# HackRF
# A Low Cost Software Defined Radio Platform

## ToorCon 14

Michael Ossmann
Great Scott Gadgets

Jared Boone
ShareBrained Technology

The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

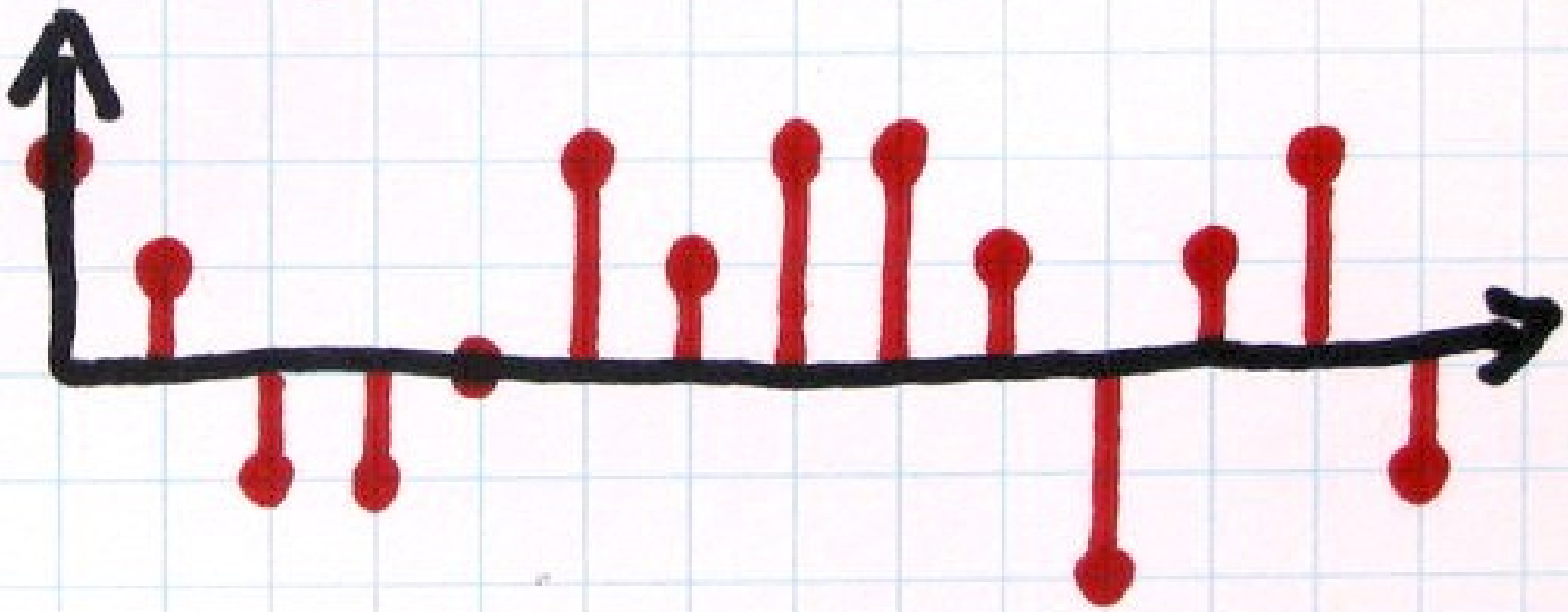
# Software Defined Radio (SDR)

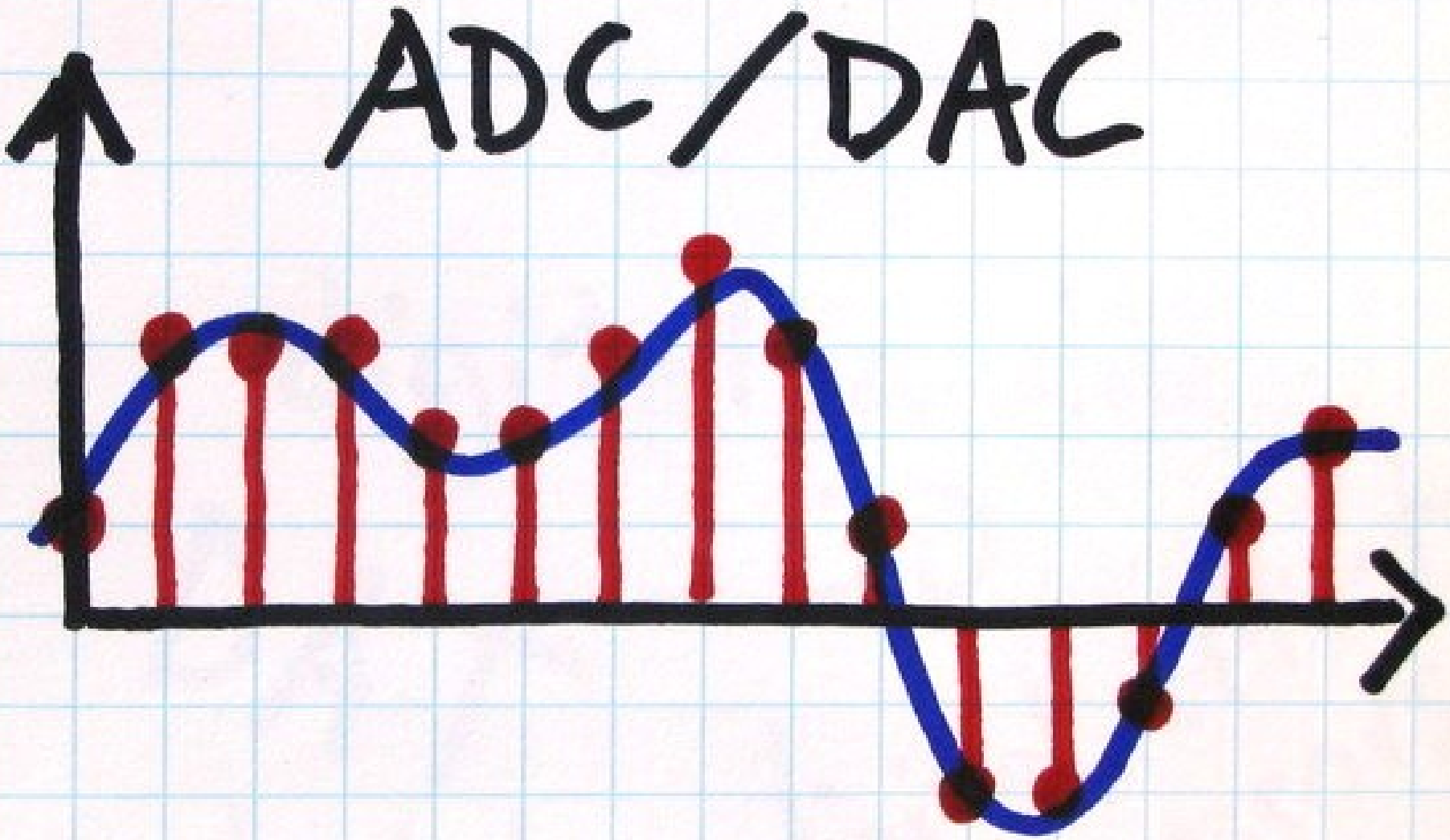
radio by

Digital Signal Processing (DSP)

# digital signals

just a sequence of values




ADC/DAC

# analog audio

vinyl records

tape

synths

Plain Old Telephone Service

# digital audio

DAT

CD

digital effects processors

digital phone switches

synths

hard disk recording

MP3

VoIP

explosion!

P2P

Napster

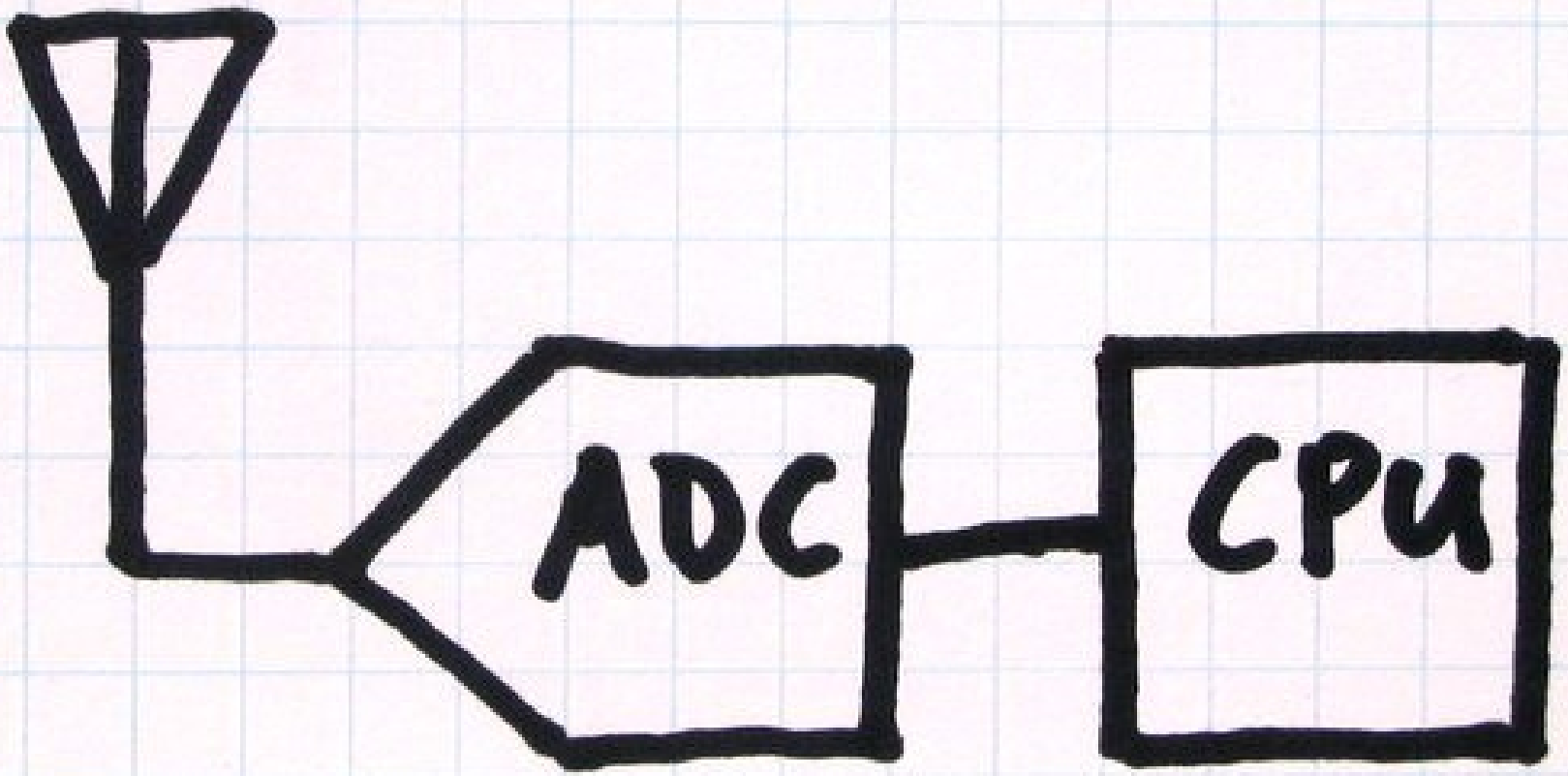
analog modling synths

Skype

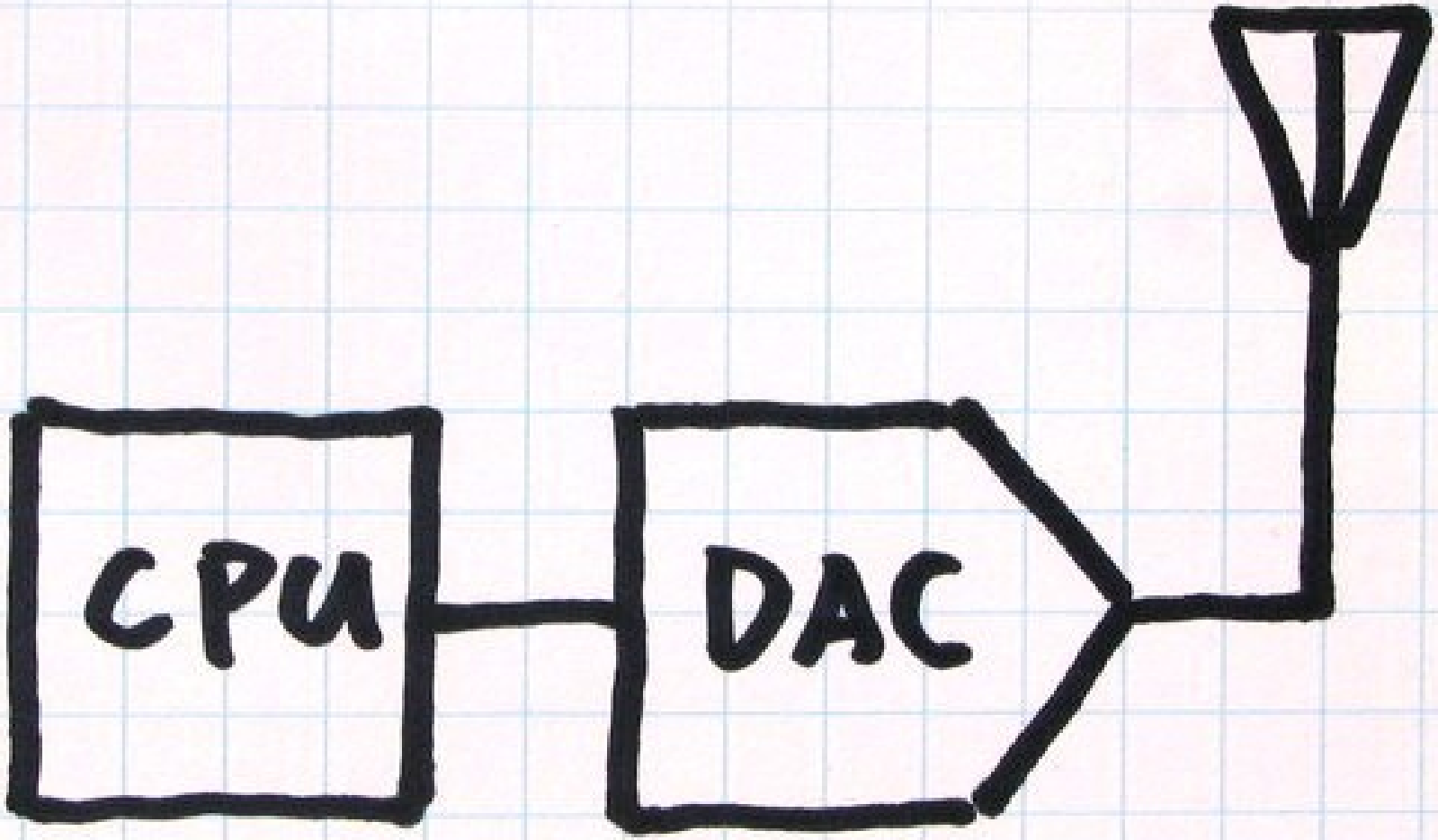
# software ~~digital~~ audio revolution

a
signal
is
a
signal

# ideal receiver



# ideal transmitter



# flexibility

many radios
in one

# reconfigurability

software modification

cost

high quality analog components

or

cheap analog components plus CPU

the future

all radios will be software radios

# the Wi-Fi lesson

what if?

# Information Security

SDR is a proven technology for wireless communication security

http://www.pixelhunt.com.au/2010/12/featured/funtime-friday-its-beginning-to-look-a-lot-like-christmas/attachment/empty-wallet/


Ettus
Research
USRP
Universal Software Radio Peripheral
CLK IN
ROBOTICON


http://michaelkonik.com/the-good-bad-and-ugly/tsa-agent/

# target operating frequencies

0 — 1 GHz: lots of stuff

1 - 2 GHz: DECT, GPS, GSM

2.4 GHz: 802.11, Bluetooth, ZigBee

5.9 GHz: DSRC, WAVE, 802.11

# target bandwidth

0–1 MHz: lots of stuff

1 MHz: Bluetooth

2 MHz: ZigBee, DECT

5 MHz: LTE

20 MHz: 802.11

receive
or
transmit?

# Portability

# Cost

Single device any laptop owner can afford

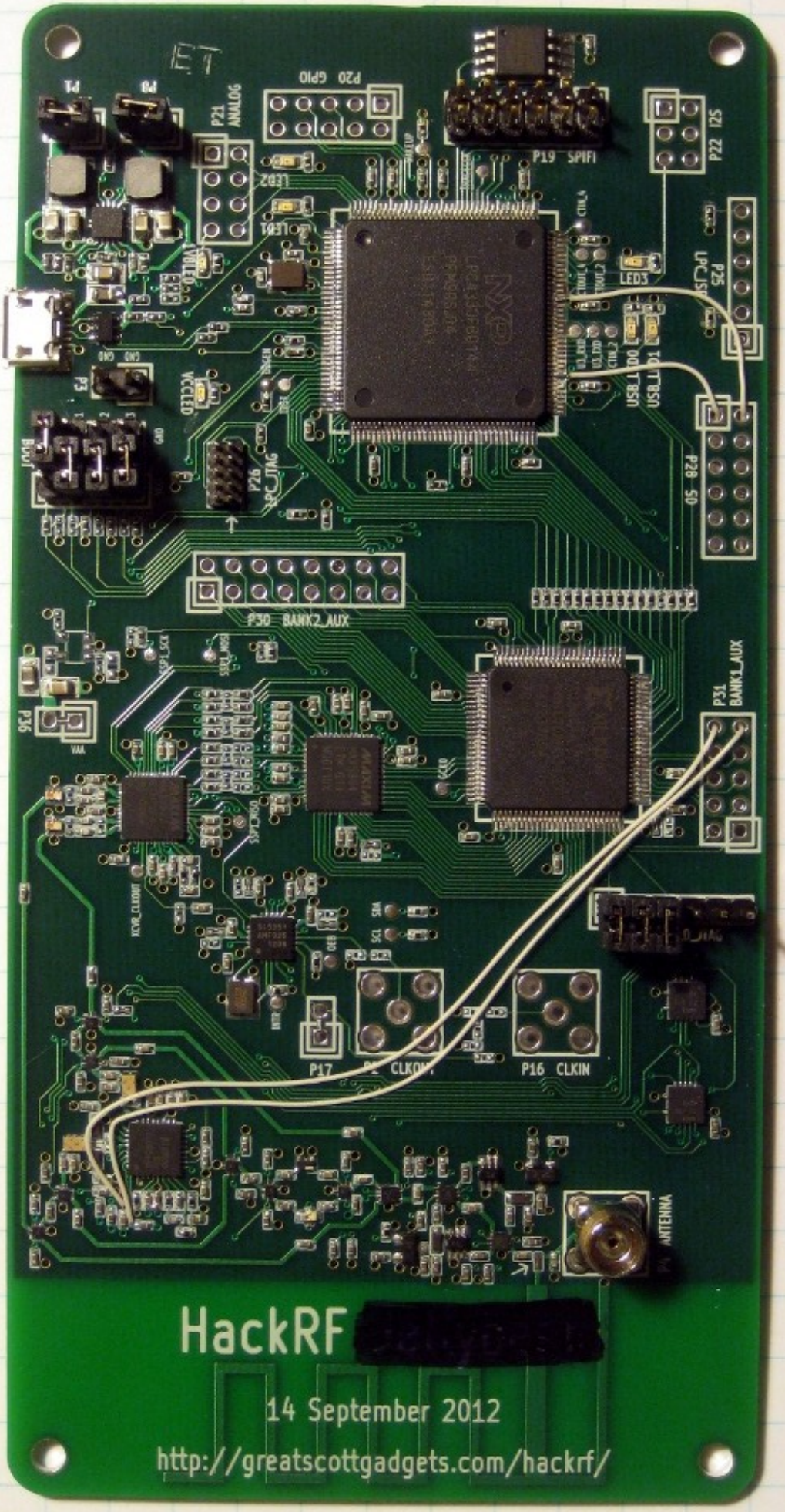
Open
Source

# We Can Live Without...

high dynamic range

DSP

full-duplex


P1
P8
P21 ANALOG
P20 GPIO
P19 SPIFI
P22 I2S
P25 LPC_USB
P28 SD
P30 BANK2_AUX
P31 BANK1_AUX
P26 LPC_JTAG
P36
P17
P16 CLKIN
ANTENNA
HackRF
14 September 2012
http://greatscottgadgets.com/hackrf/

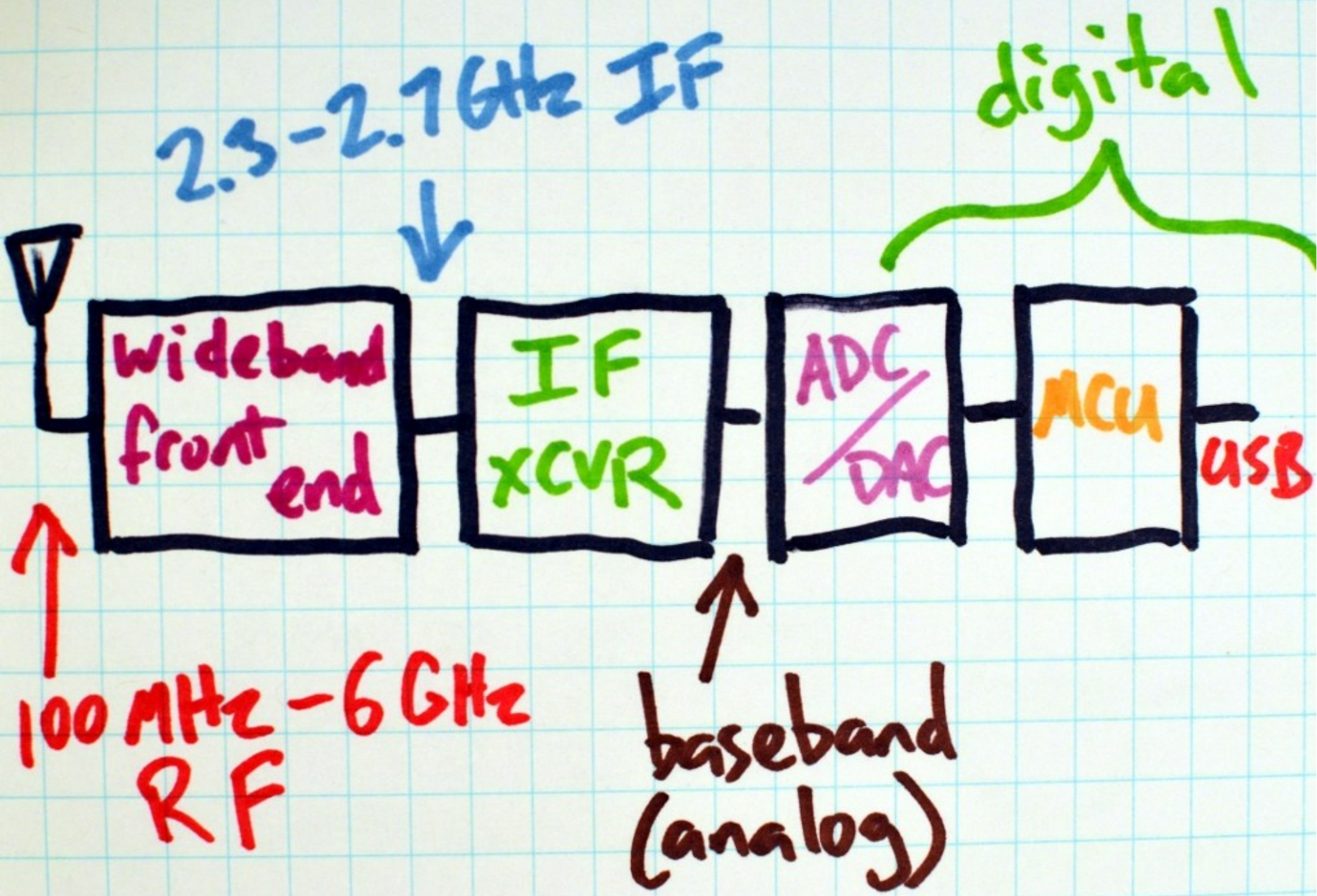
# Architecture

dual conversion

high IF

USB microcontroller

flexible clock generation


2.3-2.1GHz IF
digital
wideband front end
IF XCVR
ADC/DAC
MCU
USB
100 MHz-6 GHz RF
baseband (analog)

# Jawbreaker

High Speed USB 2.0

bus powered

30 - 6000 MHz operating frequency

half-duplex transceiver

15 - 20 MHz max bandwidth

900 MHz antenna or external

5.8" x 2.9"

open source hardware and software

# DARPA

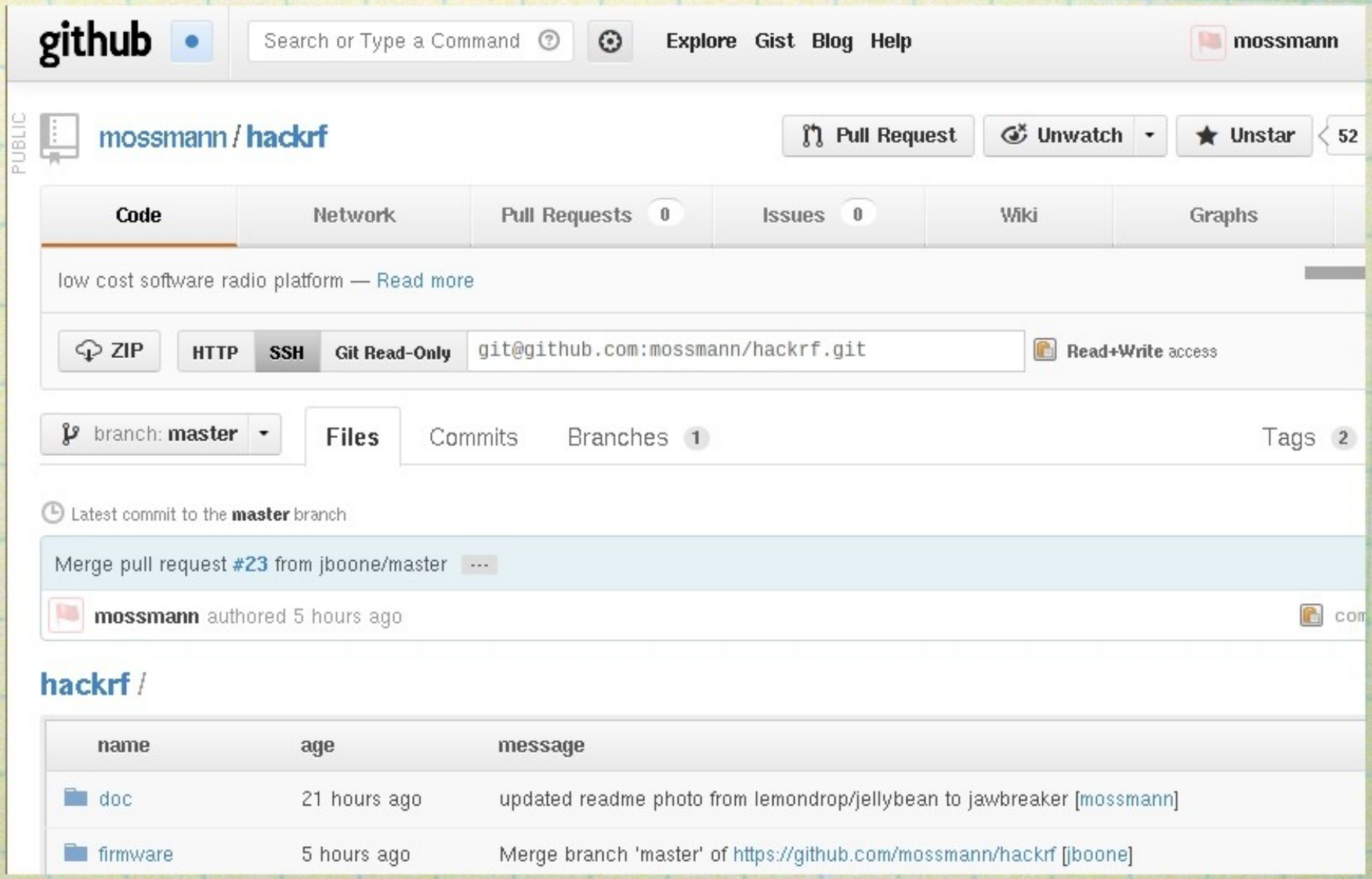
## Cyber Fast Track (CFT)

This is a big
project
for us.

This isn't a
big project
for DOD.

The world needs
open source hardware
for SDR.

# Public process



# Communication

```
mossmann@ardua: ~
http://greatscottgadgets.com/hackrf/
05:59 < sharebrained> But still, the SGPIO interrupt is going to chew a fair amount
                      of the CPU. Time to learn how to program the M0...
05:59 < mossmann> Yeah, DMA may still be helpful there.
05:59 < sharebrained> The M0 can be our DMA engine... :-)
06:00 < sharebrained> Helpful where?
06:00 < mossmann> potentially gaining a few cycles by having it move stuff while the
                  CPU is doing USB setup.
06:01 < mossmann> but I always figured the M0 would be near 100% busy just moving
                  samples around.
06:01 < sharebrained> Move what stuff, though? The SGPIO interrupt is dumping
                      samples straight into the USB buffer. So there's nothing more
                      that needs moving.
06:01 < mossmann> ah
06:02 < sharebrained> And unfortunately, the SGPIO shadow registers are not
                      contiguous or in order. So some smarts need to deinterleave
                      that junk.
06:02 < mossmann> I suggest sticking to the M4 for now.  We can migrate to the M0
                  once we actually have something else for the M4 to do.
06:02 < sharebrained> I think the overhead of asking the DMA to scatter-gather
                      individual 8-word sets with 8 single-word linked list
                      descriptors would be considerable.
06:03 < sharebrained> Yeah, I'm going to keep with the M4 for the next week+. Just
                      mentioning that the M0 might be able to do this work and hide
                      it away.
 [00:33] [mossmann(+Zi)] [3:freenode/#hackrf(+ns)] [Act: 4,5,8,9]
[#hackrf] []
```

Volunteers!

# tools

KiCad

GCC

# hardware design process

Michael
designer

Jared
consultant

modules

100%
NDA
free!

NXP LPC43xx

ARM Cortex-M4 + M0

204 MHz

High Speed USB

FPU

SGPIO

libopencm3

We are not...

we are...

HackRF beta

Thanks, DARPA!

# Thank you!

DARPA CFT

BIT Systems

Benjamin Vernoux

Will Code

David Hulton

ToorCon

http://greatscottgadgets.com/hackrf/