付録 A
bitcoin_miner の性能

このペーパーは本文にて「FPGA で高速化」と言いながら、FPGA ボード（PYNQ-Z1）に実装した bitcoin_miner が他と比較してどれだけ速い（スループットが高い）か本文中に記載していないことに気づいて後付けで執筆したものです。これがないと画竜点睛を欠くですね。

なお、このペーパーについては PDF を筆者 Web サイト[*1]にて誰でも無償でダウンロードできるようにするつもりです。本文に入れられず、申し訳ないです。

A.1　FPGA / CPU / GPU / ASIC の性能比較

		FPGA	CPU	GPU	ASIC
性能 (スループット MHash/s)	絶対値	50.0	33.0	981.4	76719.6
	対 CPU 比	1.5	1.0	29.7	2324.4
消費電力（W）		2.5	52.6	225.0	7.2
消費電力あたり性能（MHash/J）	絶対値	19.8	0.6	4.4	10622.7
	対 CPU 比	31.6	1.0	7.0	16944.2

上の表は、FPGA ボード（PYNQ-Z1）実装した bitcoin_miner（FPGA)、CPU、GPU、ASIC の bitcoin マイニング処理性能値（スループット）と消費電力当たりの性能値の絶対値と CPU を 1 としたときの相対値を示したものです。FPGA は CPU より速く、また消費電力当たりの性能で考えれば GPU よりも速くマイニング処理ができていることが分かります。ASIC はけた違いですね。残念ながら勝負になりません。

表中の CPU、GPU、ASIC の具体的な製品名と それぞれの性能値・消費電力値の測定方法 または 引用元について次に示します。

FPGA　PYNQ-Z1 に実装した bitcoin_miner

PYNQ-Z1 に搭載されている FPGA は Xilinx の ZYNQ Z7020 です。bitcoin_miner は 1 クロック当たり 1 ハッシュを処理し 50MHz[*2]で動作するため、性能値は約 50MHash/s です。消費電力は Vivado の Power analysis 機能で見積もった On-Chip Power の値です。

[*1] https://d-rissoku.net/

[*2] タイミング解析でエラーとならないのが 50MHz。実際にはもっと高い周波数でも動かせると考えられます。

CPU　Intel Core i5-4670 (4Core・3.4GHz)
性能値は cpuminer-opt-3.8.8.1[*3]を当該 CPU を搭載した筆者の PC にて引数 -a sha256d –benchmark で実行した時の 4Core 分のハッシュレートの合計値です。CPU の消費電力は、性能測定中に Intel Power Gadget 3.5 で計測した値です。

GPU　NVIDIA GeForce GTX 1070
性能値は Bitcoin Forum[*4]に張られていた ASUS DUAL-GTX1070 での値を記載しています。消費電力値は当該製品のスペック上の最大消費電力を記載しています。

ASIC　Antminer S9i
Antminer S9i には 189 個の ASIC が搭載されており、スペック上の性能値は全体で 14.5THash/s です。表にはスペック上の性能値・消費電力値を 189 で割って ASIC 1 個当たりの値に換算したものを記載しています。

A.2　もっと高価な FPGA を使ったら・・・

本文中で「お小遣いの範囲で買える FPGA では・・・」という表現を利用し、実際にその範囲で購入できる FPGA ボード（PYNQ-Z1）に bitcoin_miner を実装したわけですが、もっと高価で高性能な FPGA を使った場合の性能を大雑把ですが試算してみました

ここではクラウドで高性能な FPGA が使えると話題となった Amazon EC2 F1 インスタンスで利用可能な Xilinx の Virtex UltraScale+ FPGA VU9P に実装した場合を考えます。なおこの FPGA 1 つを Digi-Key でばら買いする場合、本ペーパ執筆時点[*5]で価格は約 590 万円です。

まず高性能な FPGA にはたくさんの回路を詰め込むことができます。ここでは bitcoin_miner で特に消費が多い LUT の数で考えてみます。PYNQ-Z1 の FPGA Zynq-7020 への実装では、本文に記載した通り全部で 53,200 個ある LUT のうち 43,306 個を利用しました。VU9P には LUT が 1,182,000 個あるため、単純計算で 27 個の bitcoin_miner を VU9P に詰め込めます。

次に、高性能な FPGA は同じ回路をより高い周波数で動作させることができます。どれだけ高い周波数で動かせるかは、VU9P 向けの実装を行ってツールによるタイミング解析を行わないと具体的には分からないのですが、Xilinx の資料に Artix-7 と Virtex-7 の MicroBlaze の性能値が記載されたもの (番号:DS180）があるで、それから考えてみます。Zynq-7020 内の FPGA 部分には Artix-7 というシリーズの FPGA が用いられており、Virtex-7 は Virtex UltraScale+ より「前」のシリーズです。MicroBlaze はソフトプロセッサコアというユーザが作成した回路と同じような回路情報として Xilinx から提供される CPU のことです。そのため MicroBlaze の性能比較から Artix-7 と Virtex-7 に同じ回路を実装した時の性能差を想像でき、その値は DS180 によれば Artix-7 が 303 DMIPs、Virtex-7 が 441 DMIPs です。よって 1.4〜1.5 倍の周波数で動作できそうだということが分かります。

VU9U に 27 個の bitcoin_miner 実装し 50MHz の 1.5 倍の周波数で並列動作させれば性能は 2,025MHash/s です。金があれば FPGA で GPU(GTX 1070) に絶対性能でも勝てますね。

[*3] https://github.com/JayDDee/cpuminer-opt/releases
[*4] https://bitcointalk.org/index.php?topic=2054800.0
[*5] 2018/10/6