修平科技大學

資訊網路技術系

專題製作報告

比特幣的相關研究

指導老師：沈良澤老師

組長:林啓軒 YN99002

組員:段泓瑋 YN99041

中華民國 103 年 01 月 07 日

1. 摘要

現今比特幣越來越火紅比特幣的價值也一直漲然而依該還是又很多人不知道，比特幣是什麼樣的東西比特幣是如何產生而中本聰又是誰，那比特幣如何取得比特幣是要如何交易比特幣現在有哪些國家可以使用，知道了這些我們還要看看比特幣是如何運作的如何在網路間運行，而比特幣會有哪些風險會有什麼樣的狀況發生，這些疑問我們都會一一的說出來。

2. 前　言

比特幣這個虛擬貨幣在近幾年越來越流行，到底甚麼是比特幣？比特幣又有哪些優缺點？而比特幣又會對現有的經濟體系造成怎麼樣的衝擊？還有比特幣對於消費者權益有沒有保障？以及比特幣這款虛擬貨幣是否會被竄改或駭客入侵導致所有的資料都毀損或消失，而這款虛擬貨幣有哪些國家接受又有哪些國家不接受？基於以上問題以及上述沒說到的問題故我們將對比特幣進行研究說明。

3. 目　錄

4. 比特幣的起源

比特幣是由名為中本聰的人製作中本聰是誰目前也沒有人知曉但是在本次探討比特幣的時候我們也會把中本聰的線索告訴個位來推論大概是怎麼樣的人，而比特幣是在 2008 年提出比特幣是由開源軟體以及塊密碼的工作模式在 P2P 對等網路和分布式的資料庫平台上開發出來，比特幣的系統遍部整個對等網路的使用者端的各節點，然後以種子檔案來確保貨幣發行時在管理以及使用中的公平安全以及可靠性，然後在 2009 年 50 個比特幣問世，而上述又說到開源軟體我大致說明開源軟體是什麼開源軟體也可以稱為，開放原始碼軟體而著個軟體是需要滿足一定條件，我在這裡會說明一部份的條件那條件是什麼，第一自由再散布:也就是受到許可而獲得原始碼的人可自由再將此原始碼在散佈出去，第二原始碼:這一個是說一個程式的執行檔，在散布的時候必須把原始的程式碼也付再檔案旁，或是放在一個可以讓後面的人好取得的地方，第三衍生著作:這一點是說散布出去的程式碼別人取得後，修改成他的版本他可以依授權條款再把他自己的程式碼散布出去，等等還有很多的條件滿足後那一個軟體才可以稱得上是開源軟體，然後塊密碼的工作模式是什麼我說明一下，它的意思是允許使用者使用同一組密碼或密鑰對多於一塊數據進行加密，上述也有說到 P2P 而 P2P 就是所謂的點對點技術如果這樣說覺得

有點不太懂，我舉個例子大家應該都知道 Foxy 這個程式吧那就是一種 P2P 的軟體而 P2P 的技術是這樣的,它是一款無中心伺服器依靠的是使用者交換資訊跟有中心伺服器有很大的不同，因為無中心伺服器的節點與伺服器都是使用者。

而分布式資料庫是一種將網路上分散的多個資料庫連線起來變成一個邏輯上統一的資料庫。

5. 爭議性

現在的比特幣有好的聲浪也有壞的聲浪，覺得好的人是說比特幣會開創新的商業模式以及可以為消費者帶來更便利的生活但是覺得壞的人是說會擾亂金融產業，也有說會有人以比特幣因為不受政府控制來逃漏稅，或是以比特幣因為匿名交易方式來做非法活動，例如恐怖攻擊需要資金這時使用比特幣就很難查到，比特幣我覺得很有可能會一下就沒落就以資料分析比特幣的漲幅太誇張一瞬間就衝上很高的點，這時會急脫手的機率很高加上中國那邊的問題這之後會說到，所以他會瞬間泡沫化不是不可能的事情。

6. 管理

對於管理比特幣的管理方式大家應該都想知道，因為一個管理的方式會影響到的地方會非常的廣泛舉個例子有一個網站管理方式非常差，當你知道了著個消息你還會願意花錢去消費他的物品，絕對沒辦法，因為你會有恐懼怕哪天買了東西以後東西沒寄，你匯的錢被網站吃掉所以在想要掏出錢消費物品時我們第一個想到的東西一定都是，他的管理方式或他們的品質如何我一定要去看看大家對這個網站的評語，OK 說了那麼多直接來看比的幣的管理方式，他的管理方式就像前面說過的是利用對等網路加分佈式資料庫來架構，所以創作比特幣也是利用上述兩點來發揮共識主動性，什麼是共識主動性我說一個例子大家應該都知道維基百科，這個網站就是由共識主動性來構成你知道什麼資料就可以去發表你知道的資訊如果有錯的地方會有其他網友去更改來讓資料更完整，但是依網站的不同我覺得網站的管理要有所不同在後面會說明我會覺得這種管理有什麼不妥。

7. 比特幣的市場情況

在現在比特幣的盛行但是有誰知道比特幣在各國的發展情形那，我就說明目前比特幣在哪些國家是接受有哪些國家不接受而接受的理由是什麼不接受的又是什麼。中國:

中國目前是不接受比特幣甚至是打壓比特幣有人說，比特剛出來時就是由中國那裡傳出消息的，那現在怎麼會禁止發行，我以自己的觀點來看那就是，中國會怕那怕什麼。

第一是打壞自己國家金融匯率。

第二怕人民會開始做亂自古的中國歷朝代會滅亡都會有一些自稱宗教的團體出現才開始走向滅亡，所以依這個觀點來看中國政府會怕比特幣如果盛行，人民會壓過政府所以中國一這點當然也不會同意比特幣。

第三中國政府害怕比特幣瞬間泡沫化的風險這點應該不用多說應該是所有的國家都會害怕的加上中國的人口那麼多，如果比特幣在自家裡盛行然後瞬間泡沫化那個後果會不堪設想。

第四怕有人會鑽比特幣的程式漏洞來洗錢。

第五因為中國有項法規規定中國的人民，在一年內能帶出境外的錢不能超過五萬，而這項規定跑出了一個問題就是中國的有錢人，會跑去其他國家旅遊說旅遊實際是賭博他們要是賭博的籌碼因為籌碼可以兌換其他國家的錢幣,然後再匯到海外帳戶，所以中國才有此項政策，所以今天突然跑出了比特幣又加上比特幣不受國家政府影響那中國的那項政策有跟沒有是一樣的。

1. 印度:

目前印度跟中國一樣都是嚴格禁止比特幣的發行，印度也警告民眾比特幣所帶來的風險，如果泡沫化後所帶來的後果，所以印度央行方面也以最快速度關閉比特幣交易所，印度央行的解釋是比特幣波動劇烈加上政府缺乏相應的擔保資金。

新加坡:

對於新加坡處理比特幣的方式，從原來的不認同轉變成認同，

原本的新加坡處理方式是政府不承認自己國家的人民也不會

去管他們有沒有在使用比特幣，但是在 2014 年 1 月的時候新

加坡政府轉變成了認可比特幣，並公布了比特幣的稅收條款，

稅收條款是說用比特幣購買虛擬物品例如公司的投資，則無需

上繳稅金，若是實體則需要上繳。

泰國:

目前泰國政府說明是缺乏合適的法規，所以現在泰國還不認同

比特幣。

韓國:

韓國跟泰國一樣目前也還是不承認比特幣

台灣:

目前台灣政府不承認比特幣，台灣的中央銀行下禁止令，禁止

比特幣，台灣政府認為比特幣不是貨幣不具法償效力對消費者也沒有保障，加上比特幣可能淪為洗錢與非法交易的工具等風險而且比特幣還有泡沫化的風險所以台灣政府不認同比特幣。

美國:

美國現在把比特幣視為合法的貨幣，雖然比特幣的風險很高但是美國有些人認為比特比如果成功的話會為消費者帶來更大的便利，擁有很長遠的前途。

德國:

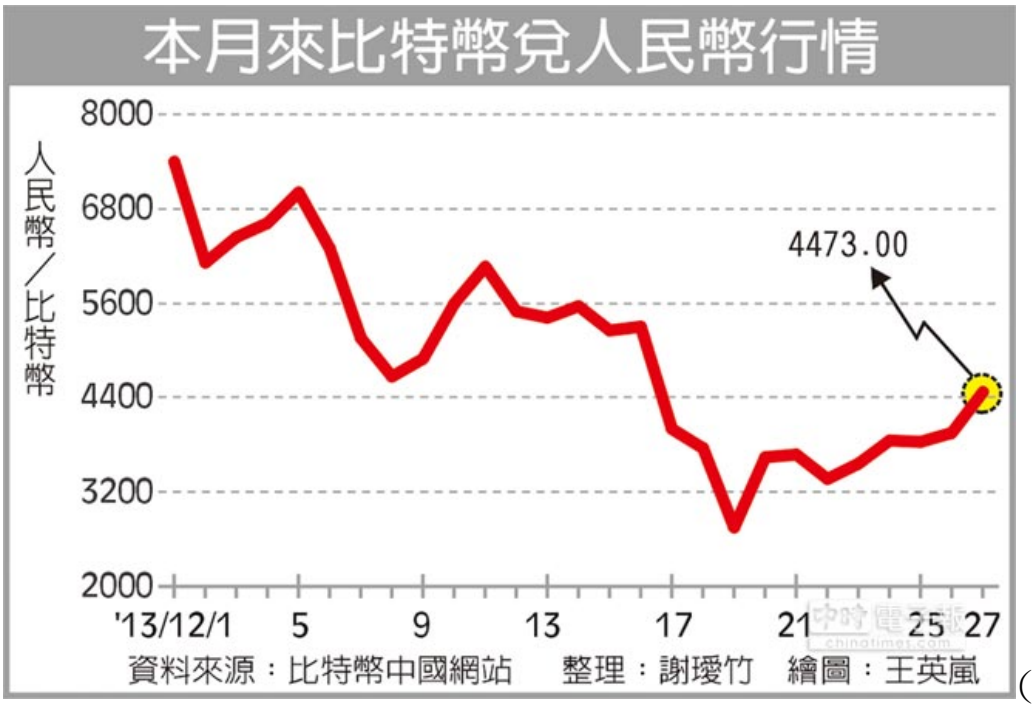
在 2013 年 9 月得時候德國認可了比特幣，德國認為比特幣不是虛擬貨幣而是金融工具，所以得過以法規規限了比特幣讓比特幣在德國是有價值的貨幣，德國是目前歐盟內經濟實力最強的，有了德國的肯定目前比特幣在德國應該是有很好的地位。

我認為現在的比特幣有美國與德國的支持比特幣會被認可應該不遠了但是還有幾點要注意的是比特幣的風險，如果不把這點處理掉其他國家就很難真正的認可比特幣我認為比特幣如果能讓有一國來接收以及釋出那比特幣的風險就會降低很多。

8. 比特幣各國匯率

雖然有些政府不認可比特幣但是各國還是有各國的匯率，我在下面會說明各國的匯率以及有些國家在什麼時候有對比特幣發出宣言導致比特幣的漲或降。

下圖(圖一)為比特幣的交易行情比特幣開出來時中國為之瘋狂，兌換情形一開始八千人民幣可換一比特幣，但是中國央行開始禁止後比特幣跌至兩千七左右，然後又隔一段時間比特幣才又爬回四千左右



(圖一)

印度:

(圖二)

圖二是印度 2014 年 1 月的匯率。

雖然印度政府不認同比特幣但是在印尼要換比特幣的匯率還是算很高。

日期	最新	开盘	高	低	百分比变化
2014年1月14日	1145.23	1172.30	1199.19	1132.58	-2.31%
2014年1月13日	1172.30	1193.77	1209.29	1115.92	-1.80%
2014年1月12日	1193.77	1276.95	1299.16	1178.53	-6.48%
2014年1月11日	1276.48	1206.61	1282.66	1168.08	5.79%
2014年1月10日	1206.61	1158.40	1220.38	1131.09	4.16%
2014年1月9日	1158.40	1192.59	1228.33	1103.08	-2.24%
2014年1月8日	1184.97	1116.21	1209.37	1087.80	5.44%
2014年1月7日	1123.82	1281.09	1324.48	1104.85	-12.28%
2014年1月6日	1281.09	1283.75	1331.37	1209.45	-0.21%
2014年1月5日	1283.75	1163.97	1287.54	1126.37	9.74%
2014年1月4日	1169.83	1117.26	1176.27	1058.39	4.20%
2014年1月3日	1122.66	1082.14	1122.66	1047.31	3.62%
2014年1月2日	1083.40	1021.40	1117.50	1000.42	6.07%
2014年1月1日	1021.40	1021.72	1048.05	954.73	-0.03%
2013年12月31日	1021.71	1020.17	1031.13	968.77	0.15%
2013年12月30日	1020.17	1001.30	1039.73	968.25	1.88%
2013年12月29日	1001.30	943.00	1019.05	930.97	6.18%
2013年12月28日	943.00	1028.19	1028.19	943.00	-8.29%
2013年12月27日	1028.19	1022.96	1052.81	975.59	0.51%
2013年12月26日	1022.96	896.58	1049.58	884.93	14.10%
2013年12月25日	896.58	889.86	904.07	858.39	0.76%
2013年12月24日	889.86	883.03	915.81	862.70	0.77%
2013年12月23日	883.03	810.67	883.03	788.71	10.22%
2013年12月22日	801.17	806.96	887.37	775.33	-1.33%
2013年12月21日	811.94	834.95	892.04	782.27	-1.39%
2013年12月20日	823.40	875.00	980.36	786.98	-5.90%
2013年12月19日	875.00	708.85	886.93	707.33	23.44%
2013年12月18日	708.85	897.33	910.44	600.00	-20.60%
2013年12月17日	892.72	1007.30	1007.30	856.07	-11.37%
2013年12月16日	1007.30	1156.18	1167.03	1000.00	-12.88%
2013年12月15日	1156.18	1133.76	1166.22	1079.55	0.00%
最高: 1331.37	最低: 600.00	差价: 731.37	平均: 1038.94		百分比变化: -0.95

新加坡(圖三)

圖三為新加坡 2013 年 12 月 15 日至 2014 年 1 月 14 日的匯率

新加坡在 2013 年九月時雖然還沒有認可比特幣，但是在 2014 年 1 月的時候政府認可了比特幣就像之前提到過的，所以從上三圖的匯率圖我們看到了認可後匯率有漲有降但是基本上，趨勢都還是在往上漲。

德國:

(圖四)

圖四是比特幣 2014 年 1 月的匯率

台灣:

(圖四)

(圖四為比特幣兌換台幣的匯率)

在台灣比特幣也是沒有認同有認同的只有公司自己來做發行的但是從匯率來看比特幣現在要換也是很貴雖然比特幣有高風險但是還是有很多人來投資比特幣。

美國:

日期	最新	开盘	高	低	百分比变化
2014年1月13日	900.10	940.00	948.53	900.00	-4.24%
2014年1月12日	940.00	1005.50	1022.99	924.00	-6.48%
2014年1月11日	1005.13	957.90	1011.00	938.77	5.90%
2014年1月10日	949.17	937.00	962.00	906.00	1.30%
2014年1月9日	937.00	933.01	964.70	866.66	0.43%
2014年1月8日	933.00	880.00	965.89	860.00	4.83%
2014年1月7日	890.00	1012.90	1044.20	880.00	-12.13%
2014年1月6日	1012.89	1010.11	1092.90	875.00	-0.21%
2014年1月5日	1015.00	924.92	1029.88	911.59	9.74%
2014年1月4日	924.92	884.89	932.00	848.48	4.52%
2014年1月3日	884.89	858.00	888.80	843.00	3.01%
2014年1月2日	859.00	816.00	885.00	810.56	5.27%
2014年1月1日	816.00	805.58	830.00	775.00	0.25%
2013年12月31日	814.00	804.88	814.00	777.00	2.24%
2013年12月30日	796.18	790.00	818.00	782.72	0.78%
2013年12月29日	790.00	762.00	801.00	735.00	3.67%
2013年12月28日	762.00	803.23	805.00	721.20	-5.34%
2013年12月27日	805.00	807.00	830.55	768.00	-0.25%
2013年12月26日	807.00	707.30	829.59	707.30	14.11%
2013年12月25日	707.21	702.80	710.00	674.00	0.63%
2013年12月24日	702.80	713.35	729.84	666.01	-2.12%
2013年12月23日	718.00	639.48	724.00	631.11	12.28%
2013年12月22日	639.50	640.50	700.00	615.00	-0.16%
2013年12月21日	640.50	650.00	734.77	610.40	-1.46%
2013年12月20日	650.00	729.00	773.90	622.50	-10.84%
2013年12月19日	729.00	541.00	744.89	528.75	34.75%
2013年12月18日	541.00	715.00	717.01	455.00	-24.34%
2013年12月17日	715.00	758.00	780.00	678.89	-5.67%
2013年12月16日	758.00	920.00	925.00	715.00	-17.61%
2013年12月15日	920.00	908.99	927.99	840.03	1.21%
2013年12月14日	908.99	945.50	948.00	876.00	0.00%
最高: 1092.90	最低: 455.00	差价: 637.90	平均: 821.65		百分比变化: -0.98

（圖四）

上圖為美國 2013 年 12 月 14 日到 2014 年 1 月 13 日的匯率在美國 11 月 18 日承認比特幣後過一個月他的幣值已經漲到了如上圖那樣到了 900 多所以有人說你如果再 2013 年初挖 100 個比特幣那你的身價已飆漲 96 倍

泰國:

日期	最新	开盘	高	低	百分比变化
2014年1月13日	30091.5	31083.6	31506.2	29117.7	-3.19%
2014年1月12日	31083.6	33398.3	33827.9	30704.6	-6.48%
2014年1月11日	33237.3	31339.6	33398.3	30414.8	6.06%
2014年1月10日	31339.6	30952.6	31730.2	29377.9	1.25%
2014年1月9日	30952.6	31068.7	31954.3	28696.0	0.27%
2014年1月8日	30870.2	29105.0	31928.8	28164.1	6.07%
2014年1月7日	29105.0	33447.6	34528.1	29016.6	-12.98%
2014年1月6日	33447.6	33452.2	34999.0	32316.8	0.28%
2014年1月5日	33355.4	29999.0	33616.2	29416.8	11.19%
2014年1月4日	29999.0	29025.7	30776.4	27633.4	2.96%
2014年1月3日	29136.8	27999.0	29390.4	27196.4	4.06%
2014年1月2日	27999.0	26498.8	27999.0	25954.4	5.66%
2014年1月1日	26498.8	26435.7	27190.0	24769.0	0.24%
2013年12月31日	26435.5	26460.7	26679.2	25065.8	-0.10%
2013年12月30日	26460.7	25971.4	26968.0	25113.9	2.53%
2013年12月29日	25807.3	25051.2	26366.0	24151.4	2.13%
2013年12月28日	25270.3	26337.2	26699.4	23670.6	-4.05%
2013年12月27日	26337.2	26402.7	27159.9	24886.2	-0.25%
2013年12月26日	26402.7	23140.8	27141.7	22909.1	14.10%
2013年12月25日	23140.8	22968.5	23334.1	21533.3	0.75%
2013年12月24日	22968.5	23254.9	23839.3	21673.1	-0.77%
2013年12月23日	23147.8	20847.4	23631.2	20514.0	11.03%
2013年12月22日	20847.6	20752.0	22819.8	19938.6	-0.16%
2013年12月21日	20880.2	21102.3	22750.9	19847.6	-1.05%
2013年12月20日	21102.3	23523.2	25121.9	20219.2	-10.29%
2013年12月19日	23523.2	17378.2	24178.6	16707.2	35.36%
2013年12月18日	17378.2	22761.9	23257.4	14290.5	-23.71%
2013年12月17日	22778.9	24361.9	25029.3	21745.1	-5.71%
2013年12月16日	24157.1	29490.7	29702.1	22439.4	-18.09%
2013年12月15日	29490.7	28918.6	29746.6	26705.0	1.98%
2013年12月14日	28918.6	30271.5	30388.2	28080.2	0.00%
最高: 34999.0	最低: 14290.5	差价: 20708.5	平均: 26844.0		百分比变化: 4.06

（圖五）

圖五為泰國的匯率圖

由上述的幾個國家的匯率圖可以發現一件事例如，第一個美國在 11 月之前比特幣兌換的匯率大約是在 180 到 200 之間但是到了 11 月之後匯率突飛猛進到了 12 月就已經除破了 900 大關，在這之間只發生了美國政府認可了比特幣，第二新加坡在 1 月之前匯率大約在 800 左右但是 1 月之後就突破 1000 而中間也只發生了政府認可比特幣雖然也只上漲了 200 點但是以匯率來看這 200 點要在一瞬間上漲這麼多是非常困難的更不要說美國的那根本是少之又少，從上訴兩點來看比特幣因為政府的支持都上漲也會因政府的封鎖而下降，而上圖還沒有走勢圖是因為該國家還沒有可以兌換或者沒有走勢圖。

9.比特幣的安全性

就之前說明過的，比特幣的架構是如何，是如何產生比特幣的但是就這些來看比特幣的安全性真的足夠嗎在現在比特幣的匯率飆漲真的有笨的駭客或是其他人不會想到要走捷近取得比特幣賺一手嗎?真的就有可能不會被駭客入侵?或是不可能會中駭客蓄意寫的病毒軟體?

在 2013 年 12 月多時就有一篇新聞說台灣是繼美國、日本、澳洲等國第六大受害的國家，什麼災害呢?那就是惡意程式是 3 種專門竊取比特幣的惡意程式，程式名稱為 BKDR_BTMINE、TROJ_COINMINE 及 HKTL_BITCOINMINE 這 3 種，當比特幣被偷時，用戶個資恐一併洩露，建議比特幣擁有者，要採取個別錢包與離線管理方式，以降低受害機率，只是降低並不是完全就不會有受害的可能性，當電腦有在場礦有就是採比特幣時如果中了上述的程式要怎麼知道?非常簡單的辦法就是，當沒有在採礦時電腦的速度跟採礦時一樣慢，而且電力的耗損也會非常高如果上述兩點都有的話，那就有很高機率是種了上述之惡意程式，因為採礦時會非常耗損電力以及電腦上可用資源，如果中了上述之惡意程式會有什麼後果，1.你的電腦上的資源會被駭客奪走拿去挖比特幣，2.你電腦上再挖的比特幣也會被駭客拿走，所以你會以為妳什麼都沒有挖到但實際是，被不肖的駭客拿走了，根據 12 月那時的統計，全球已經超過了 1

萬 2000 多台電腦中了這種惡意程式而 50%的受害者來自日本、美國、澳洲等前三名的受害者，這些惡意軟體還只是一開始以現在資訊發達的年代，再過個幾個月如果比特幣還是沒有退熱的趨勢那是必還會有更厲害更危險的惡意軟體出現。

10. 比特幣的交易方法

既然比特幣在國際間那麼火熱，那麼它又是怎麼交易的呢？有哪些平台是有比特幣的交易項目的呢？在這段裡將會做詳細介紹。

比特幣是比較像是電子郵件般的電子現金，而要進行交易的時候交易的雙方必須有兩種東西才能交易，這兩中東西分別是類似電子信箱的『比特幣錢包』還有像是電子信箱位址的『比特幣位址』而交易的過程則是由收款方發出一個收款位址，然後付費方則是透過電腦或平板、智慧型手機按收款方發出的位址將比特幣發送給收款方，其實這個過程很像是電子信箱的收發，而下表則是比特幣錢包與位址的一些相關網站。

使用者端名稱	網址	許可協定
Multibit（雲端資料區塊功能）	http://multibit.org/	MIT
Bitcoin-Qt（中本聰使用者端）	http://sourceforge.net/projects/bitcoin/	MIT
My Wallet（線上錢包，獨立式）	https://blockchain.info/wallet	專有軟體
Coinbase（線上錢包，混合式）	http://coinbase.com	專有軟體

使用者端名稱	網址	許可協定
Electrum	http://electrum.ecdsa.org/	GPL
Armory（具有離線儲存功能）	http://bitcoinarmory.com	AGPL

10-1 比特幣位址

比特幣的位址是在交易的時候必到的其中一個東西，那麼他的位址結構又是怎麼樣的呢？

首先比特幣位址它是一組３４位元的字母和數字組成的，但是它的位址開頭總是會由數字１或３來當開頭例如下列這串位址

『1DwunA9otZZQyhkVvkLJ8DV1tuSwMF7r3v』

而比特幣的生成軟體通常可以自動生成位址，而在生成位址的過程中是可以不用連線的，據說比特幣能用的位址大約有 2^{160}個，也就是說比特幣位址基本上是很難用完的。

10-2 比特幣私鑰

關於比特幣的私鑰,我們可以把它理解為我們一般銀行的帳戶密碼一樣，基本上一組比特幣私鑰是跟一組比特幣位址是一對的，比特幣位址就像

是我們的銀行帳號一樣它會記錄你所擁有的多少比特幣，而使用者隨時都可以為自己的比特幣生成一組位址，生產出來的位址會搭配一組私鑰而這組私鑰就是你擁有比特幣位址的證明，如果私鑰遺失了那麼互相匹配的比特幣位址也將無法被使用，他並不像銀行帳戶那樣提款密碼忘記的時候，只要有辦法提出身分證明就能把密碼重設，因此在比特幣位址生產出來以後互相匹配的那組私鑰就一定要保管好以免無法使用。

10-3 交易手續費

大家都知道在銀行跨行轉帳或是提款的時候都會有一筆金而不大的手續費,那麼比特幣的交易是否也要交易手續費呢？基本上是不用手續費的，就像前面交易方式中有提到的比特幣的交易就好比是傳送電子郵件一樣，當然還是有特殊情況比如一次交易的比特幣金額過於龐大，所以需要從多個比特幣位址上提領來支付的話，由於資料量過於龐大因此比特幣網路就會要求附加一點小額的手續費，只是到目前為止比特幣的交易大多是沒有支付手續費的。

10-4 交易確認

比特幣在交易時他的交易資料通常會被打包到資料塊或是區塊中，而當交易資料被打包的時候比特幣的交易就算是進行了初步的確認了，當資料區塊要連接到前一個資料區塊的時候，比特幣的交易會在得到更進一步的確認，在連續6個資料區塊連結確認以後，這筆交易基本上就是得到了不可逆轉的交易確認了。

比特幣的所有歷史交易紀錄都會被儲存在對等網路中的區塊鏈，區塊鏈到目前為止都還在持續延長中，而所謂的區塊鏈實際上就是一群分散的使用者端的節點，這些使用者會組成一個分散式的資料庫，這個資料庫中會儲存所有的比特幣交易歷史，而這些資料量慢慢的變大的時候相信使用者都不希望太多的資料儲存在自己這邊，基於這個原因比特幣的發表者中本聰也有準備了對策，他採用了雜湊函式的機制，使用這機制的話就能自動的去剔除使用者端那些使用者自己永遠用不到的部分，列如一些在最早期的時候的那些比特幣交易紀錄。

10-5 錢包的概念

前面有說到在比特幣的交易必須要具備兩個東西才能交易，一個是比特幣位址，而另一個就是比特幣錢包，比特幣位址在前面已經有解說相關的一些概念了，那麼現在來說說比特幣錢包吧。

比特幣錢包的概念其實很簡單，它就像我們的儲蓄帳戶一樣比特幣通常都會儲存在比特幣錢包中，並且我們能用比特幣錢包來生成一組位址跟私鑰，只要有了位址那麼使用者就能接收來自其他人傳過來的比特幣，而我們也需知道了他人的比特幣位址我們才能進行比特幣的轉帳步驟，這就好像是當人家要匯款給自己的時候我們必須給他我們的儲蓄帳戶的帳號，而比特幣錢包裡面儲存的不只是比特幣的數量，他還會把我們生成的位址跟私鑰也一併保管在裡面，簡單的說比特幣錢包的作用就是在儲存與保管跟比特幣有關的相關資料。

11. 比特幣的法律現況

現在比特幣那麼夯那麼比特幣到底有沒有受到法律的保戶或約束呢？

以目前的狀況來看，比特幣是被認為合法的，但是它的卻是被以一種虛擬商品來受到法律的保護，而把比特幣當成貨幣來看的話到目前為止國際中還沒有確立的法律來指出它是一種貨幣，既然它不是一種貨幣的話那麼它在現實生活中會帶來哪些的不便呢？例如當商家接受了消費者用比特幣來買東西的話，這樣的交易只能被看成以物易物而已，但是以物易物的交易在將來要稅收申報的時候卻比一般金錢交易還要麻煩。

11-1 國家相關法律

到底比特幣在各國中有哪些相關的法令呢？這邊就舉幾個比較大的國家來說吧。

1.中國：在他們的人民幣管理條例中就規定了，禁止製作或販售代幣票券可是它們卻沒有明確的司法解釋與定義，所以比特幣如果在中國被列入代幣票券的話，那麼比特幣在中國將是不被承認的，而在 2009 年的時候終於明確的規範，在規範中指出網路虛擬貨幣將不得用在支付或是購

買任何實體產品與任何企業的產品或服務，這樣做是為了防止虛擬貨幣可能對實際貨幣的經濟金融秩序造成衝擊。

2.歐洲：歐洲央行發表了虛擬貨幣架構的報告，報告中說道有關虛擬貨幣的體系與相關架構，並說到儘管這個虛擬貨幣體系可能是金融架構上的創新，並為消費者提供了另一個支付管道，且能發揮其積極的作用，但是它也會產生一些風險，但是在報告中有補充道由於虛擬貨幣體系的規模小，所以它的風險基本上只會對這個體系的使用者有影響，至於其他人將不會受到虛擬貨幣體系的影響。

3.美國:在美國的財政部裡的金融犯罪執法系統FinCEN也發表了虛擬貨幣的個人管理條例，在條例中首次闡明了虛擬貨幣 FinCEN 法規定義貨幣(這裡也包括實際的貨幣)為美國或者其他國家的硬幣或紙幣,它們被指定為法定的貨幣,可以流通,通常有國家發行,作為交換的媒介被使用。

12. 比特幣是否能瞬間致富

現在比特幣瞬間上漲，但是之前就有人在開採比特幣了，那現在豈不是像前面說的身價瞬間漲了 90 多倍，不是瞬間就變成富翁了，在之前就有個例子在比特幣還沒有像現在一樣那時比特幣大約 200 多美元左右，然後就有個冰島人就想說那是什麼不然買個 100 個比特幣來看看好了，那個冰島人也沒多想就買了 100 個結果到了最近比特幣突然的上漲一長就是好幾倍，結果現在那個冰島人瞬間便成了富翁。

同樣還有以現在的經濟不景氣想要環遊世界根本是在說白日夢，除非你是那個有錢的富豪或富二代不然真的有辦法環遊世界真的很難，但是現在就有人因為之前買的比特幣現在突然的上漲成功的完成了環遊世界，也有人用了比特幣買，小至比薩大至房子、汽車。

前面說了那麼多的例子換另一個角度說比特幣真的可以致富嗎?如果某一天起床發現比特幣跳票了那不就是完蛋了，就有人說一個例子說比特幣就像黑色鬱金香為甚麼這樣說，黑色鬱金香的故事是這樣的在十七世紀中葉荷蘭掀起黑色鬱金香的熱潮，在那時單株名貴的鬱金香可以賣到的價錢與那時的牛相比，差了 13 倍也就是說一株鬱金香換 13 頭牛，而那時的人民也要不吃不喝 10 年才買得起，然後隔一年後價格不減反上漲

人民要不吃不喝 44 年才買得起，然後再同一年的二月的某一天鬱金香的價格突然暴跌，跌到一文不值因為有很多人投資在這次的鬱金香，導致有很多人損失慘重還血本無歸，所以這就是別人說的黑色鬱金香事件，到底比特幣會不會跟鬱金香一樣突然的暴跌著個沒有人知道，比特幣到底能不能致富這也沒人清楚，這裡只能說不要貪一時之快，一步一腳印做踏實人才是最好的。

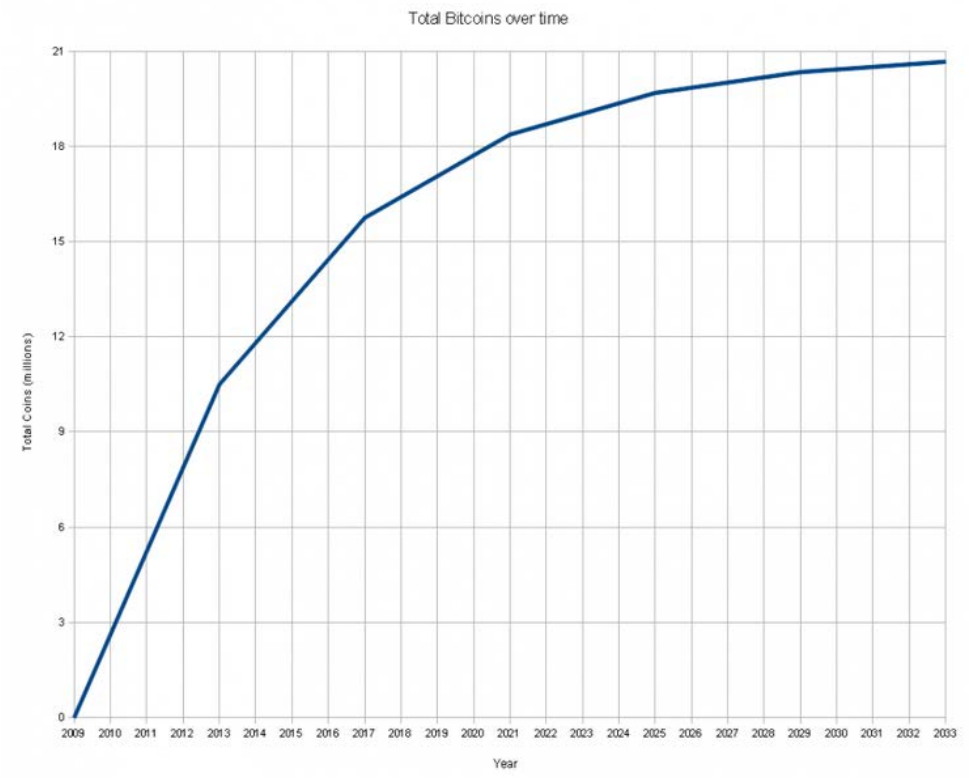
13. 比特幣的發行數量

大家都知道國家貨幣是由國家的中央銀行所發行的，在中央銀行要發行貨幣的時候是有相關的規定的，雖然各個國家的規定都不一樣，但是在其數量上還是會有所限制的，那麼跟現實貨幣做比較的話比特幣的發行有甚麼樣的規定或限制呢？

首先比特幣跟現實貨幣不一樣的地方在於，現實貨幣是各國央行發行的而比特幣則沒有所謂的央行，但是比特幣會透過一些技術讓比特幣每四年就會把發行量減半，最終能夠流通使用的比特幣總數量大約２１００萬個，而且已發行的比特幣總量是能夠隨時查詢的。

那麼到底有多少比特幣發行了呢？目前估算大約有１２００萬個比特幣在市場上流通，這個量已經超過最終數量的５０％，而且到２０１７年的下半年全世界流通的比特幣大約是最終數量的７５％，而最終估算在２１４０年的時候將會生產出最終數量的２１００萬個，其生產完２１００萬個比特幣以後也將不會再有比特幣備生產出來，看完了以上的數量估算相信大家都發現了為什麼生產時間越來越長了呢？其實這是跟一開始就有提到的讓比特幣產量每四年就減半的技術有關。

接下來我們就來說說這個技術吧，比特幣會產生得越來越慢是因為比特幣網路生成資料塊需要的計算難度只要每次過2016個資料塊就會進行調整，則調整方式是以之前產生2016個資料塊實際所消耗的時間，這個調整讓使得之後每生成一個資料塊的預期時間為10分鐘，而2016個資料塊整理也就等同約兩個星期就會調整一次難度，到2012年11月要生成資料塊的計算量所要耗損的時間相當於創世資料塊的100萬倍，而這樣子的設定是為了讓那些早期就把電腦資源加入比特幣挖礦活動中的使用者比晚加入的使用者還容易獲得比特幣，會這樣的設定也是為了在早期就讓比特幣可以有很高的吸引力讓比特幣可以吸引到足夠的計算力，如果不這樣子的話最初的比特幣就會因為無法做交易活動，那比特幣的經濟也就無法成立那也就將停止了。



（圖六）

圖六是上述的從 2009 年開始到 2033 年比特幣的生成走勢圖由上圖所見的與我上述說明的大約會在 2017 年比特幣的生成率就會到達 75%

14. 中本聰

大家應該都想知道中本聰吧?應該說連我自己都想知道了因為看了所有與比特幣相關的文章後，吸收到了比特幣的相關知識知道比特幣是用很厲害的演算法，誕生的得知了如果想要攻破比特幣網站是非常困難的，所以同是資訊類的人應該都會想知道中本聰是誰，他是怎麼寫出這個程式想要研究一下，如果不是上述的那種，那我猜想知道中本聰是誰的第二點，因為目前比特幣只知道是中本聰但卻不知道他真正的身分，而他做出比特幣是想作什麼有沒有可能是，中本聰他這個人想要讓比特幣紅起來在把自己已經事先，製作好的比特幣賣出來大賺一筆錢想要來炒個短期的買賣，再來他就可以不用再管比特幣讓比特幣泡沫化，但中本聰沒想到比特幣會比她預想的還紅又或者他是故意想讓他更紅，來賺更大一筆,所以有使用比特幣的人會想知道比特幣的創造者是誰也不意外了，，雖然目前也都還不知道中本聰到底是誰但是有關中本聰的線索還是有的，由於線索說法太多所以這也只是猜測但是這些線索慢慢的在解開，慢慢的就會知道中本聰是誰了那我們就來看看線索吧，第一個在 2013 年 9 月多的時候有一則新聞是這樣說的，有研究人員說中本聰有可能是美國華盛頓大學的經濟學教授 Nick Szabo，他們說 Szabo 教授早在 1998 年開始研究類似比特幣的數字貨幣，也有創造一套名為 bit gold 的程式研究人

員認為這套程式是比特幣的測試版，不只這樣研究人員還有其他說法他們說 Szabo 教授在博客(網路的日志)以及中本聰的論文，發現兩個人的用詞一致性非常的高，連書寫習慣也都一樣，還有比特幣要發布的幾個月前 Szabo 教授在找合作的對象但是是不是要做比特幣就不知道了，在這之後 Szabo 教授有出來澄清自己不是中本聰但是因為證據顯示，中本聰有可能是他，第二個在 2013 年在日本有一篇文章是說中本聰或中本哲史，(中本哲史同中本聰)在 2009 年他為比特幣的系統建立了開放原始碼的項目，然後宣告比特幣的誕生到了 2012 年的 5 月在國外的報導在 YouTube 上有人爆料比特幣的創始者是誰，影片中是說比特幣的創造者是京都大學的數學教授望月新一，望月新一再 16 歲就進了普林斯頓大學在 22 歲就讀完博士，33 歲就當上東京大學的全職教授，就上面的資訊告訴我們他是一個天才如果他是中本聰也不意外，而爆料者說有三點證明我是覺得這三點就要證明他是中本聰是有點難，他說的第一點是說望月新一以他的頭腦是有可能想比特幣複雜系統的那個人，第二點他說望月新一不常使用常規的學術發表而他是習慣獨自工作，發表論文後是讓別人自己理解，第三點是說望月新一的工作領域也有含括像比特幣那種的數學演算法，依我的觀點來看我覺得中本聰是望月新一的可能性會比較高，第一我覺得以第一的線索來看在論文方面那些都是可以拿過來在自己重製的，而線索一中有說 Szabo 教授在找人技術合作這點我覺得如果真的

找到人合作做出了比特幣，那在網路上有人提問中本聰是誰的時候就會有人出來爆料因為，我覺得如果比特幣是一個團隊做出來的話被爆料出來的機率會非常高，而單獨做的話要不要說自己都能做決定所以我覺得比特幣應該是自己完成的，第二我覺得從望月新一他以前的資料來看 16 歲就上了大學 33 歲當教授，這是一件非常厲害的事以他的聰明才智加上他的專業領域，說他是比特幣的創造者不為過。

15. 如何挖比特幣

在這前面說了很多關於比特幣，說了有關比特幣是如何製作出來的、說了比特幣用了甚麼機制來做到比特幣的生產越來越慢、說了比特幣被國家承認會有甚麼樣的風險會帶來怎樣的商機以及帶來怎樣的便利性，但是說了那麼多怎麼沒說到怎麼去挖比特幣，所以現在我就要把怎麼挖比特幣的方法說出來，那就切入正題要挖礦是需要一點工具的第一我們需要一個錢包，錢包就是要把挖到的比特幣收到放進來保管，而錢包有大致分成兩種一種是軟體式第二種是網頁銀行我介紹的是軟體式的錢包，因為軟體式的錢包的安全性是自己來掌握了，所以應該是比較多人選擇的錢包種類而網頁銀無法保證網頁的安全性，應該是比較少人要選的種類而錢包在網路上也有很多種，我在這裡要介紹的是 bitcoin 的軟體式錢包，把這個軟體安裝好了之後把程式打開，第一次打開會先要更新而因為比特幣是採取全世界金融資料同步模式，所以有出現一筆金融交易資料的出現就都會更新到電腦程式裡，導致第一次的更新時間會有點久更新時間是依網路的速度來決定，網速越快更新越快網速也慢更新越慢這樣錢包就完成了但是切記，請時常做好備份因為比特幣錢包是把你所有挖到的比特幣資料存放在你的電腦裡，如果沒有備份到那哪天電腦中毒或出問題你的比特幣資料就會全都不見，有了錢包再來是挖礦的工具

就像礦鎬而礦鎬就是電腦，礦鎬的好壞也就是電腦的好壞的差別是挖礦時的執行速度，有了挖礦工具再來就是要有地點可以挖礦的地點而逛池也就是所謂的 Server(伺服器),不同的 Server 也有不同的抽成規則選好 Server 再來需要去註冊註冊完了就可以來去挖礦了喔。

16.參考文獻

http://zh.wikipedia.org/wiki/Wikipedia:%E9%A6%96%E9%A1%B5

維基百科

http://stock2012.pixnet.net/blog/post/156213656-%5B%E6%99%82%E4%BA%8B%5D-%E5%BE%B7%E5%9C%8B%E8%AA%8D%E5%8F%AF%E6%AF%94%E7%89%B9%E5%B9%A3%E4%BD%8D%E5%85%83%E5%B9%A3(bitcoin,btc)%E5%90%88%E6%B3%95,#axzz2pL5aLT1Y

比特幣相關之料

http://www.chinatimes.com/newspapers/20131228000044-260202

中時電子報-大陸相關

http://www.chinatimes.com/newspapers/20131231001176-260303

中時電子報-台灣禁用比特幣

http://www.chinatimes.com/newspapers/20131218000276-260210

中時電子報-華義承認比特幣

http://www.chinatimes.com/realtimenews/20131230004818-260410

中時電子報-台灣不接受比特幣的原因

http://news.cnyes.com/Content/20140103/KISZ1Y5053H62.shtml?c=us_stock

鉅亨網新聞中心-中印為何打壓比特幣

https://tw.money.yahoo.com/column_article/adbf/d_a_140108_53_47gmq

奇摩理財-比特幣與黑色鬱金香

http://cn.investing.com/currencies/btc-usd-historical-data

比特幣現有匯率走勢圖

http://media.yucasee.jp/posts/index/13807

中本聰的身世之謎

http://www.techbang.com/posts/16009--finds-the-nearest-bitcoin-inventor-astute-person-who

T 克邦-中本聰

http://home.gamer.com.tw/creationDetail.php?sn=2232607

比特幣錢包

17. 結論

比特幣或許真的能瞬間致富，但是比特幣也能讓人瞬間一無所有，雖然比特幣的網站以及網站的演算法很厲害，是很難被破解攻破但是弱勢的並不是比特幣的網站，而是即將與比特幣合作而推出的商品的網站，所享用比特幣購買東西的人須特別注意要仔細想想風險，尤其是現在有關比特幣的惡意程式出現哪時你以比特幣交易突然被重複扣款，等之類的問題出現也不會覺得奇怪，雖然比特幣能帶給我們更方便的生活但是要等比特幣真的能用還要等上一段非常長的一段時間了，或許等哪天美國真的讓比特幣合法，也正式發行比特幣，其他國家也認同比特幣的時候到了那時說不定也就能比較放心使用比特幣了，不然現在要用要擔心的事太多了。