

# Cryptocurrency ASICs

David Vorick

# Background

- + Cryptocurrency Enthusiast Since 2011
- + Sia Lead Developer
  - + Decentralized Cloud Storage Cryptocurrency
- + Obelisk CEO
  - + Cryptocurrency ASIC miner manufacturing company

# Presentation Format

- + Firehose of broad topics
- + Longer Q&A at the end

# Foundries

- + Foundries are companies capable of making semiconductor chips
- + Fabrication plants, or “fabs” are facilities capable of making semiconductor chips
- + There just a few dozen foundries in the world

# Processes

- + A “process” is a method for making semiconductor chips.
- + Usually processes have a nanometer associated with them
- + The nanometers of a process is less a description of the process and more a marketing term to tell you what “level” the process is. For example, 7nm processes have feature sizes that are ~40 nanometers in size.

# Cryptocurrency Processes

- + The processes relevant to cryptocurrency are TSMC 16nm, TSMC 7nm, and Samsung 14nm
- + Samsung is working on a 7nm, it's not ready yet
- + Other foundries really aren't competitive
- + There are other processes, like "TSMC 12nm" which are really more "TSMC 16nm but slightly improved"

# Chip Design

- + Foundries generally do not design chips, chips are instead designed by chip design houses
- + There are two major methodologies for design: digital and analog

# Digital Design

- + Most chips today are digital chips. Most CPUs, GPUs, AI and ML chips.
- + Digital designers work with gates and cells. They use base components like 'xor' and 'full-adder' and compose those into more full circuits
- + The base components are then compiled together using “place and route” tools which translate these designs into physical chip layouts.



# Digital Advantages

- + Digital design flows are very agile.
- + Complex chips can be designed in one to two years, and simple chips can be designed in periods of just a few months
- + Most chips today are very complex, and are only possible using digital design.

# Analog Design

- + Analog design works less with 'gates' and more with the physical features of the chips. Analog designers think about things like fins and planes and substrates.
- + Analog design can be very heavily optimized
- + Simple chip designs can take analog designers 6 to 12 months to complete
- + Complex designs are not really possible with analog methodologies

# Cryptocurrency Designs

- + Most “ASIC friendly” chips are created using analog design methodologies. Competitive sha256 chips are analog.
- + Most “ASIC resistant” chips are more complex, and have to be created using digital design methodologies

# Algorithmic Optimization

- + In typical chip design, algorithmic optimization is a big part of the competitive advantage.
- + An example of an algorithmic optimization would be early termination in sha256d chips - sha256d is 128 rounds, but you know if there are >32 leading zeroes after ~121 rounds
- + Software developers are capable of finding algorithmic optimizations

# Circuit Optimization

- + Circuit optimization is making decisions on actual circuit structure.
- + For example, there are probably 20 different common methods to add 2 numbers together
- + Each method has different tradeoffs in terms of speed, power, and size.
- + Knowing what adder to use for your design is a circuit optimization

# Place and Route Optimization

- + Once you have your choice of circuit, you have to figure out how to place the circuit onto the physical chip, and how to route all of the gates together
- + There are tools to do this for you. While they are occasionally better than humans, typically a human will find a more optimal routing path for the gates.

# Standard Cells

- + Generally designers will work with a set of ‘standard cells’ from the foundry
- + Standard cells might be, for example, a half-adder, which has 2 inputs, and 2 outputs
- + The foundry will have temperatures, voltages, and conditions where the cell is “qualified” to operate

# Cell Timings

- + The foundry will provide timing and power ratings for cells.
- + Timing requirements and power ratings change depending on the inputs. A '10' input will have different power and timing from a '01' input.
- + Timing requirements might be something like 'if the second input is a '1', then the first output will be ready 15 picoseconds after the second input arrives. Second output ready in 20 picoseconds.



# Cell Optimization

- + If you know that you need cells at an exotic voltage, or if you know that you have unique timing requirements, or if you know that you have unique power requirements, you can make your own cells.
- + Making a cell is very difficult, and generally requires heavy simulation and for heavy optimization requires prototyping.

# “Tape Out”

- + When a chip design is completed, it is finalized into a ‘GDS’ image which gets sent to the foundry
- + The foundry can use this image to create “masks”, which can then be used to manufacture chips
- + A set of masks typically costs several million dollars to manufacture.

# Turnaround Times - “TAT”

- + The turnaround time is very important to cryptocurrency chips. This is how long it takes to go from tape-out to a fully functional chip.
- + For 16nm, a typical turnound time is 75-100 days, depending on a number of factors

# Whole Process

- + For simple digital chips, design from scratch can be as little as 2 months. If you are just making a tweak on an existing design, it can be as little as 2 weeks.
- + Tape-out on a competitive node costs \$3-5 million, and you get chips back within 3 months
- + In total, a streamlined team can get simple chips to market within about 6 months, while more advanced chips can take over a year.

# The Other Stuff

- + Bitmain's S15 chip has an efficiency of about 42j / TH
- + Bitmain's S15 rig has an efficiency of about 57j / TH
  
- + A traditional approach to building an S15 might cost \$5,000 per machine to manufacture
- + Bitmain's S15 probably costs closer to \$1200 to manufacture

# More Topics

- + Chip power and speed simulations
- + Predatory manufacturer tactics
- + Selective Hardforks
- + North America vs. China manufacturing
- + General parts sourcing and lead times

# Questions?

I left out a great many details.