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

ALCHEMINER
YOUR ALCHEMIST

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

區塊	From	To	Amount
1	?	孔明	50BTC
99	孔明	關羽	40BTC

區塊	From	To	Amount
1	?	孔明	50BTC
99	孔明	關羽	40BTC

區塊	From	To	Amount
1	?	孔明	50BTC
99	孔明	關羽	40BTC

區塊	From	To	Amount
1	?	孔明	50BTC
99	孔明	關羽	40BTC

區塊	From	To	Amount
1	?	孔明	50BTC
99	孔明	關羽	40BTC

區塊	From	To	Amount
1	?	孔明	50BTC
99	孔明	關羽	40BTC

雙花?

區塊	From	To	Amount
1	?	呂布	50BTC
49	呂布	貂蟬	50BTC
49	呂布	小喬	50BTC

internet

internet

internet

internet

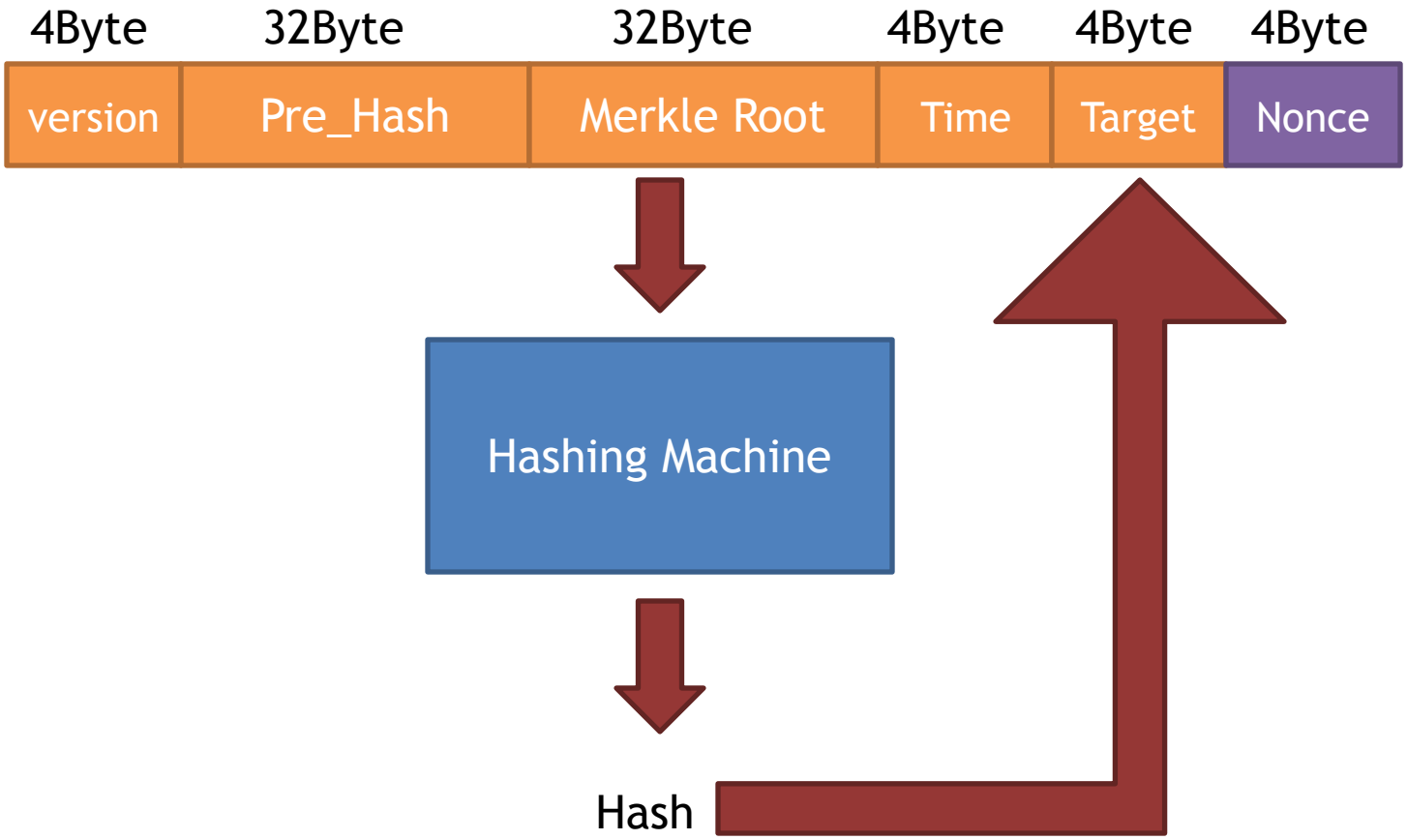
internet

區塊	From	To	Amount
1	?	呂布	50BTC
49	呂布	貂蟬	50BTC
49	呂布	小喬	50BTC

誰說得算?

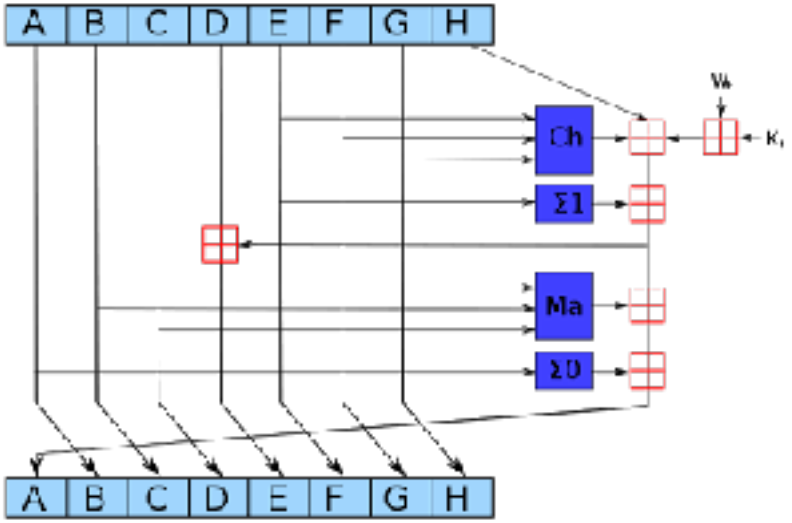
- 結、清算動作
- 比賽
  - 沒有捷徑
  - 憑實力決勝負
  - 贏的人有獎品

Bitcoin Hash



SHA256

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



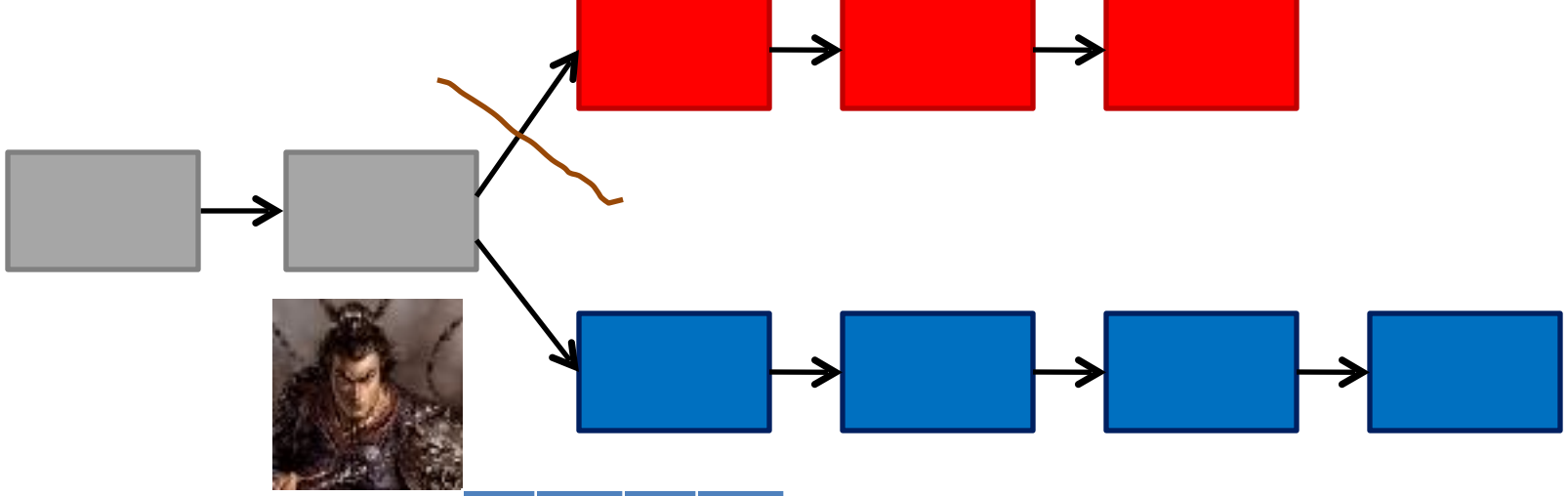
為何交易所需要超過N個確認?

- 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

區塊	From	To	Amount
1	?	呂布	50BTC
49	呂布	貂蟬	50BTC

第3個確認



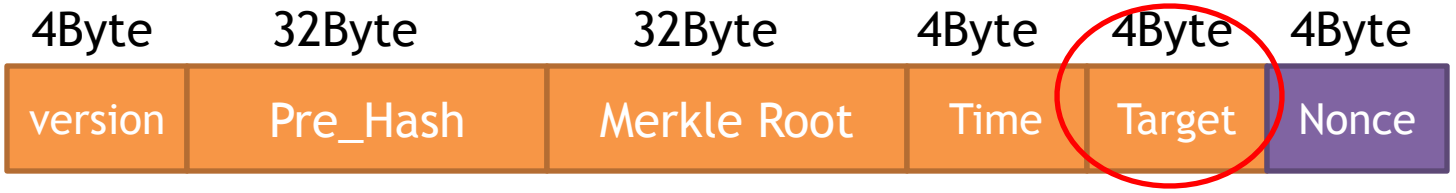
區塊	From	To	Amount
1	?	呂布	50BTC
49	呂布	小喬	50BTC

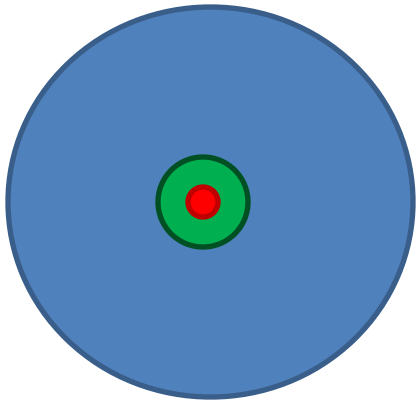
挖礦的演進

- 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

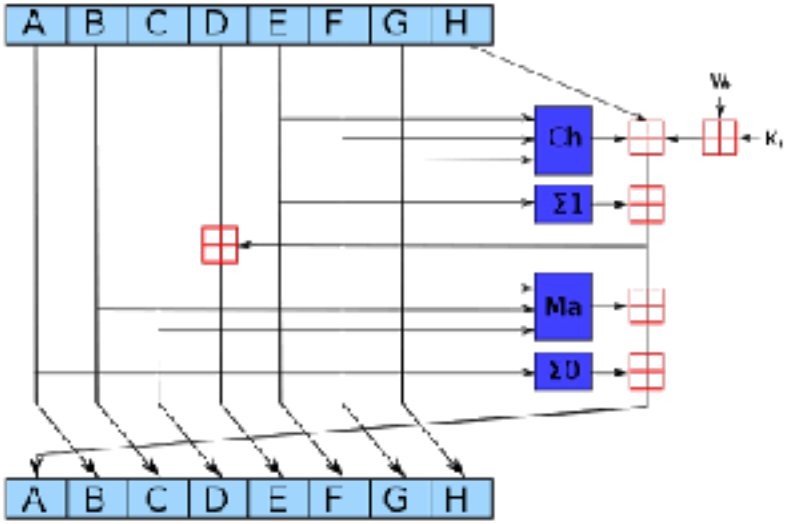


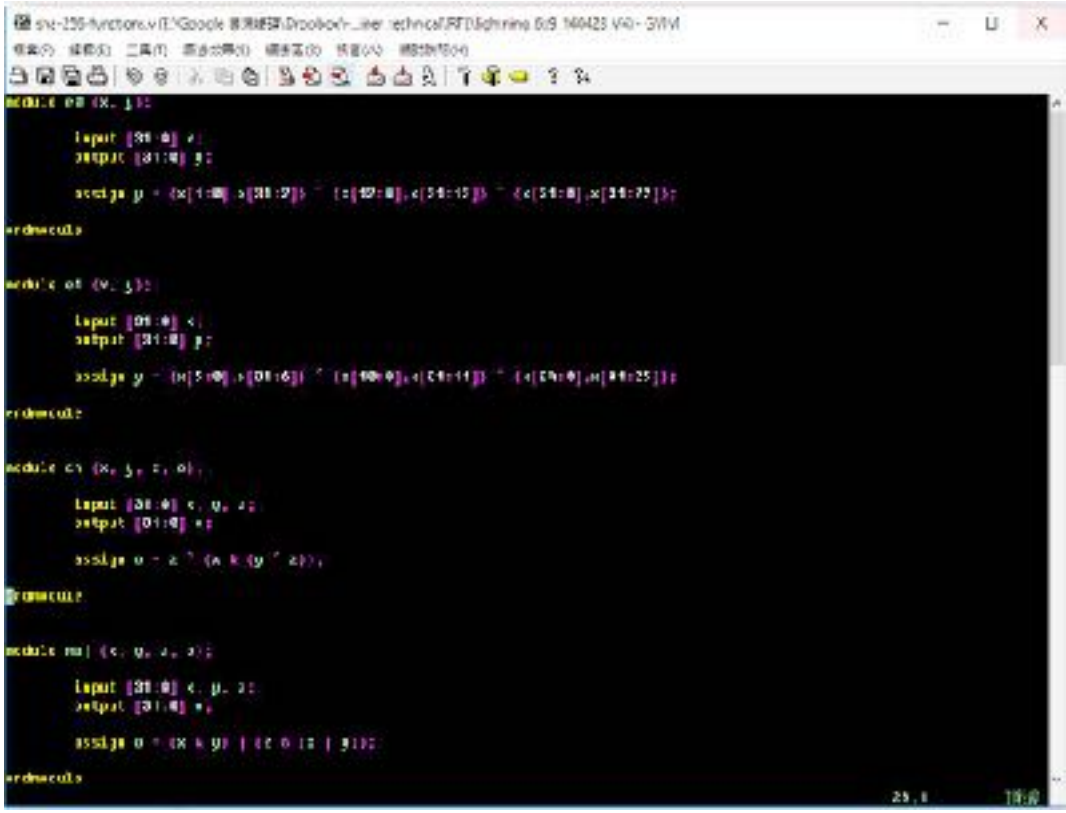


所有Nonce
礦池許可的Nonce
真正目標的Nonce

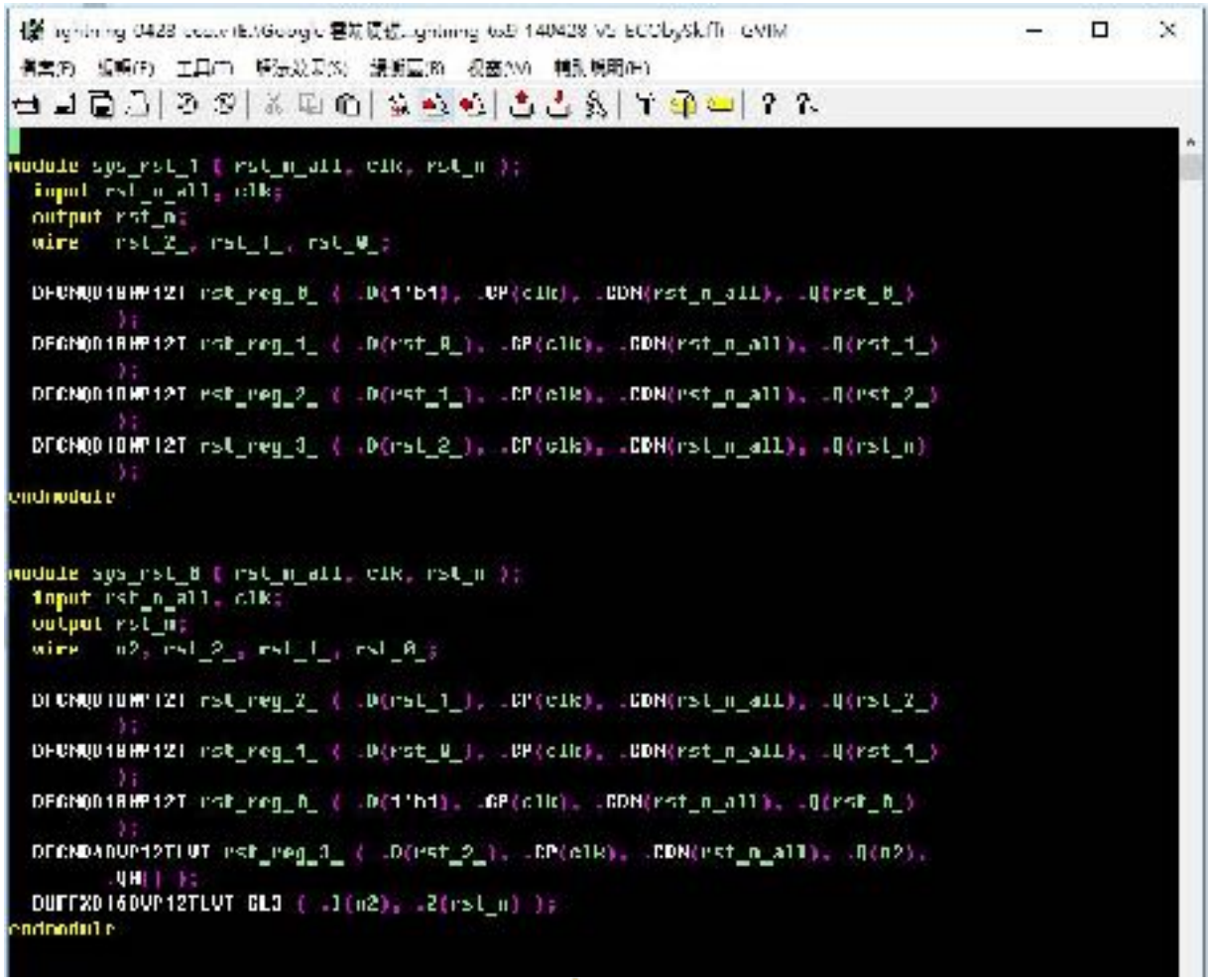
如何製作挖礦機

RTL





Gate-level netlist



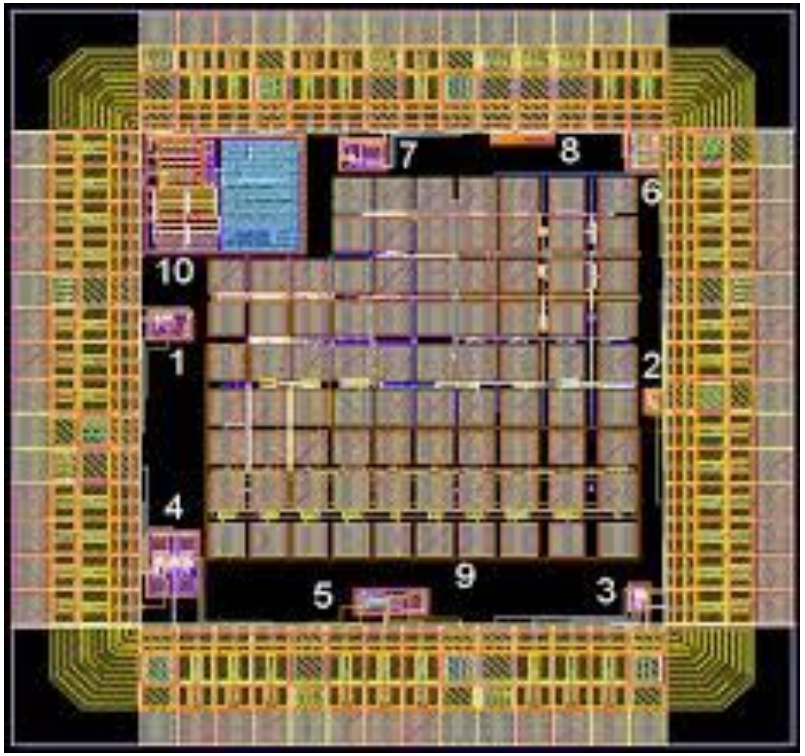
```
module sys_rst_1 ( rst_n_all, clk, rst_n );
  input rst_n_all, clk;
  output rst_n;
  wire   rst_2_, rst_1_, rst_0_;

  DFCNQD1BWP12T rst_reg_0_ ( .D(1'b1), .CP(clk), .CDN(rst_n_all), .Q(rst_0_)
        );
  DFCNQD1BWP12T rst_reg_1_ ( .D(rst_0_), .CP(clk), .CDN(rst_n_all), .Q(rst_1_)
        );
  DFCNQD1BWP12T rst_reg_2_ ( .D(rst_1_), .CP(clk), .CDN(rst_n_all), .Q(rst_2_)
        );
  DFCNQD1BWP12T rst_reg_3_ ( .D(rst_2_), .CP(clk), .CDN(rst_n_all), .Q(rst_n)
        );
endmodule


module sys_rst_0 ( rst_n_all, clk, rst_n );
  input rst_n_all, clk;
  output rst_n;
  wire   n2, rst_2_, rst_1_, rst_0_;

  DFCNQD1BWP12T rst_reg_2_ ( .D(rst_1_), .CP(clk), .CDN(rst_n_all), .Q(rst_2_)
        );
  DFCNQD1BWP12T rst_reg_1_ ( .D(rst_0_), .CP(clk), .CDN(rst_n_all), .Q(rst_1_)
        );
  DFCNQD1BWP12T rst_reg_0_ ( .D(1'b1), .CP(clk), .CDN(rst_n_all), .Q(rst_0_)
        );
  DFCNQD1BWP12TLVT rst_reg_3_ ( .D(rst_2_), .CP(clk), .CDN(rst_n_all), .Q(n2),
        .QN() );
  DUFFX0.16BWP12TLVT CL3 ( .I(n2), .Z(rst_n) );
endmodule
```

GDSII

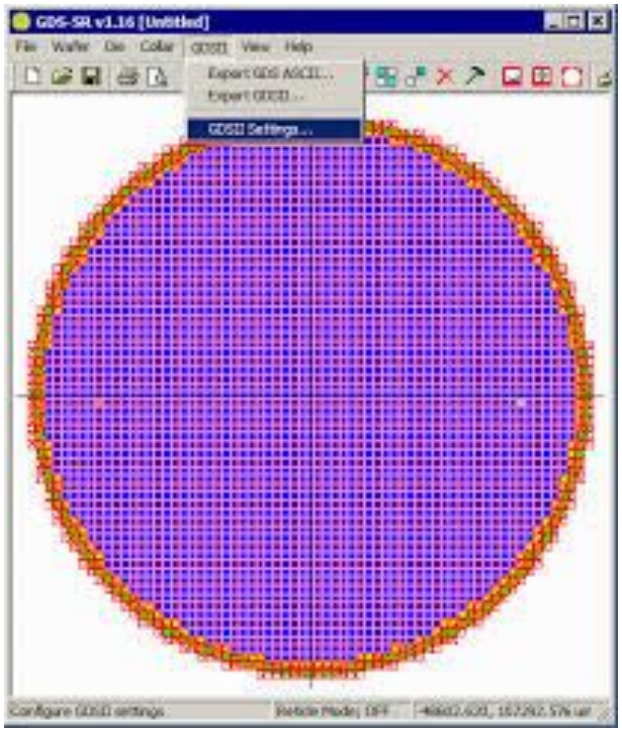


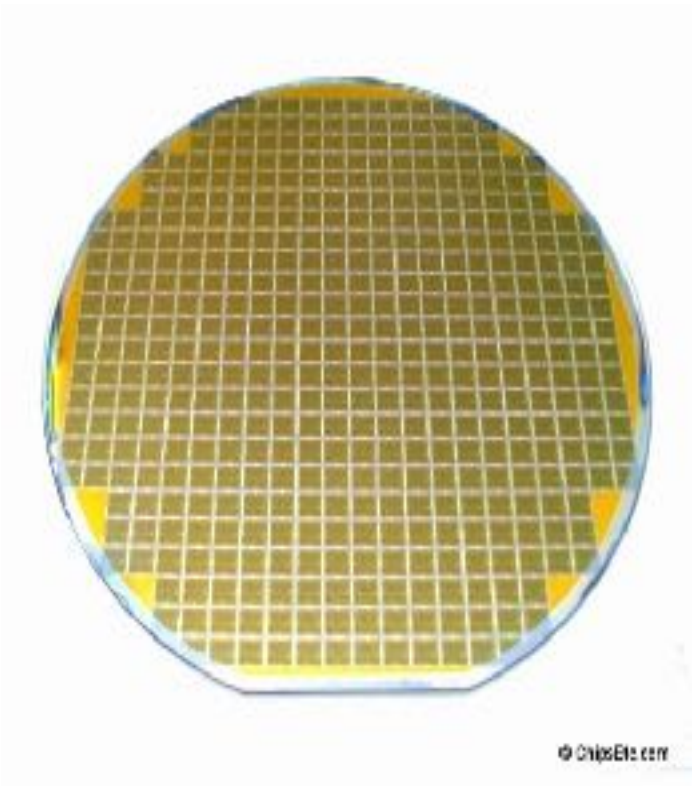
40奈米?

28奈米?

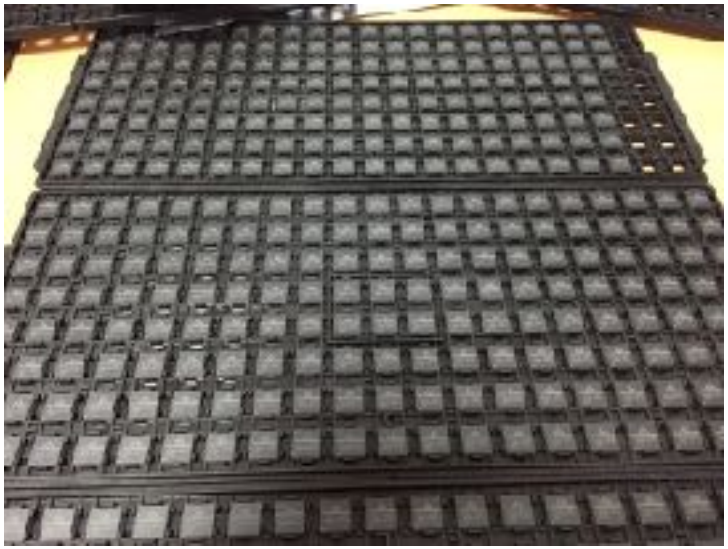
16奈米?

Wafer => Dies


GDS-SR v1.16 [Untitled]
File Wafer Die Color GDSII View Help
Export GDS ASCII...
Export GDSII...
GDSII Settings...

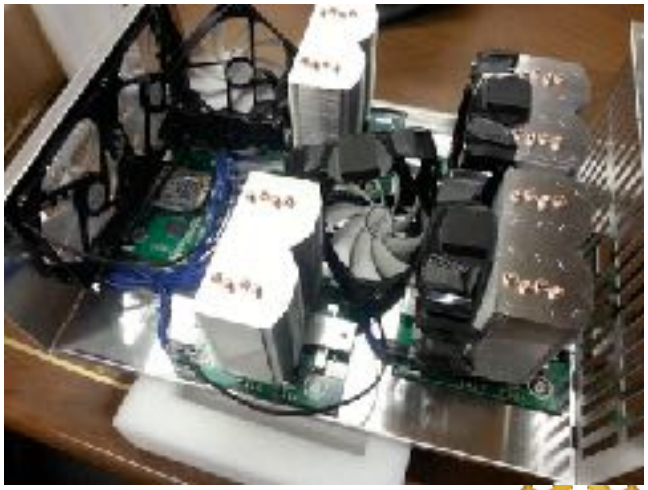

© ChipsEtc.com

Package



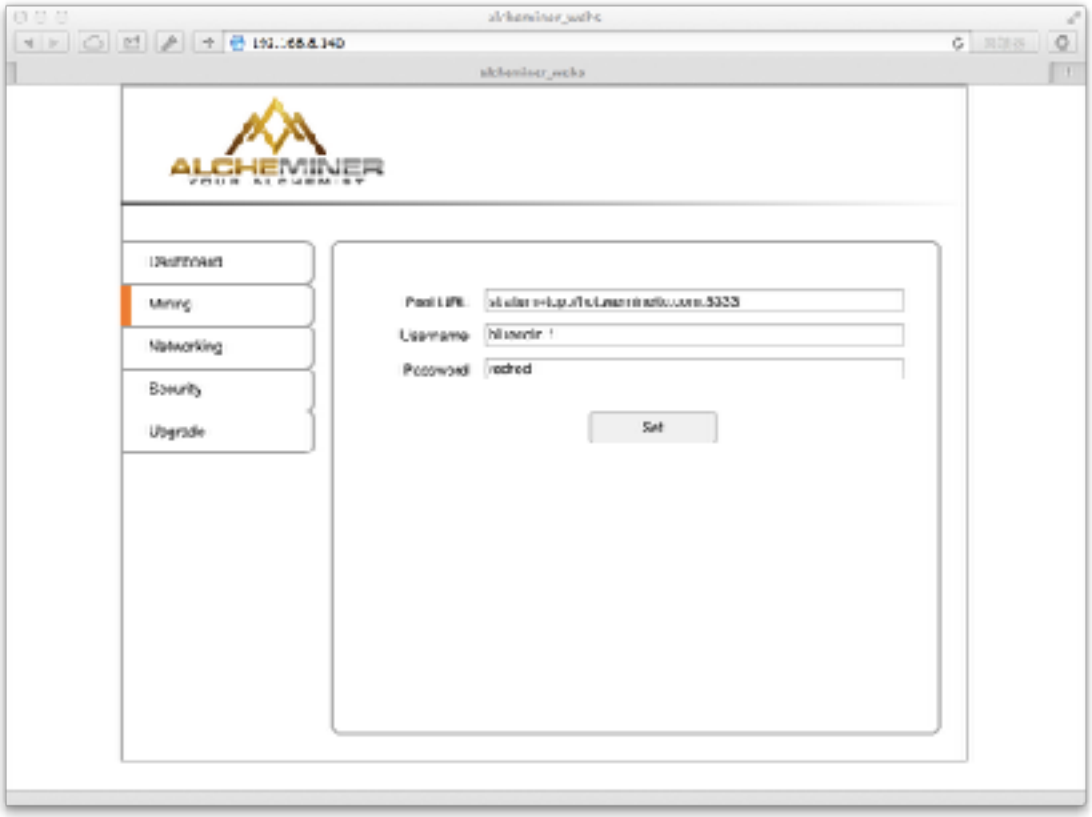
PCB => SMT

挖礦系統



ALCHEMINER
YOUR ALCHEMIST

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!!!

ALCHEMINER
YOUR ALCHEMIST

Q & A