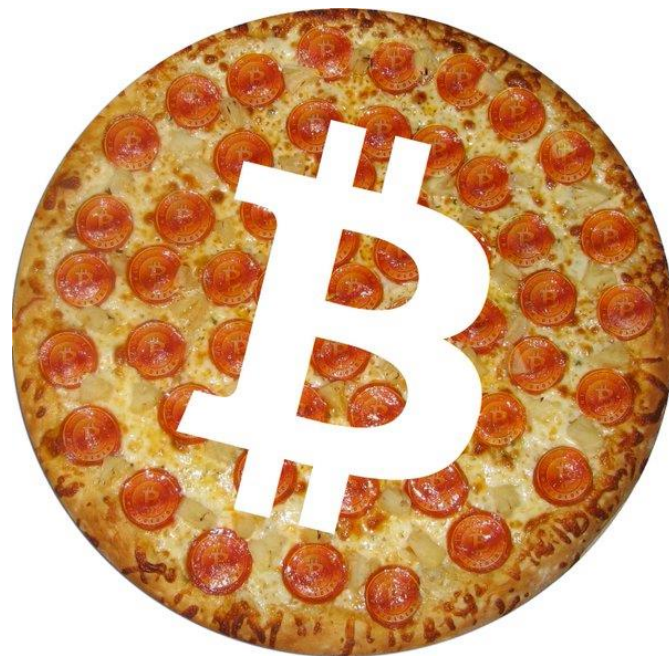
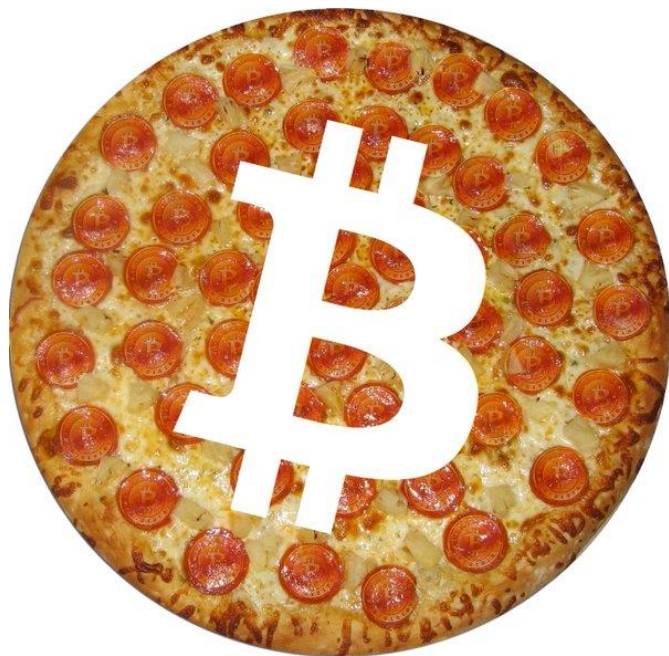
台幣定存利率: <http://rate.bot.com.tw/twd/2014-01-01>

比特幣牌價參考: <https://tradeblock.com/>

What the fuck?






回到2010年






值幾顆比特幣？

10000

2010/5/22 · Bitcoin Pizza Day

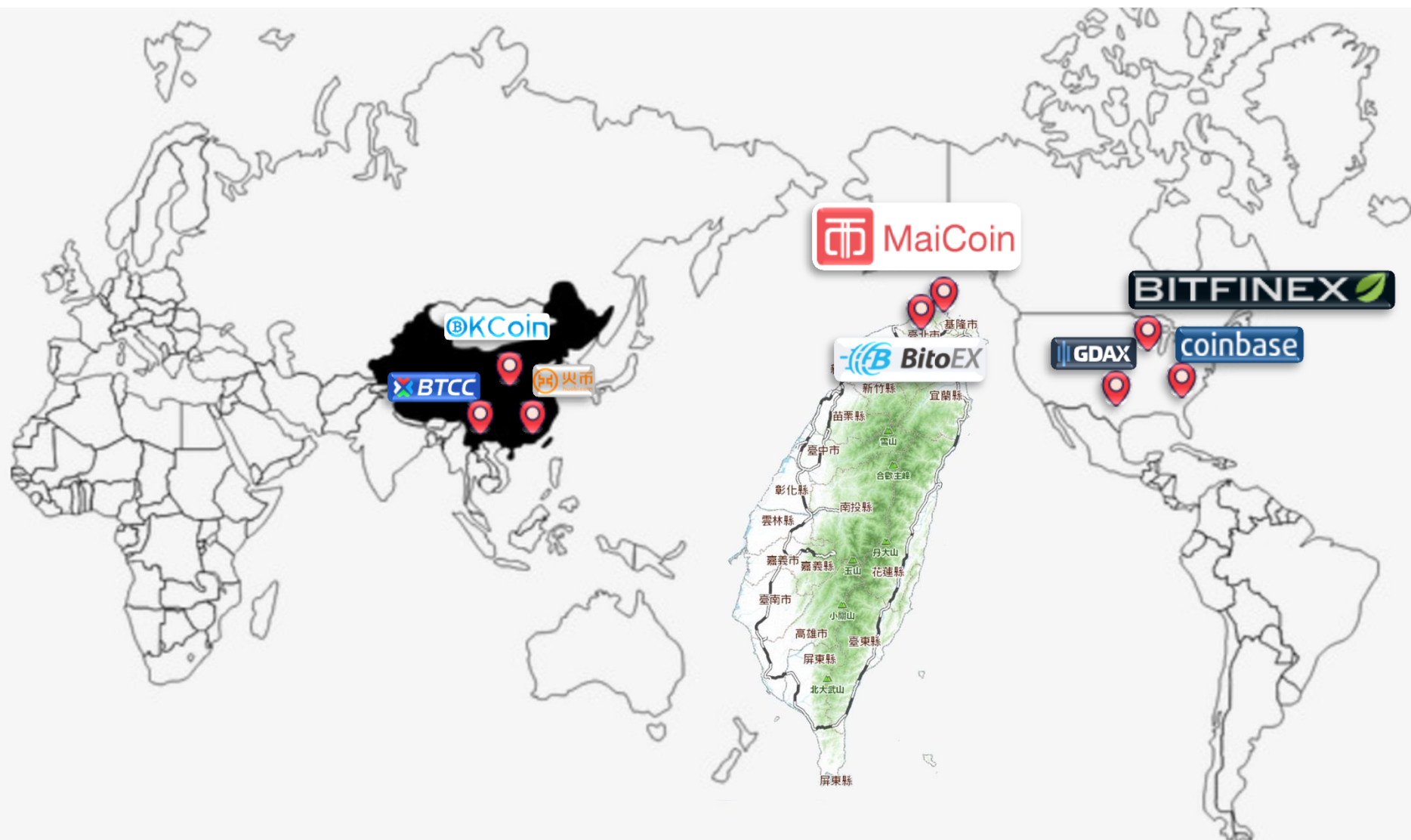
Author	Topic: Pizza for bitcoins? (Read 571320 times)
laszlo Full Member  Activity: 199 	 Pizza for bitcoins? #1 May 18, 2010, 12:35:20 AM I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy! I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire. If you're interested please let me know and we can work out a deal. Thanks, Laszlo BC: 157fRqAKrDyGHR1Bx3yDxeMv8Rh45aUet

laszlo Full Member  Activity: 199 	 Re: Pizza for bitcoins? #11 May 22, 2010, 07:17:26 PM I just want to report that I successfully traded 10,000 bitcoins for pizza. Pictures: http://heliacal.net/~solar/bitcoin/pizza/ Thanks jercos! BC: 157fRqAKrDyGHR1Bx3yDxeMv8Rh45aUet
---	--

現今價值： 10000×3200 (美金)

如何獲得比特幣？

交易所買賣



購買比特幣方法

 帳戶首頁 比特幣地址 聯絡人 安全 設定 new

帳戶概況

比特幣餘額	0.00000000 BTC
價值	NT\$0.00

● 現在價值是依據平均價格

買/賣

接收

 帳戶首頁 比特幣地址 聯絡人 安全 設定 new

快捷下單

歡迎 

目前購買和出售比特幣只對台灣用戶開放。

買比特幣

賣比特幣

● 購買單價: NT\$15,051.99 帳戶可用比特幣: 0.00000000 BTC

買比特幣

用新台幣支付

1.2

BTC



18,062

TWD

買比特幣

請先提交訂單再支付款項。

每日購買上限: NT\$500,000 (還可購買NT\$500,000)

顯示金額為最後需支付之金額, 無需支付其他手續費用給MaiCoin



1. 提交訂單

2. 確認訂單

3. 支付訂單

核對訂單明細並創建訂單

購買時間	2016年05月06日 14:28
購買單價	NT\$15,036.08 (將保證此價格 15 分鐘)
購買數量	1.2 BTC (暫定)
購買金額	NT\$18,043

☒ 我同意在提交購買訂單後立即匯款至 MaiCoin，若在十五分鐘內完成匯款 (以MaiCoin收到款項時間為準)，MaiCoin 會保證下單時的購買單價。若 MaiCoin 在下單十五分鐘後收到款項，MaiCoin 保有以當時的市場價格為基準，重新計算購買單價的權利。

[返回](#)[提交並開始支付](#)



1. 提交訂單

2. 確認訂單

3. 支付訂單

感謝您訂購比特幣，您的訂單已發出

訂單號	b1ced1cecb4cbf343e99a6c9ea85612b9c7a0250909a4981
購買時間	2016-05-06 14:30:10 +0800
購買單價	NT\$15,039.86 (將保證此價格 15 分鐘)
購買數量	1.20000000 BTC (暫定)
購買金額	NT\$18,048

[取消訂單](#)[確認訂單](#)

[1. 提交訂單](#)[2. 確認訂單](#)[3. 支付訂單](#)

支付訂單


請先閱讀以下須知：

1. **請勿分次付款**，例如將 4 萬元拆成兩筆 2 萬元的匯款。如您的轉帳金額超過「非約定轉帳」單日 3 萬元上限，建議您在轉帳選擇使用「繳費繳款」的選項來取代「非約定轉帳」，或是將下方您專屬的玉山銀行轉帳帳號綁定成「約定帳號」來進行付費動作，即可不受新台幣 3 萬元的限制。
2. 若未依照指示付款，系統將無法自動完成您的訂單，請通知我們的客服人員協助您處理。
MaiCoin 不為因付款錯誤而導致的延遲或金額損失負責。

銀行代碼: 玉山商業銀行808

銀行分行: 南港分行

轉帳帳號名: 現代財富科技有限公司

轉帳帳號: 

轉帳金額: NT\$18,048

請支付款項到上方玉山銀行的轉帳帳戶。您可透過以下方式轉帳：

1. **全台灣任一實體 ATM**
2. **您的網路銀行** (需使用讀卡機或是動態密碼)
3. **臨櫃轉帳** (我們不建議您使用臨櫃轉帳來付款。臨櫃轉帳通常需要較長的人工處理時間，因此可能導致我們收到您的款項時已經超過 15 分鐘，進而影響您訂單的購買單價。)

[取消訂單](#)[查看交易明細](#)

自己的錢，自己賺





24/07/2017 18:47:59

KEDAI EMAS SRI ALAM Seksyen 23 授權

馬國鐵鎚大盜去銀樓「挖礦」
敲到手痠連1條金飾都沒帶走

組一台可挖礦的主機

品名	數量	小記
套裝主機/柯博文550	1	6300
顯示卡/GTX-1080	6	92450
記憶體/16G	4	11900
硬碟/HDD+SSD WD Blue	1	8499
電源供應器/1300W	1	6690
TDP耗電: 911瓦，估計價格: NTD 128440		

組一台可挖礦的主機

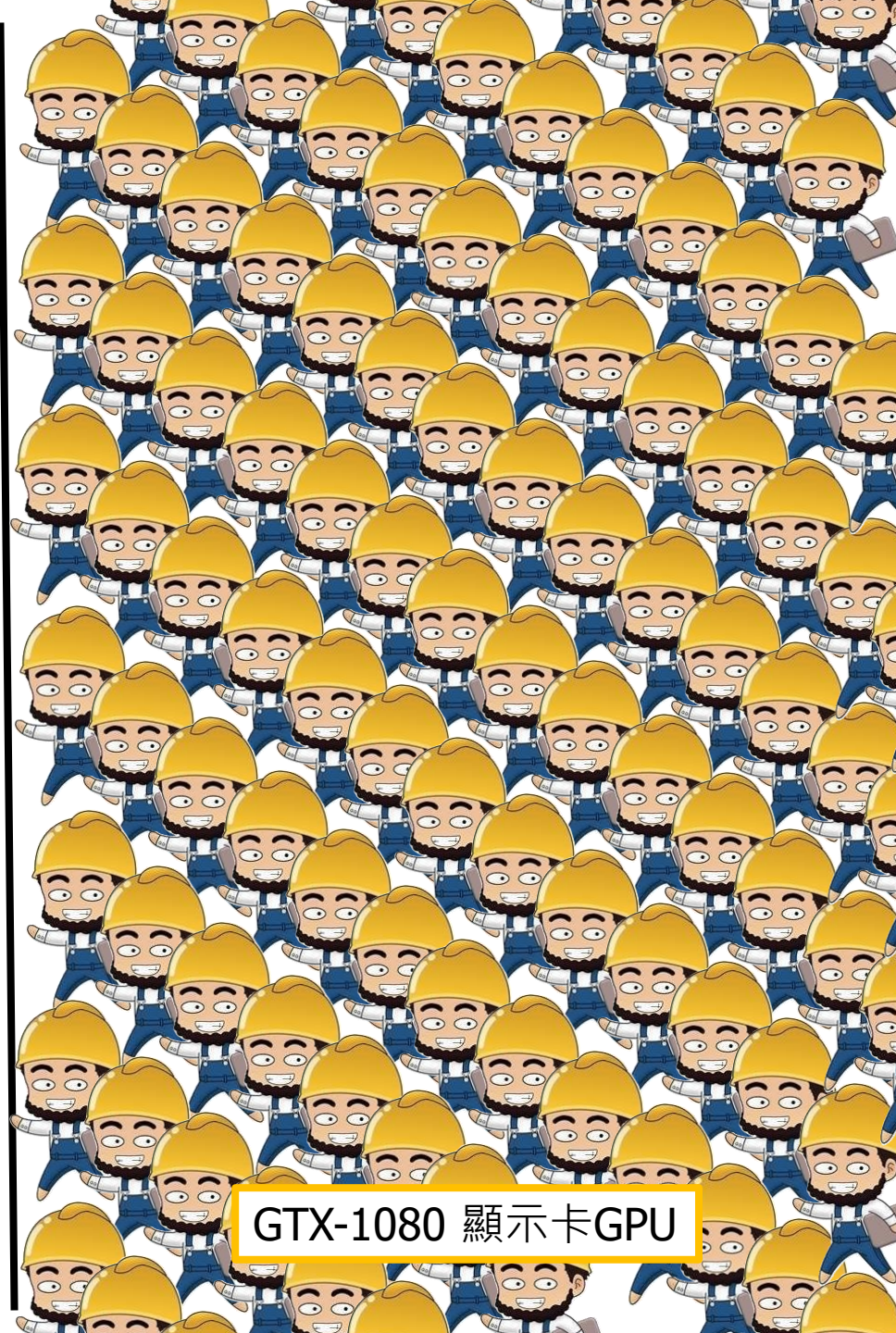
品名	數量	小記
套裝主機/柯博文550	1	6300
顯示卡/GTX-1080	6	92450
記憶體/16G	4	11900
硬碟/HDD+SSD WD Blue	1	8499
電源供應器/1300W	1	6690
TDP耗電: 911瓦，估計價格: NTD 128440		

等一下

有6個顯示卡? 哩丟搞喔?



i7-7700 CPU

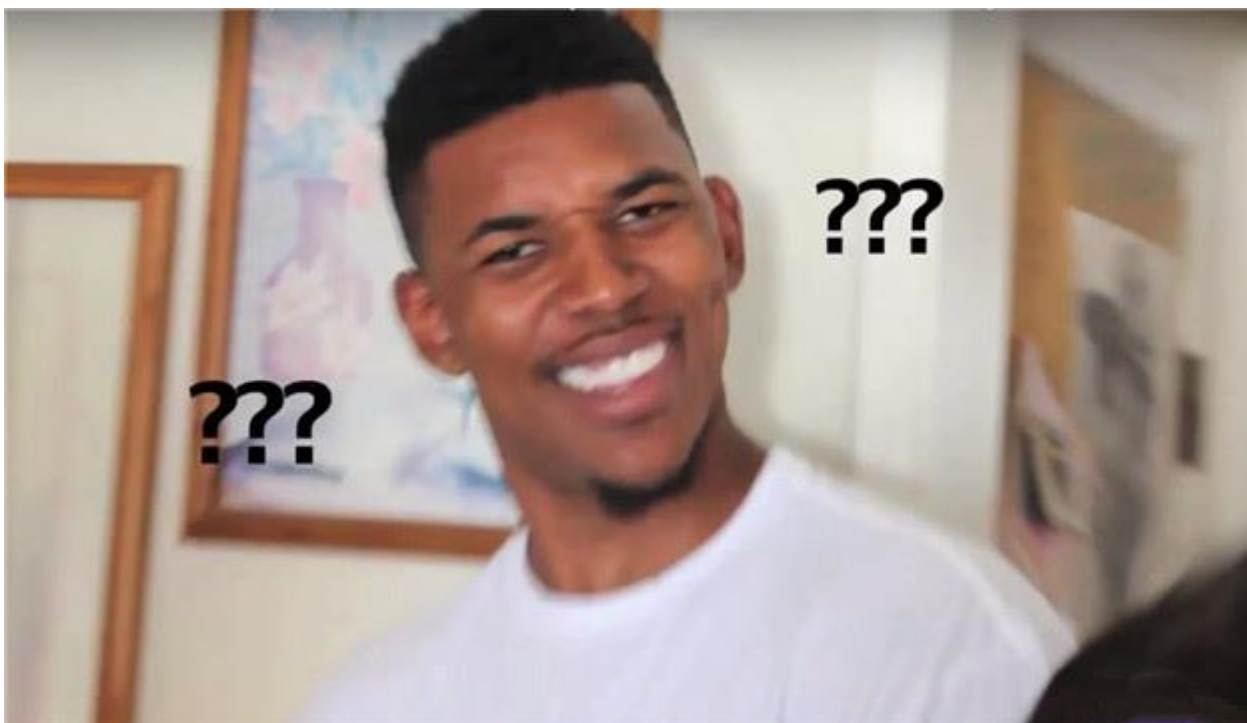


GTX-1080 顯示卡GPU

但還是沒你想的這麼簡單



What the fuck?



現在越來越多的人選擇四川作為比特幣挖礦的首選地。這裡不僅有非常廉價的電力，還有低密度的人口和寒冷的氣候，對解決礦機噪音和散熱問題有先天優勢。

出於節省鋪設線路成本以及用電便利性方面的考慮，比特幣「礦場」大多直接建在水電站內部。



礦場機房

接收比特幣



BTC

ETH

發送比特幣

發送以太幣

帳戶餘額: 0.00000000 BTC (發送全部) (購買)

BTC地址或郵件地址

填寫對方地址

0.00 BTC

0 USD

填寫發送的數量or金額

留言

填寫備註

發送比特幣

您每天可以透過簡訊 (SMS) 方式進行雙層驗證的次數為 20 次，目前您還剩 20 次的驗證次數。當您的驗證次數抵達上限後，需要等待次日 0 時重置。建議您使用 Google 驗證器或是 Authy 來進行雙層驗證，透過此類 APP 將不會有驗證次數的限制。

常見問題

- 如何發送數位資產？
- 關於數位資產向外發送每次之限額
- 為何無法發送數位資產？

- 帳戶首頁
- 我的錢包地址
- 聯絡人
- 安全
- 設定 new

接收

BTC

ETH

接收比特幣

接收以太幣

提供此地址給發送方以接收比特幣：

3BTyZKRtRtBN6fdu6WhzTWsAKkz4Aye7Y

將地址提供給發送方



• 比特幣交易確認有可能需要花費一個小時才能完成。

地址	標籤	創建日期
3BTyZKRtRtBN6fdu6WhzTWsAKk...		03/08/17

詳細資料

如果您想使用新的地址接收比特幣，請點擊以下按鈕：

獲取新地址

常見問題

- 如何接收數位資產？
- 從外部錢包轉移數位資產至 MaiCoin 錢包時，需要多少時間？
- 為何從外部傳送比特幣至 MaiCoin 錢包，但一直沒收到？
- 可以獲取新的地址嗎？舊的地址還能用嗎？

您有什麼問題嗎？

講了那麼多，比特幣是甚麼

Bitcoin是一個共識網路，它讓一種新的支付系統和一種完全的數位貨幣成為可能。它是第一個去中心化的點對點支付網路，它由用戶來支撐，不需要中央機構或中間人。從用戶的角度看，Bitcoin就像是網路上的鈔票一樣。

比特幣的交易運作原理

比特币的交易运作原理

www.TTbit.com 汉化翻译

比特币交易是如何进行的

波比，是在线卖商家，决定开始接受比特币作为收款方式。
爱丽丝，是买家，拥有比特币，并且向要从波比那儿购买商品。

钱包和地址



在电脑中波比和爱丽丝都拥有比特币钱包



钱包是一种特殊文件通过它们可以访问多个比特币地址



一个地址是一串由字母和数字组成的字符串
例如
1HULjMwZEP
k1EPeCh
438eKjLjYb
LCWrfDpH

每个地址都有着自己的比特币数量余额



波比创建了一个新的比特币地址用于接收爱丽丝的款项

新建一个新地址



私钥 公钥

公钥加密算法 101

当波比创建一个新地址，他实际上所完成的动作是生成了一个“密钥对”，由一个公钥和一个私钥组成。如果你使用私钥（只有你自己知道）对一个消息签名，它便可以被对应的公钥（大家都知道）进行验证。波比的新比特币地址代表了一个唯一的公钥，并且对应的私钥保存在他的钱包里面。这个公钥允许所有人可以对那个用私钥进行签名的消息进行验证。

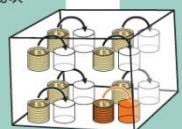
可以简单的认为地址就像是银行账号，但是运行机制又有一些不同。比特币用户可以随意创建任意多个地址。事实上，我们鼓励大家为一个新的交易单独创建新地址。这样一来就没有谁知道哪个地址是属于爱丽丝的。她的匿名性得到了保障。



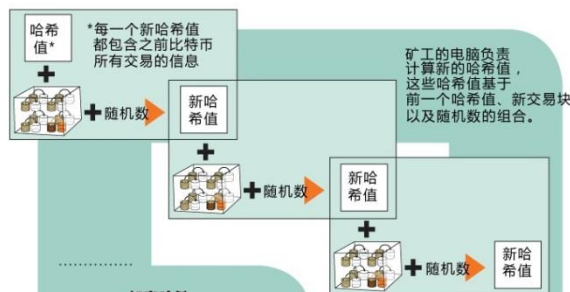
Gary, Garth 以及 Glenn 都是比特币矿工

验证交易

他们的电脑将过去十分钟内的交易数据打包成一个新的“交易块”



矿工的电脑被用于计算加密的哈希函数



加密哈希

加密哈希函数将数据转换成成为一串特定长度的字符串，称为哈希值。源数据的任何一个细微的改变都会导致最终计算出来的哈希值的变化。并且，几乎无法预测一个初始数据集将会产生哪一种特定的哈希值。

The root of all evil
6d0a1899 086a...
(56 more characters)

The root of all evil
486c 6be4 6dde...

The root of all evil
b8db 7ee9 8392...

随机数
从相同的数据创建不同的哈希值，比特币协议使用了“随机数”。一个随机数就是一个添加在数据前面的一个随机数字，改变随机数可以产生大量不同的哈希值。

The root of all evil ???
0000 0000
0000...

创建哈希的计算微不足道，但是比特币系统要求新的哈希值拥有特定的格式——必须以一连串特定数量的0开始。

矿工无从知道哪一个随机数可以产生一个这样的哈希值（以特定数量的0为开头）。所以他们不得不使用不同的随机数生成大量的哈希值，直到他们碰巧找到一个符合规则的哈希值。



每一个区块都包含一个名为“coinbase”的初始交易，这个交易是胜出挖矿所得，金额为50BTC——在这个例子中，是Gary。新挖到的比特币会被支付到Gary的钱包里面一个新生成的地址中。



交易验证

随着时间流逝，爱丽丝发给波比的传送被埋藏到其他最近交易的下面。因为只要有人修改了细节，他就必须重新做一遍Gary所做的事情——因为所有的改变都需要一个完全不同的随机数。然后，其他所有矿工又必须重新计算。这样一来，作弊就几乎不可能实现。



私钥

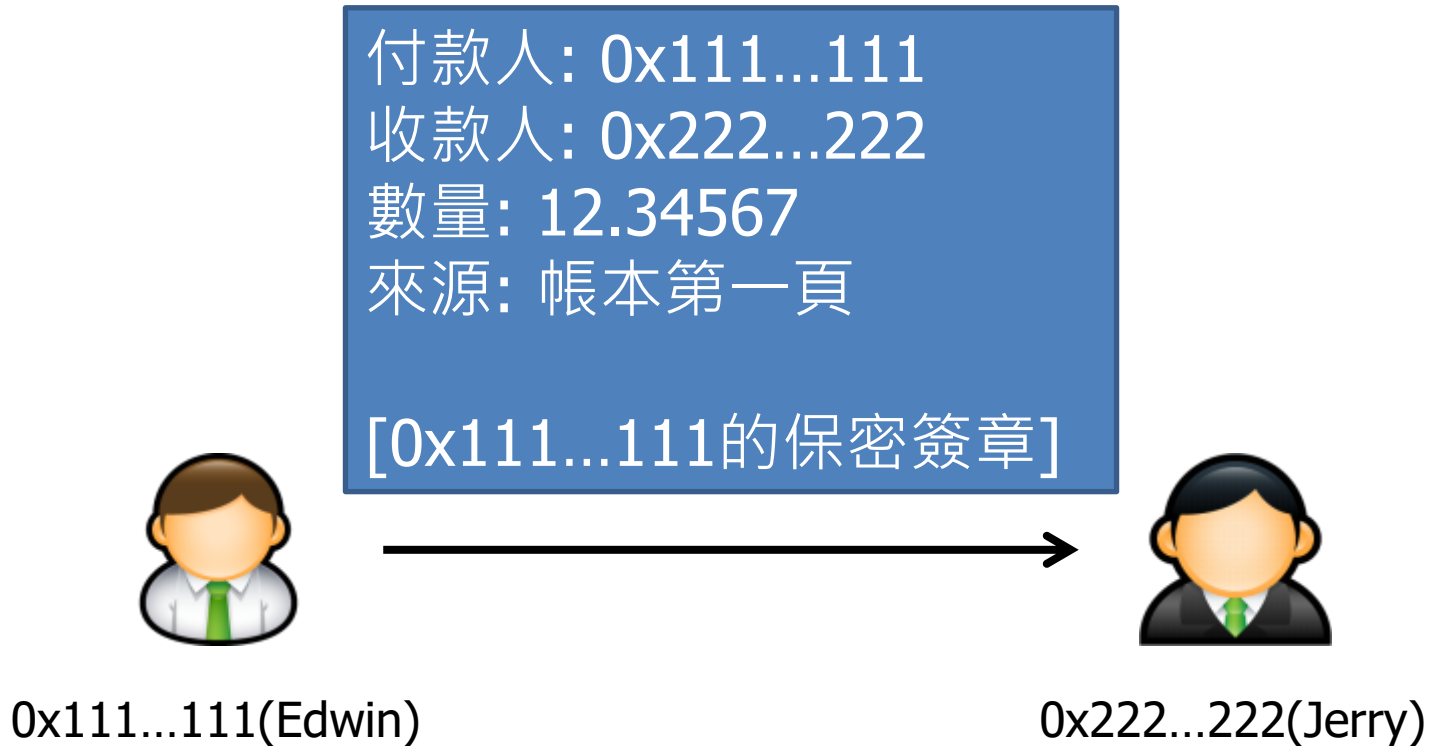
公钥

爱丽丝的钱包里面有着所有地址的私钥。在发送比特币时，比特币客户端使用一个私钥对她的交易申请进行签名。该私钥就是扣款地址所对应的私钥。

此时，网络上的任何人便可以使用对应的公钥对这个交易申请进行验证，看看这个申请是否是来自一个合法的账户所有者。

炸拉！講人話行嗎！

交易





付款人: 0x111...111

收款人: 0x222...222

數量: 12.34567

來源: 帳本第一頁

[0x111...111的保密簽章]



0x111...111(Edwin)



0x222...222(Jerry)

帳本

交易清單：

0x111...111 -> 0x222...222(10)

0x333...333 -> 0x444...444(3)

...

上一帳本編號：0x111

幸運數字：

本次帳本編號（手寫無效，共256碼）：

▶ 帳本編號生成器，每個礦工都有

- 生成的編號與帳本上的內容有關
- 如果更動帳本上的資訊，編號將會面目全非
- 所有交易單皆須放入，且會驗證保密簽章



礦工

- 每個礦工家門都有蒐集交易單的箱子，定時取出塞入帳本
- 一直不斷計算幸運數字，藉以取得報酬
- 帳本編號必須是小於某個數值，此次編號有效



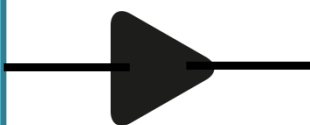
交易清單：
0x111...111 -> 0x222...222(10)
0x333...333 -> 0x444...444(3)
...
上一帳本編號：0x00004835...654
幸運數字：123
本次帳本編號（手寫無效，共256碼）：

⋮

交易清單：
0x111...111 -> 0x222...222(10)
0x333...333 -> 0x444...444(3)
...
上一帳本編號：0x00004835...654
幸運數字：124
本次帳本編號（手寫無效，共256碼）：

⋮

交易清單：
0x111...111 -> 0x222...222(10)
0x333...333 -> 0x444...444(3)
...
上一帳本編號：0x00004835...654
幸運數字：125
本次帳本編號（手寫無效，共256碼）：



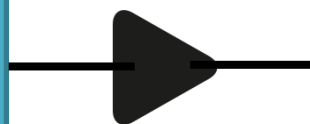
交易清單：
0x111...111 -> 0x222...222(10)
0x333...333 -> 0x444...444(3)
...
上一帳本編號：0x00004835...654
幸運數字：123
本次帳本編號：0x10434686...654

⋮

交易清單：
0x111...111 -> 0x222...222(10)
0x333...333 -> 0x444...444(3)
...
上一帳本編號：0x00004835...654
幸運數字：124
本次帳本編號：0x04568086...457

⋮

交易清單：
0x111...111 -> 0x222...222(10)
0x333...333 -> 0x444...444(3)
...
上一帳本編號：0x00004835...654
幸運數字：125
本次帳本編號：0x00000086...432



失敗

失敗

成功

所有帳本串起來長這樣

交易清單：

0x111...111 -> 0x222...222(10)

0x333...333 -> 0x444...444(3)

...

上一帳本編號：0x111

幸運數字：123

本次帳本編號：0x00000086...432

交易清單：

0x222...444 -> 0x352...415(0.5)

0x333...333 -> 0x463...778(1)

...

上一帳本編號：0x00000086...432

幸運數字：225

本次帳本編號：0x00000097...653

交易清單：

0x222...444 -> 0x352...415(0.5)

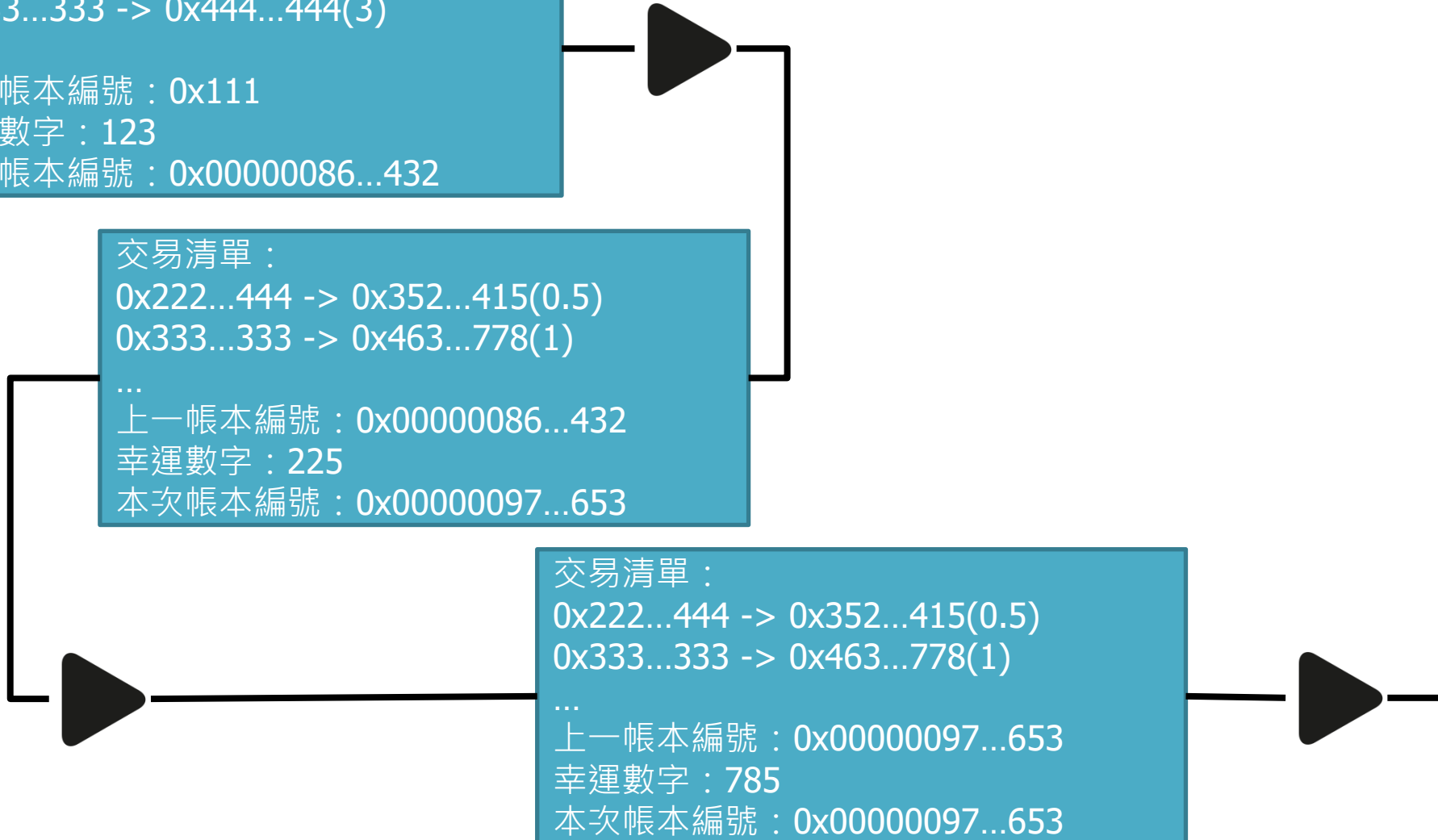
0x333...333 -> 0x463...778(1)

...

上一帳本編號：0x00000097...653

幸運數字：785

本次帳本編號：0x00000097...653



再回来看

www.TTbit.com 汉化翻译

比特币交易是如何进行的

波比，是在线卖家，决定开始接受比特币作为收款方式。
爱丽丝，是买家，拥有比特币，并且向要从波比那儿购买商品。

钱包和地址



在电脑中波比和爱丽丝都拥有比特币钱包



钱包是一种特殊文件通过它们可以访问多个比特币地址



一个地址是一串字母和数字组成的字符串

例如
1HUL3mZEP
kJEPCb
438eKjLjyb
LCWrfDpH



波比创建了一个新的比特币地址用于接收爱丽丝的款项

新建一个新地址



每个地址都有着自己的比特币数量余额

提交一个支付



爱丽丝告诉她的比特币客户端她要发送金额到波比的收款地址。

私钥 公钥

公钥加密法 101
当波比创建一个新地址，他实际上所完成的动作是生成了一个“密钥对”，由一个公钥和一个私钥组成。如果你使用私钥（只有你自己知道）对一个消息签名，它便可以被对应的公钥（大家都知道）进行验证。波比的新比特币地址代表了一个唯一的公钥，并且对应的私钥保存在他的钱包里面。这个公钥允许所有人可以对那个用私钥进行签名的消息进行验证。

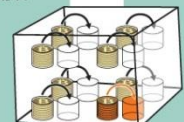
可以简单的认为地址就像是银行账号，但是运行机制又有一些不同。比特币用户可以随意创建任意多个地址。事实上，我们鼓励大家为一个新的交易单独创建新地址。这样一来就没有谁知道哪个地址是属于爱丽丝的。她的匿名性得到了保障。

Gary, Garth 以及 Glenn 都是比特币矿工



验证交易

他们的电脑将过去十分钟内的交易数据打包成一个新的“交易块”



矿工的电脑被用于计算加密的哈希函数

私钥

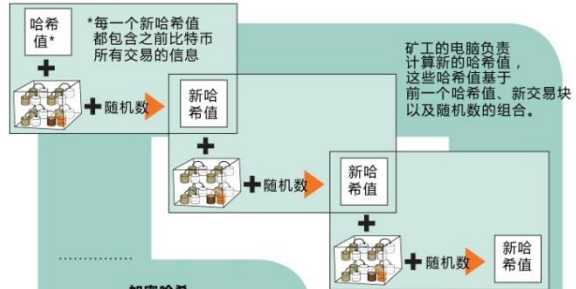


爱丽丝的钱包里面有着所有地址的私钥。在发送比特币时，比特币客户端使用一个私钥对她的交易申请进行签名。该私钥就是扣款地址所对应的私钥。



公钥

此时，网络上的任何人便可以使用对应的公钥对这个交易申请进行验证，看看这个申请是否是来自一个合法的账户所有者。



加密哈希

加密哈希函数将数据转换成成为一串特定长度的字符串，称为哈希值。源数据的任何一个细微的改变都会导致最终计算出来的哈希值的变化。并且，几乎无法预测一个初始数据集将会产生哪一种特定的哈希值。

The root of all evil
6d0a1899 086a...
(56 more characters)

The root of all evil
486c 6be4 6dde...

The root of all evil
b8db 7ee9 8392...

随机数
从相同的数据创建不同的哈希值，比特币协议使用了“随机数”。一个随机数就是一个添加在数据前面的一个随机数字，改变随机数可以产生大量不同的哈希值。

The root of all evil ???
0000 0000
0000...

创建哈希的计算微不足道，但是比特币系统要求新的哈希值拥有特定的格式——必须以一连串特定数量的0开始。

矿工无从知道哪一个随机数可以产生一个这样的哈希值（以特定数量的0为开头）。所以他们不得不使用不同的随机数生成大量的哈希值，直到他们碰巧找到一个符合规则的哈希值。

每一个区块都包含一个名为“coinbase”的初始交易，这个交易是胜出挖矿所得，金额为50BTC——在这个例子中，是Gary。新挖到的比特币会被支付到Gary的钱包里面一个新生成的地址中。



交易验证

随着时间流逝，爱丽丝发给波比的传送被埋藏到其他最近交易的下面。因为只要有人修改了细节，他就必须重新做一遍Gary所做的一切——因为所有的改变都需要一个完全不同的随机数。然后，其他所有矿工又必须重新计算。这样一来，作弊就几乎不可能实现。



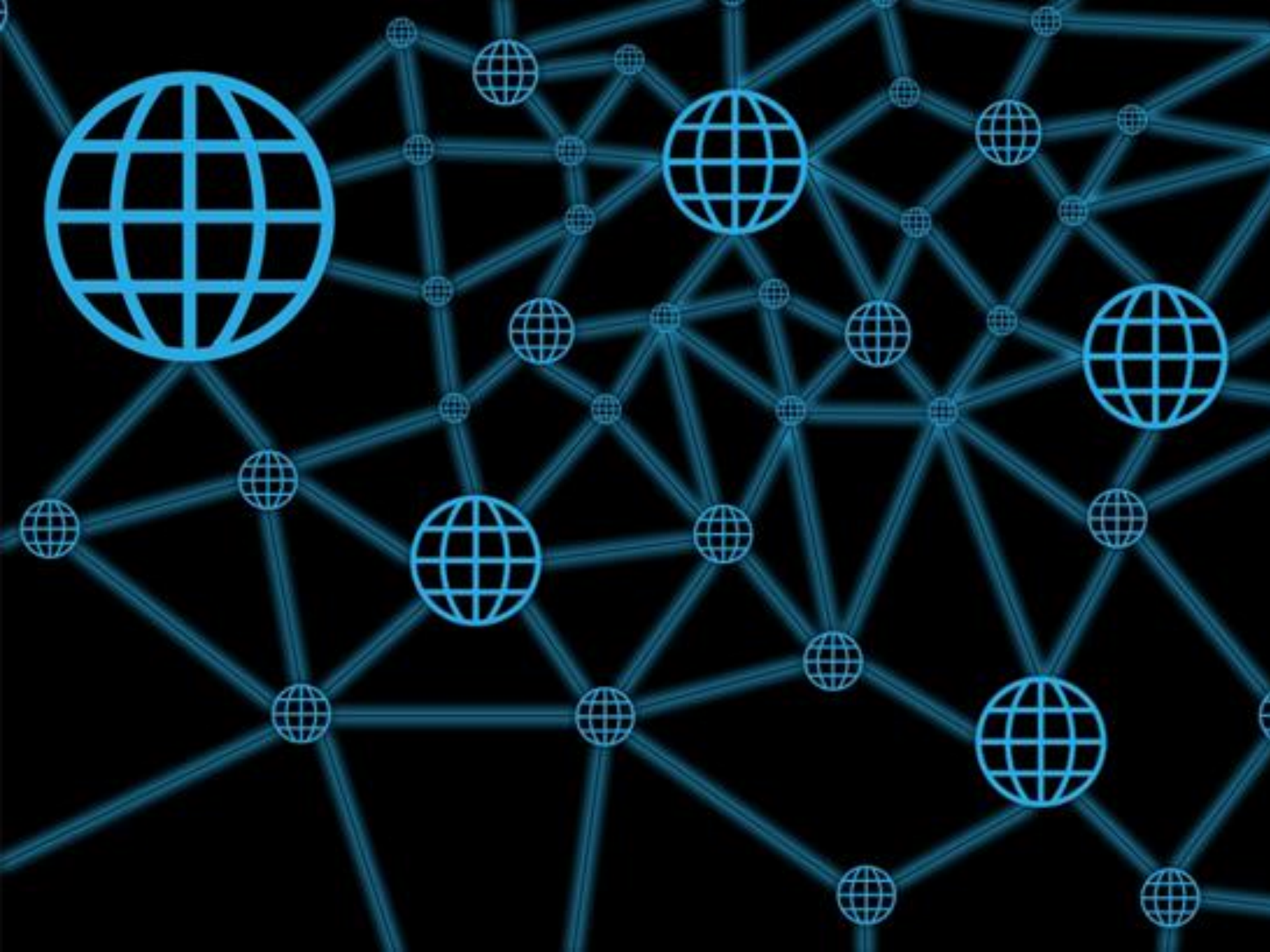
波比和爱丽丝

weibo.com/rockxie

交易量、市值

- 市值: 52,292,509,137
- 24小時交易量747,321,445 (顆)
- 全球限量2100萬顆











地址: 0x111...111



地址: 0x222...222

合法性

- 日本: 2017年4月，新版支付服務法承認虛擬貨幣的合法支付地位。
- 中國: 2017年2月對比特幣進行監管機制。
- 德國: 2013年8月，政府認可比特幣的法律和稅收地位。
- 俄羅斯: 2014年2月，政府宣布禁止比特幣。
- 印度: 2017年4月，政府委員決定監管比特幣市場。
- 澳洲: 2017年7月1日起，視比特幣為貨幣之一，並且免除商品與服務稅（GST）

與傳統貨幣的比較

	存續時間	總量控制	有無擔保	交易媒介	價值標準	價值儲藏
法定貨幣	與國家存續期間相同	O	發行保證： 如貴金屬、 外匯等	O	O	O
單向流通 虛擬貨幣 (天幣、P 幣)	網站或特 定服務存 續時間	X	X	X	X	X
比特幣	網路虛擬 世界永久 保存	O	X	已有許多 接受比特 幣支付案 例	X	?

交易之外的用途



Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Mondays to Fridays

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt







日本比特幣交易所Bitpoint 7/5宣佈，與支付服務的供應商Nippon Pay合作，為中國三大流行支付服務提供加密貨幣支付選項。有了這次合作之後，微信、支付寶和銀聯都能在這個新平臺上開放比特幣和以太幣（ETH）支付選項。



實現財務自由有時候也很簡單，比如說用 3000 美元買下 20000 比特幣。現在這位「史密斯」先生早已辭掉了矽谷的工作，開始長達 4 年的環遊世界。這是他的故事。



商周財富網：3個月漲300%又暴跌！買比特幣要當成「買●●」，挪0.5%資金投資就好



- 千萬別自己搞礦機
- 有閒錢還是要買一點比特幣
- 區塊鏈是能夠顛覆未來生態的



A M I S