GOLDSTRIKE™ 1: COINTERRA’S FIRST GENERATION CRYPTO-CURRENCY PROCESSOR FOR BITCOIN MINING MACHINES

Javed Barkatullah, Ph.D., MBA
Timo Hanke, Ph.D.
Ravi Iyengar
Ricky Lewelling
Jim O’Connor
BITCOIN MINING WORK

Purpose
• Complex computations required to gain right to clear financial transactions on the Bitcoin network
• Computational work is rewarded with new (mined) bitcoins

Definition
• Given a message \( m \) find a nonce \( n \) such that the 256-bit result
  \[
  \text{Sha-256} \left( \text{Sha-256} \left( m \ || \ n \right) \right)
  \]
  has a specified number of leading zero bits ("target")
• Cryptographic hash functions are “one way” functions
• This search problem is best solved by trial-and-error
HISTORY OF BITCOIN MINING HARDWARE

- **GPU based Platform**
- **FPGA based Platform**
- **Custom ASIC based Platform**

Network Difficulty adjusted every 2016 blocks mined

Graph source: http://bitcoin.sipa.be
GOLDSTRIKE™ 1 ARCHITECTURE

- Motorola compatible 4-pin SPI Port
- PLL with simple bit-bang interface
- 120 Hash Engines arranged into 16 super-pipes
- 128 deep Input Work FIFO
- 128 deep Output Status FIFO
- 384-bit Pipe Control Register (PCR) to enable/disable individual hash engine
- Low I/O bandwidth requirement
  - New work (384 bits) every $2^{32}$ clock cycles per engine
• Two rounds of SHA-256 processing
• Searches for a result in $2^{32}$ nonce range
• Each round consists of 64 iterations
• Fully unrolled iterations
• Two parallel but connected pipelines – message & compressor
• Generates a result out only if target criteria met
COMPRESSOR STAGE OF SHA2-256 PIPELINE

\[ \Sigma_0(A) = (A \gg s_1) \oplus (A \gg s_2) \oplus (A \gg s_3) \]

\[ \Sigma_1(E) = (E \gg s_4) \oplus (E \gg s_5) \oplus (E \gg s_6) \]

\[ \text{Ch}(E,F,G) = (E \land F) \oplus (\neg E \land G) \]

\[ \text{Maj}(A,B,C) = (A \land B) \oplus (B \land C) \oplus (C \land A) \]

All registers are 32-bits wide
• 512 bits message word divided into 16 words, 32-bit wide (W₀ to W₁₅)

• \( \sigma_0(W_{1,\text{in}}) = (W_{1,\text{in}} \gg s_7) \oplus (W_{1,\text{in}} \gg s_8) \oplus (W_{1,\text{in}} \gg s_9) \)

• \( \sigma_1(W_{14,\text{in}}) = (W_{14,\text{in}} \gg s_{10}) \oplus (W_{14,\text{in}} \gg s_{11}) \oplus (W_{14,\text{in}} \gg s_{12}) \)
• Global Foundries HKMG 28nm HPP process
• 9 metal layers
• 120 hash engines in 11x11 array (grey boxes)
• Top level logic block in the center
GOLDSTRIKE™-1 (GS1) PACKAGE

- 37.5 x 37.5 mm FCBGA package
- 4 bare dies per package
- 1296 pins
- > 500 GH/s @ 1.05GHz & 0.7v
DEVELOPMENT TIMELINE

- 4 months from RTL start to tape out!
- Packaged silicon arrived on Dec. 28, 2013
- First system shipped to customer around mid January, 2014
ASIC DESIGN CHALLENGES & CHOICES

Challenges:
• High power density and high node toggle rates
  • Power delivery
  • Heat dissipation
  • IR drop and di/dt noise
• Very high sequential cell count
• Reduce die area and power consumption
• Very short (4-month) schedule from RTL start to tape out
• Very small design team

Choices:
• Optimize common core blocks
• Maximize design repeat & reuse
• Utilize highly experienced design team
HEAT DISSIPATION CHALLENGE

- **Cooling options examined:**
  - Heat sink + Airflow ← Common in CPU applications
  - Liquid Cooling ← Popular among over-clockers
  - Immersion ← Efficient for data centers
- **Liquid cooling with direct attach cooling head selected**
  - Enable a common platform for both home & data center customers

Air Temps on Plane 3mm above PCB Top
TERRAMINER APPLIANCE

Up to 2TH/s hash rate per appliance
- Dual PCB with 4 GS1 packages total
- Power budget to meet household outlet capacity

Layout - 4U chassis Design
- Driven by cooling requirements
  - Radiator cross-section
  - Fan Size
- Similar design for TerraMiner IV data center and home models
- Push pull airflow design for maximum performance
- Fans chosen for balance between cost, performance & audible noise
- Dual 1U power supplies for minimal volume impact
TERRAMINER APPLIANCE IMAGES
CONCLUDING REMARKS

• Continued demand for higher performance and lower power appliance
• Maintain Cointerra’s leadership position in Bitcoin mining industry
  • New designs with increased power efficiency and performance