Oct. 18th 2016

虛擬貨幣挖礦 AlcheMiner Tom Soong



Tom Soong簡介

- 老礦工一枚
 - 挖過BTC、LTC、ETH
 - 挖礦工具: CPU、GPU、ASIC
 - -個人化挖礦、中心化挖礦(礦場)
- 為客戶做過世界第一顆28奈米BTC挖礦晶片
- 創立AlcheMiner: 生產LTC挖礦晶片、礦機
- 幣圈經歷:2013.06~

大綱

- 簡介比特幣挖礦原理
- 挖礦晶片和挖礦製作
- Q&A

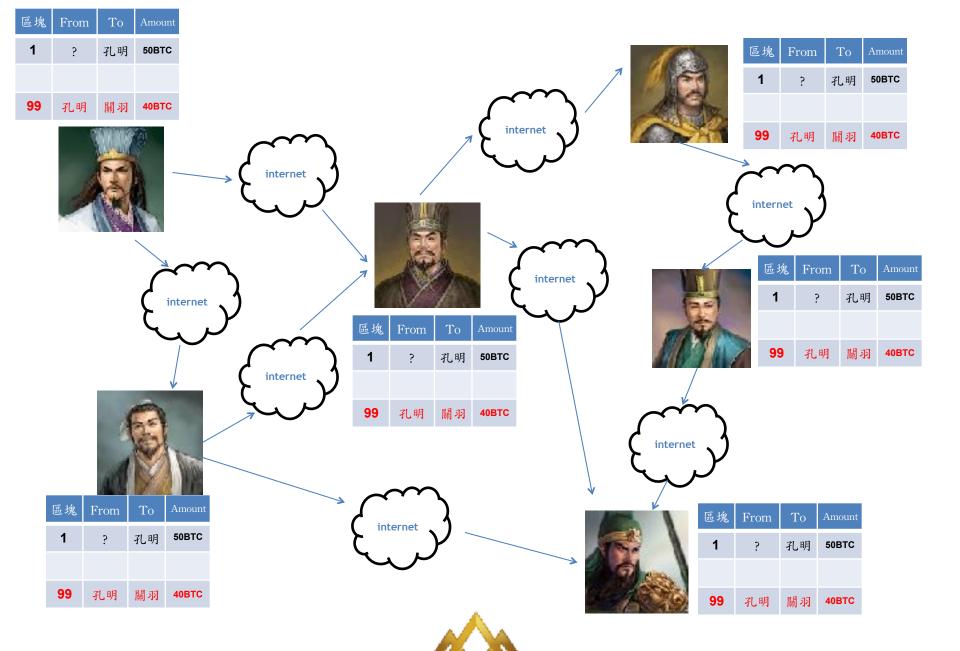


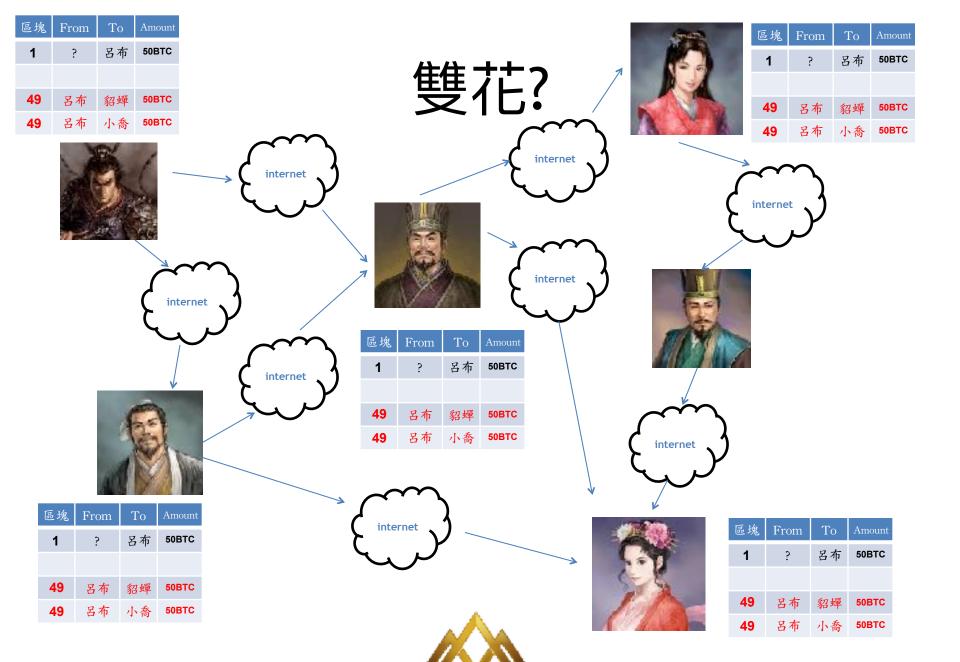
甚麼是虛擬貨幣挖礦?

- 中本聰2008提出比特幣論文和程式:
 - 找尋符合需求的SHA256特徵值
 - -系統控制平均每10分鐘會被找到一個區塊。
 - 每2016個區塊調整一次難度
 - 找到區塊的人會得到50個比特幣獎勵(貨幣發行)。
 - -找到區塊的人可以得到被打包進入此區塊內所有 交易的手續費
 - -區塊獎勵每4年減半一次

為什麼比特幣需要挖礦?

- 從礦工角度出發
 - -利益回報,得到新發行的比特幣和手續費
- 從系統角度出發
 - -事後結、清算
 - 記帳權去中心化
 - 避免雙花、交易屏蔽等系統性風險

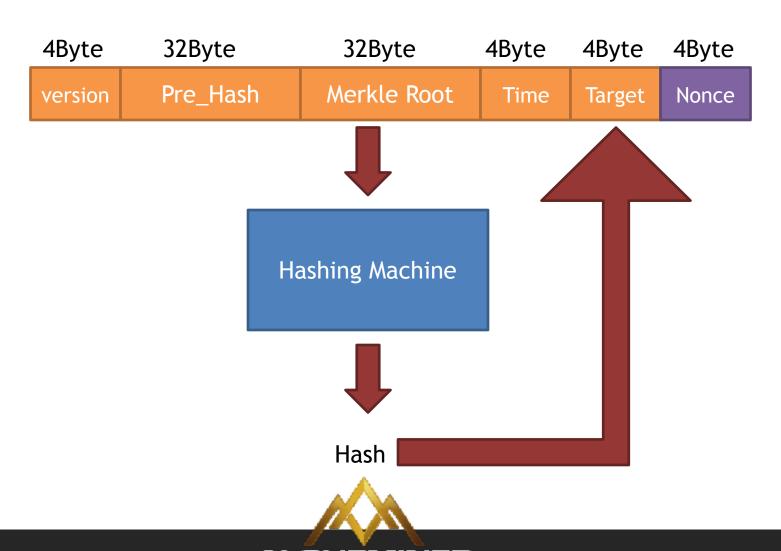




誰說得算?

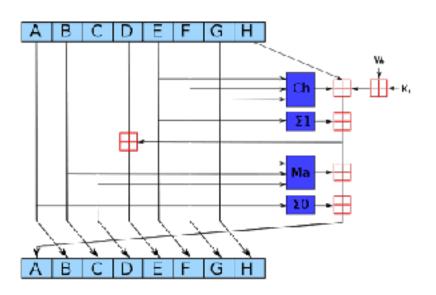
- 結、清算動作
- 比賽
 - 沒有捷徑
 - 憑實力決勝負
 - 赢的人有獎品

Bitcoin Hash



SHA256

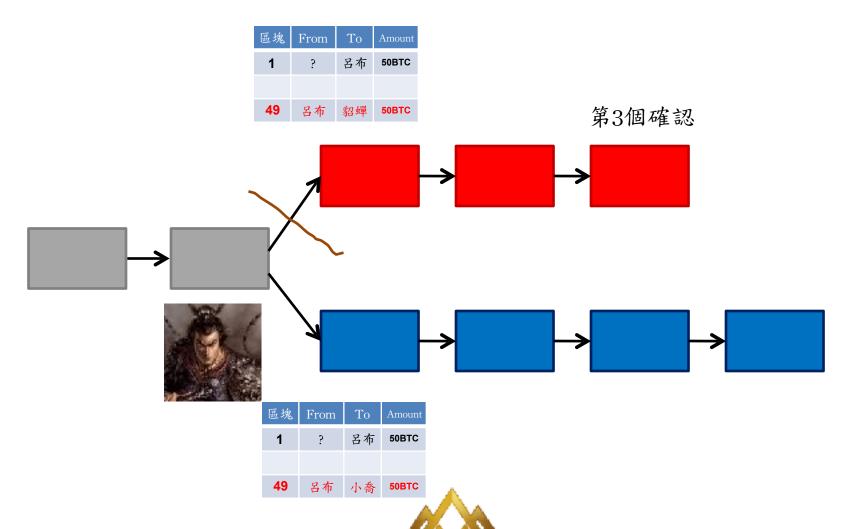
- Bitcoin Hash(x)= SHA256(SHA256(x))
- 手算一次給你看



為何交易所需要超過N個確認?

- 大部分比特幣交易所要求3個確認
- 金額愈大要求確認數愈多

51%攻擊



挖礦的演進

- 電腦(CPU)
 - Core i7 3930k 66.6 Mhash/s
- 顯示卡(GPU)
 - AMD 7970 825 Mhash/s
- 專業挖礦機(ASIC)
 - 我的第一台挖礦機 550 Ghash/s
 - 目前市場主流 4.7 Thash/s

聯合挖礦

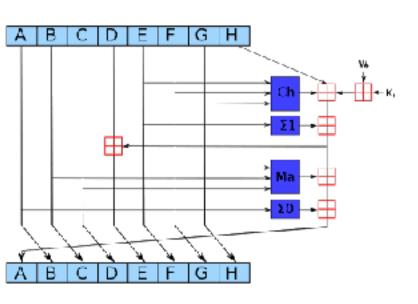
- 礦池崛起
 - 將題目變簡單分給礦工
 - -按照貢獻分潤
 - 礦池收取手續費



如何製作挖礦機



RTL

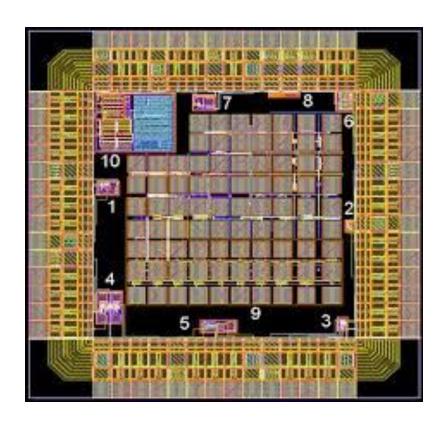


```
- U X
@ sne-256-functions.v (E/Google 表现经验Drookey)-_iner_rechnical RFT/Sight ning 5:9 140425 V40 - 3/MVI
概義の 建築の 三萬円 高きが等(1) 編ぎる(3) 核省(4) 網が物(5)(4)
MODEL OF IX. 110
       input [36 0] 2
       mepat [81:4] 9:
       acet ja p . (x[1:0] a[31:2]) . (c[42:0], c[54:15]) . (c[54:0], x[34:25]);
erdraculs
methic of (v. 33)
       taput [01:0] 4 | sutput [21:2] 1;
       2004 pe y - (H[5:00] + [01:6]) * [0[:00:0] + [4:11]) * [4[[4:0] H[#1:25]]);
erdentule.
acquir co (x, j, r, o)
       taput [30:0] c. Q. J;
petput [01:0] e:
       assign o - 2 7 (a k (y 20))
at dim time.
nedule rul (c. Q. J. a);
       isput [31:0] c. p. 21.
       petpat [Biid] ..
       155130 0 * (X & 9) | (2 0 12 | 910)
```

Gate-level netlist

```
l∰ nghining 0428 cook (E./Google 書篇模式, ghining 659 140428 V5 ECObySk/fi - GVIM
名字(5) 组织(5) 工具(7) 特法及录(5) 提明显(6) 视窗(M) 特別規則(H)
module sys_rst_1 { rst_m_all, clk, rst_m };
 imput est a all, alk;
 output est no
 wire rst_Z_ rst_t_ rst_W_:
 DFCMQU18HP121 rst_reg_8_( .D(1'b1), .CP(clic), .CDN(rst_m_all), .U(rst_8)
 DEGMODIBHE12T rist_reg_1_ ( D(rist_R_), .GP(clk), .GDM(rist_n_all), . f(rist_1_)
 DECMODITARTIZE rst_reg_2_ ( D(rst_t_), .CP(clk), .CDN(rst_n_all), .Q(rst_2_)
 DFCNQD10HF12T rst_reg_1_( .D(rst_2), .DF(clk), .DDN(rst_n_all), .Q(rst_n)
endrodule
nodule sys_rst_8 { rst_m_all_cik, rst_m );
 input rst_n_all clk:
 output rst m:
 wire n2, rsl 2, rsl 1, rsl 8;
 DICMQUIDM:121 rst_reg_2_( .D(rst_1_), .DP(c1k), .DDM(rst_n_a11), .U(rst_2_)
 DFUNQUIBHF121 rst_reg_1_( :D(rst_U_), :DF(clic), :UDN(rst_n_all), :Q(rst_1_)
 DEGNOD18HP12T rst_reg_b_( .D(1'b1). .GP(c1k). .GDN(rst_n_a11). .Q(rst_b_)
 DECMDANUP12TIUT rst_reg_3_ ( .D(rst_2_), .CP(clk), .CDN(rst_n_all), .N(n2),
        UHI I E:
 DUFFXD160VP12TLVT GL3 ( .1(n2), .2(rst_n) );
 of Futboarba
```

GDSII



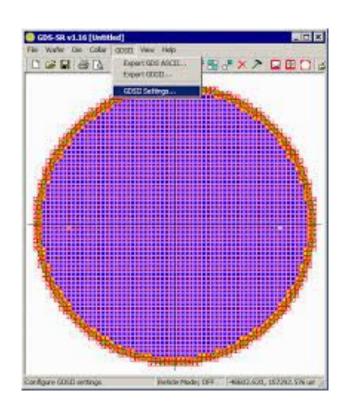
40条米?

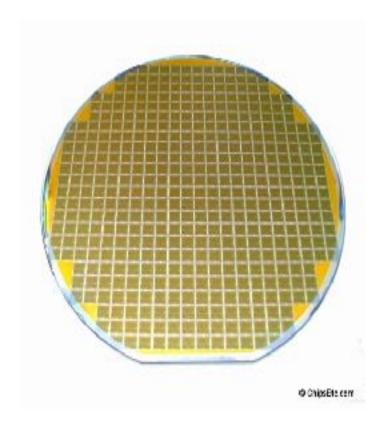
28条米?

16条米?



Wafer => Dies





Package





PCB => SMT





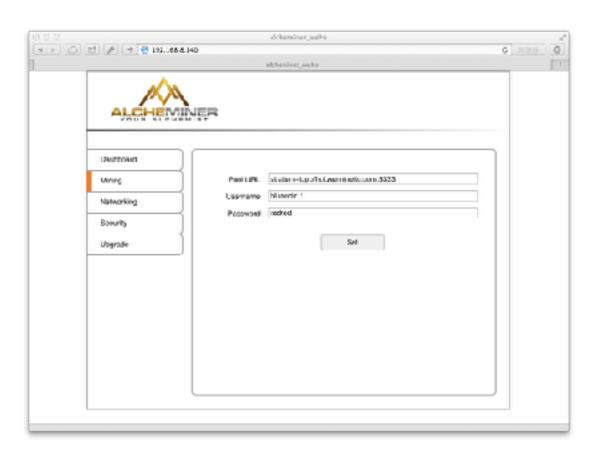
挖礦系統







挖礦軟體整合



插電連網



如何評估挖礦獲利

- 礦機參數
 - 算力、耗電、價格
- 挖礦參數
 - 算力、電費、幣價、預估難度增長、維護費、 所有機器成本
- 挖礦獲利計算機



結論





挖礦前

挖礦後



Thank you!!!



Q & A

