# Digital ASIC Fabrication

● ● ●

Team Members: Dawood Ghauri, Constantine Mantas, Soma Szabo, Courtney Violett

Client: Dr. Henry Duwe

Problem Statement

- Develop Iowa State's pedagogical framework on how to fabricate digital ASICs through the eFabless Open MPW Shuttle program

- Create a bring-up plan for chip fabrications
  - Design a SHA1 hashing accelerator for the MPW shuttle submission
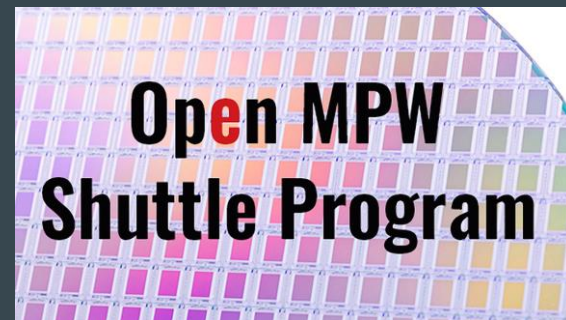
Source: [5]

Project & User Contexts

- Dr. Duwe demonstrating that a student led team can go from ideation to fabrication on an ASIC design
- Future students following our path to design their own ASICs in the future
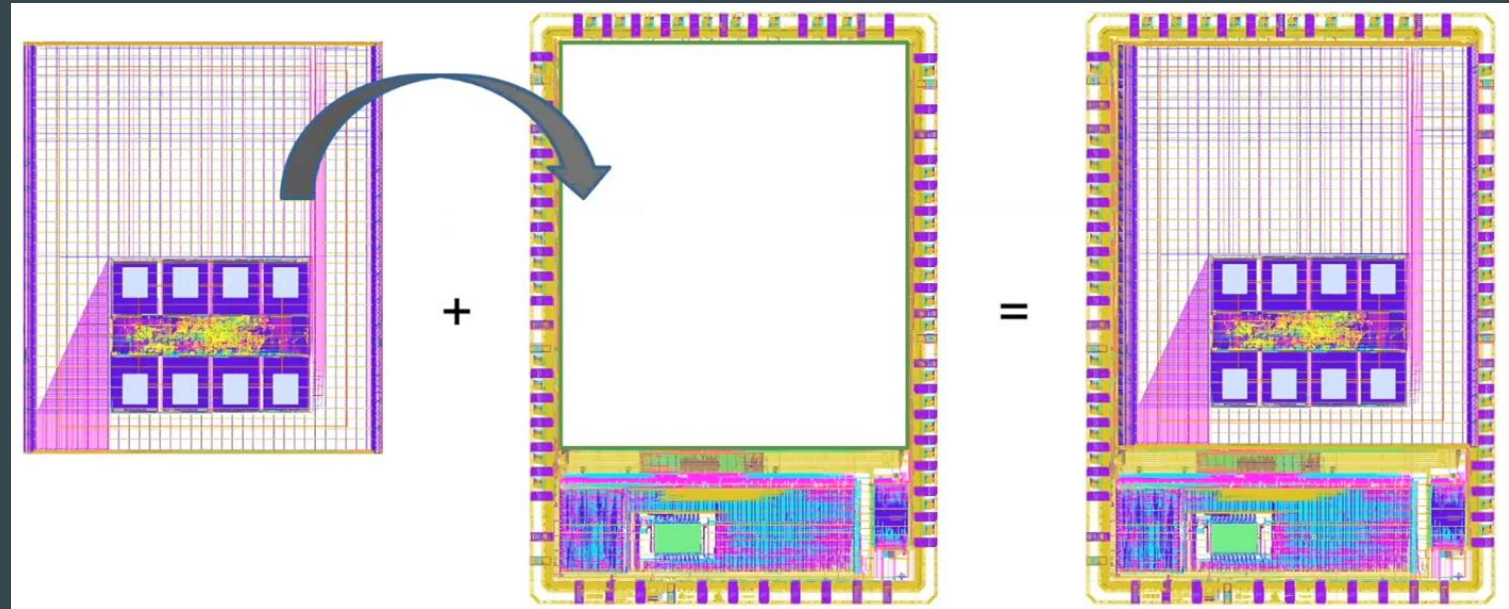

Source: [6]

Open MPW

- Efabless' solution for transforming HDL submissions into physical chips
  - No cost to us!
- Sponsored by Google.
- Manufactured by Skywater.
- Based on Open Source technologies.
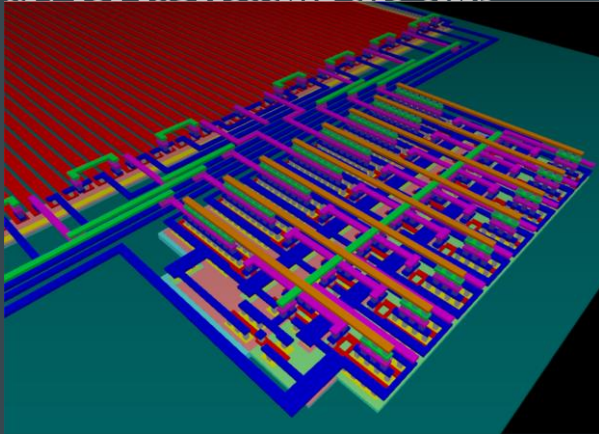- Open MPW 7 is our shuttle for design submission and closed on Sept. 12th

Source: [5]

Process to Final Product

Hardened user design   +   Integration with caravel harness   =   Submittable final design
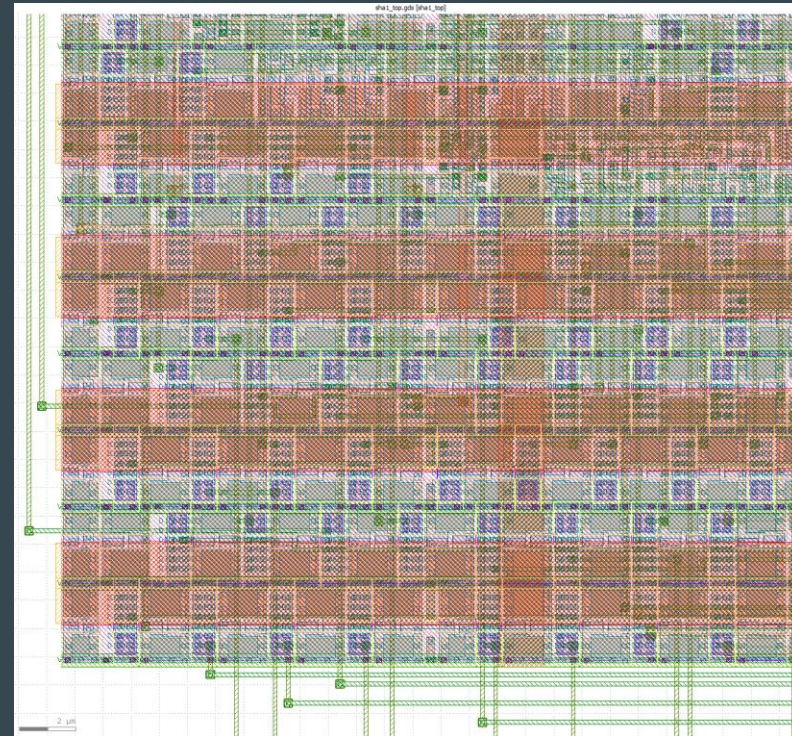
Hardening

SHA1 hardened design (GDSII file)

- OpenLANE

- Hardening turns HDL (Verilog) into a GDSII file.

- Necessary for fabricating the chip
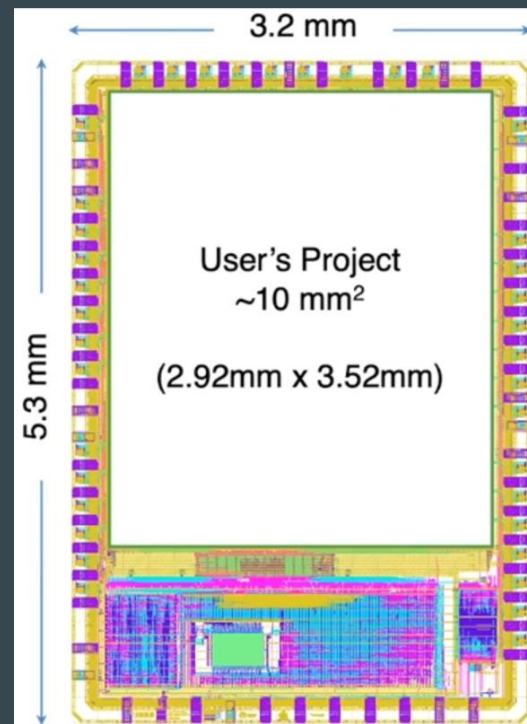

Source: [7]

Caravel Harness

- Physical frame with built in hardware and interfaces for the User Project

  - Local environment enables digital simulations

- User Project must be implemented within a Verilog HDL wrapper and undergo hardening to be integrated into the harness

3.2 mm

5.3 mm

User's Project
~10 mm²

(2.92mm x 3.52mm)

Source: [5]

Submission to eFabless

- Create a project on the efabless website.

- Execute precheck verification tool on our project's workspace.

- Download the export compliance form and complete and submit via the request.

- Review and complete our MPW service agreement.

- Review deliverables of our MPW request and select 'Submitter Confirmed' when complete.

Source: [5]

Functional Requirements

- Design passes MPW precheck and tapeout

- RTL and GL chip simulation testbenches pass

- Design functions as a hardware accelerated SHA1 hasher (modified from Bitcoin miner)

Source: [5]

Non-Functional Requirements

- Simulate unit tests in the caravel simulation environment

- Design is able to harden through OpenLane

- Design fits physically inside the User Project after hardening

- Power/timing constraints are met after hardening design

- Any IP we choose to bring in has no security risks
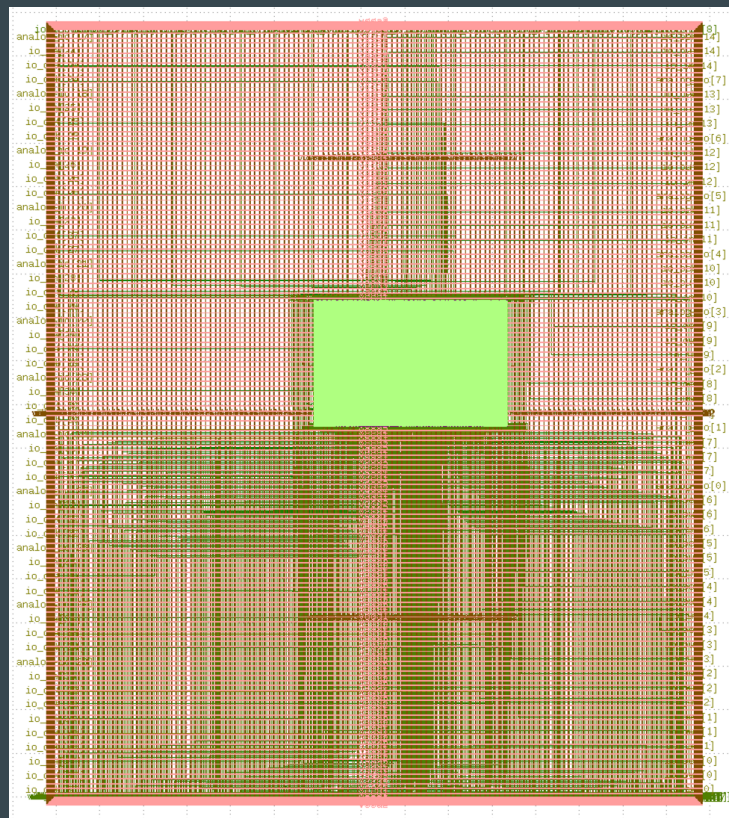
SHA-1 accelerator in User Project Area

Precheck (Requirements)

- Open Github Repository
- Checks:
  - LICENSE & README
  - YAML file
  - Consistency Checks (Logical Data Propagation)
  - DRC (Design Rule Checking) & LVS (Layout vs. Schematic) checks on the user project
  - XOR check
  - Chip passes RTL (register transfer language) and GL (gate level) simulations

  - Gate-level netlist (textual description of components) & hardened user project wrapper successfully generated

- Local precheck

  - Fast and readily available method

- Efabless website precheck
 - The official submission precheck which is much slower and more detailed

```
{{STEP UPDATE}} Executing Check 12 of 13: Klayout Pin Label Purposes Overlapping Drawing
No DRC Violations found
{{Klayout Pin Label Purposes Overlapping Drawing CHECK PASSED}} The GDS file, user_project_wrapper.gds, has no DRC violations.
{{STEP UPDATE}} Executing Check 13 of 13: Klayout ZeroArea
No DRC Violations found
{{Klayout ZeroArea CHECK PASSED}} The GDS file, user_project_wrapper.gds, has no DRC violations.
{{FINISH}} Executing Finished, the full log 'precheck.log' can be found in '/home/somasz/Documents/github/bitcoin_asic/precheck_
results/02_DEC_2022___05_55_50/logs'
{{SUCCESS}} All Checks Passed !!!
```
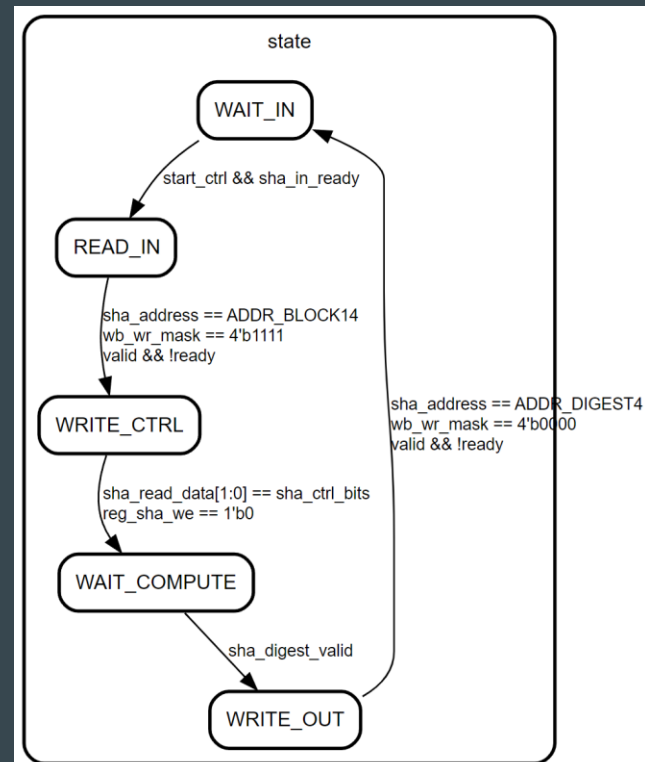
Initial Design

- Make mining process more efficient using an ASIC
- Hardware specializes in:
  - Computing as many digests as fast as possible
  - Pass block header through SHA-256 module
  - Digest shall be less than the target to create a new valid block
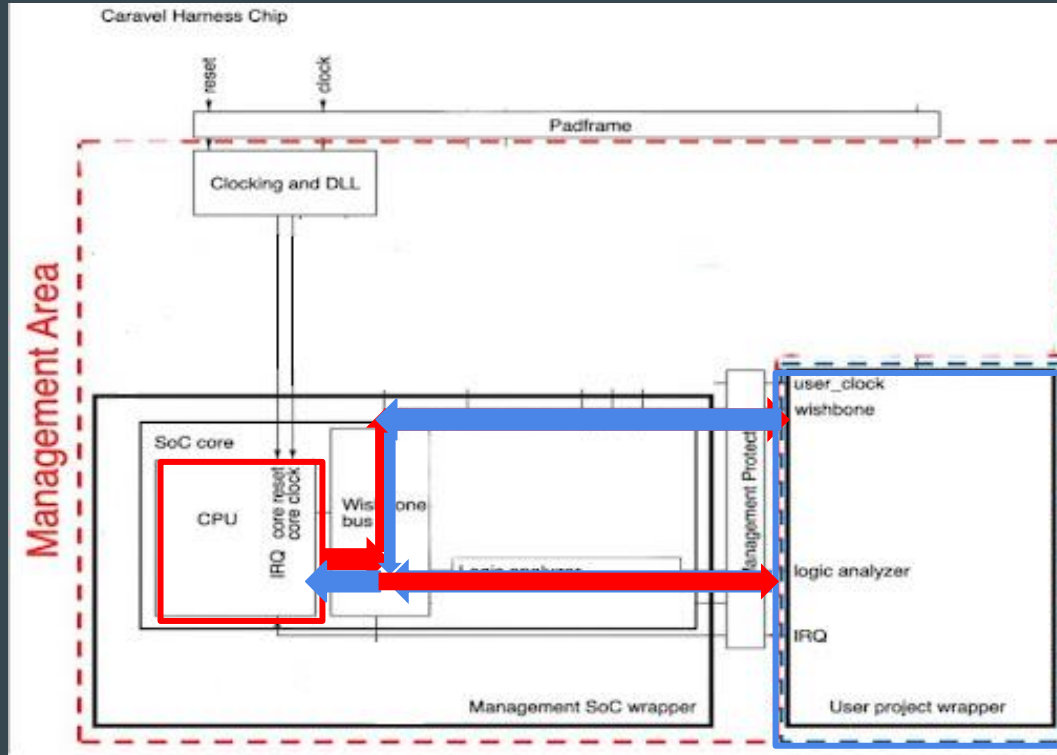

Source: Adapted from [5]
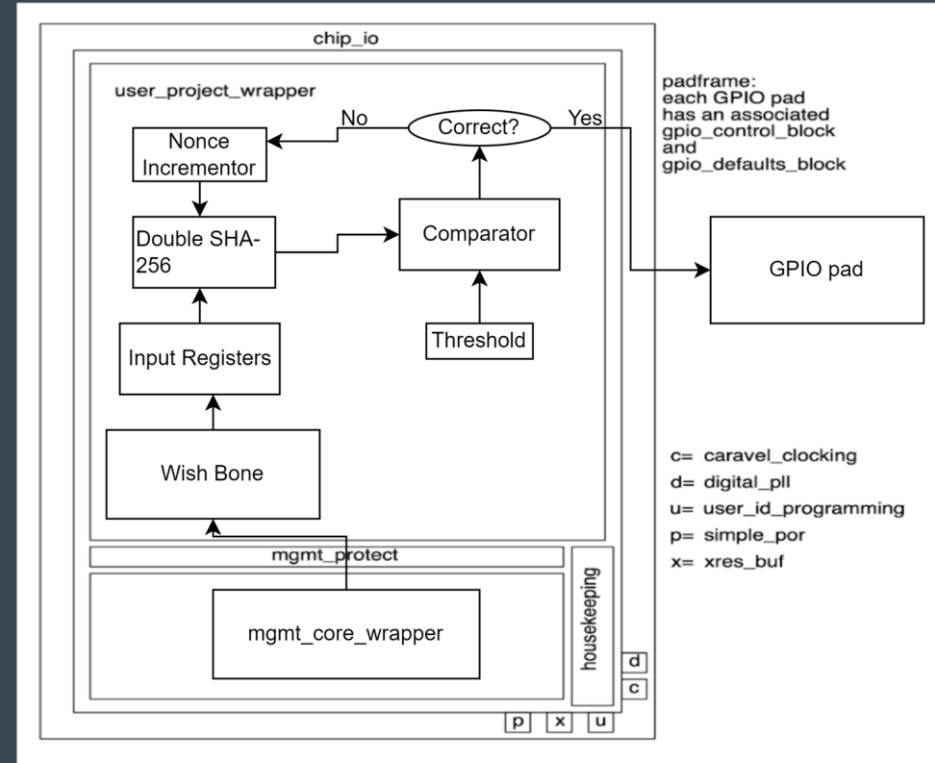
Final Design

- Due to MPW area constraints, Bitcoin miner unfeasible

- Hardware accelerator for SHA1

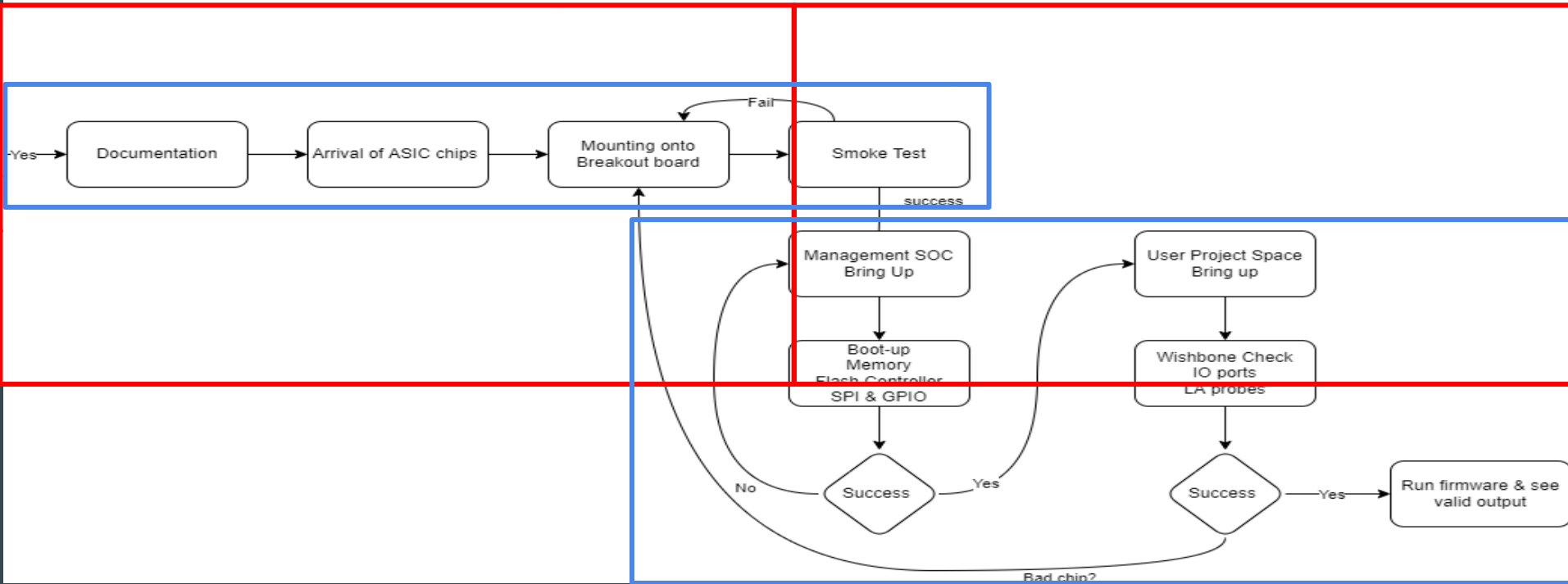- Firmware simulates a process similar to that of Bitcoin

Testing Our Design

- Tools:
  - Verilog test benches to test each individual unit
  - C test cases (firmware)
  - Probe signals using the logic analyzer (pre and post silicon)
  - OpenSSL for hardening
  - Efabless submission process for precheck and tapeout

Caravel Harness Testing Process

Digital Integration Testing/System Testing

- Critical Paths:
  - LA logic (muxing/selecting I/O)
  - SHA1 digest computation
- SHA1 I/O & controls are probed and tested using LA
  - Communication through wishbone (Rd/Wr data)
  - SHA1 controls, addresses, & status
- OpenLANE for hardened design

Bring up Plan

Unforeseen Changes in MPW 7 Shuttle

- September 12th was the original submission date which we met
  - We were originally expecting to receive the fabricated ASIC sometime in late November

- There were major errors found during the production process of the MPW 2 ASICS, so Efabless delayed the MPW 7 submission

- Now the submission date is December 5th, and the ASICs are expected to be fabricated sometime in early 2023

Our Current Status

- Fully designed and tested

- Our project has been submitted to the Open-MPW 7 shuttle
  - Passing Precheck
  - Passing Tapeout

- We are currently waiting for the shuttle to close and projects to be selected
  - If we do get selected, then the fabrication process will begin and our ASIC will be shipped to our client

Source: [5]

Citation

[1] M. Vilim, H. Duwe and R. Kumar, "Approximate bitcoin mining," 2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2016, pp. 1-6, doi: 10.1145/2897937.2897988.

[2] J. Kaur and L. Sood, "*Comparison Between Various Types of Adder Topologies,*" 2022 IJCST. Available: http://www.ijcst.com/vol61/1/13-Jasbir-Kaur.pdf. [Accessed: 26-Mar-2022].

[3] *H. L. Pham, T. H. Tran, T. D. Phan, V. T. Duong Le, D. K. Lam and Y. Nakashima, "Double SHA-256 Hardware Architecture With Compact Message Expander for Bitcoin Mining," in IEEE Access, vol. 8, pp. 139634-139646, 2020, doi: 10.1109/ACCESS.2020.3012581.*

[4] "Getting Started with Open MPW and chipIgnite" YouTube, uploaded by Efabless, 3rd of February 2022, https://www.youtube.com/watch?v=vJqP7ZR0NrI.

[5] "Efabless.com," eFabless. [Online]. Available: https://efabless.com/open_shuttle_program.

[6] Y. S. | J. 08, "Bitcoin data center construction marches on, despite low value," Data Center Knowledge | News and analysis for the data center industry, 08-Jun-2015. [Online]. Available: https://www.datacenterknowledge.com/archives/2015/06/08/bitcoin-hardware-firms-continue-building-data-centers-despite-low-currency-value.

[7] Cgracey, "PROP2 layout viewer," Parallax Forums, 26-Apr-2016. [Online]. Available: https://forums.parallax.com/discussion/164113/prop2-layout-viewer-try-it-out.

Thank You

...