STEALING CHROMIUM: EMBEDDING HTML5 WITH THE SERVO BROWSER ENGINE

Lars Bergstrom
Mozilla Research

Mike Blumenkrantz
Samsung R&D America

Why a new web engine?

- Support new types of applications and new devices
- All modern browser engines (Safari, Firefox, Chrome) originally designed pre-2000
  - Coarse parallelism
  - Tightly coupled components
- Vast majority of security issues are related to the C++ memory model

Servo

- Written in a memory-safe systems language, Rust
- Architected for parallelism
  - Coarse (per-tab), as in Chrome
  - Lightweight (intra-page), too
- Designed for embedding

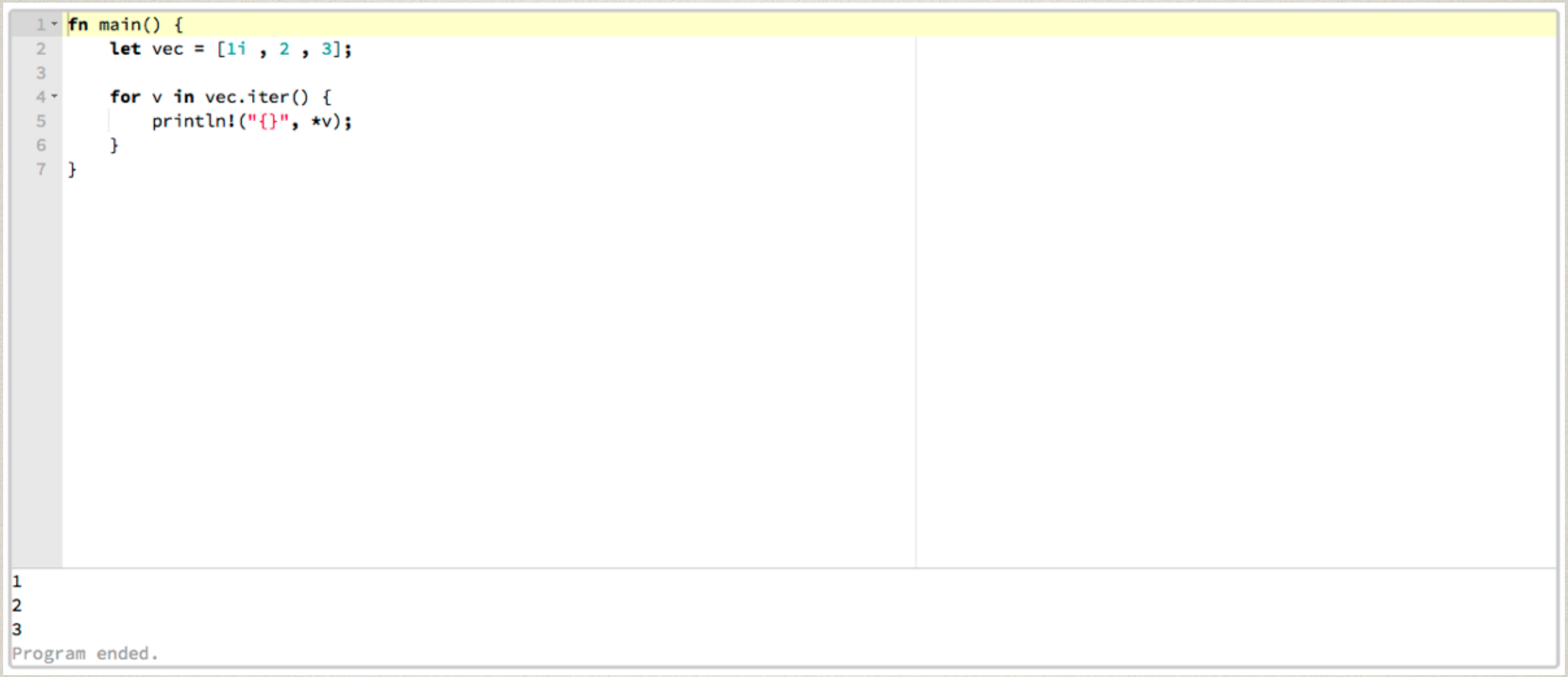
mozilla SAMSUNG

Rust - safe systems programming

- C++ syntax and idioms
- C++-like performance
- Memory safety
- Concurrency
- Parallelism

http://www.rust-lang.org

Familiar syntax and performance



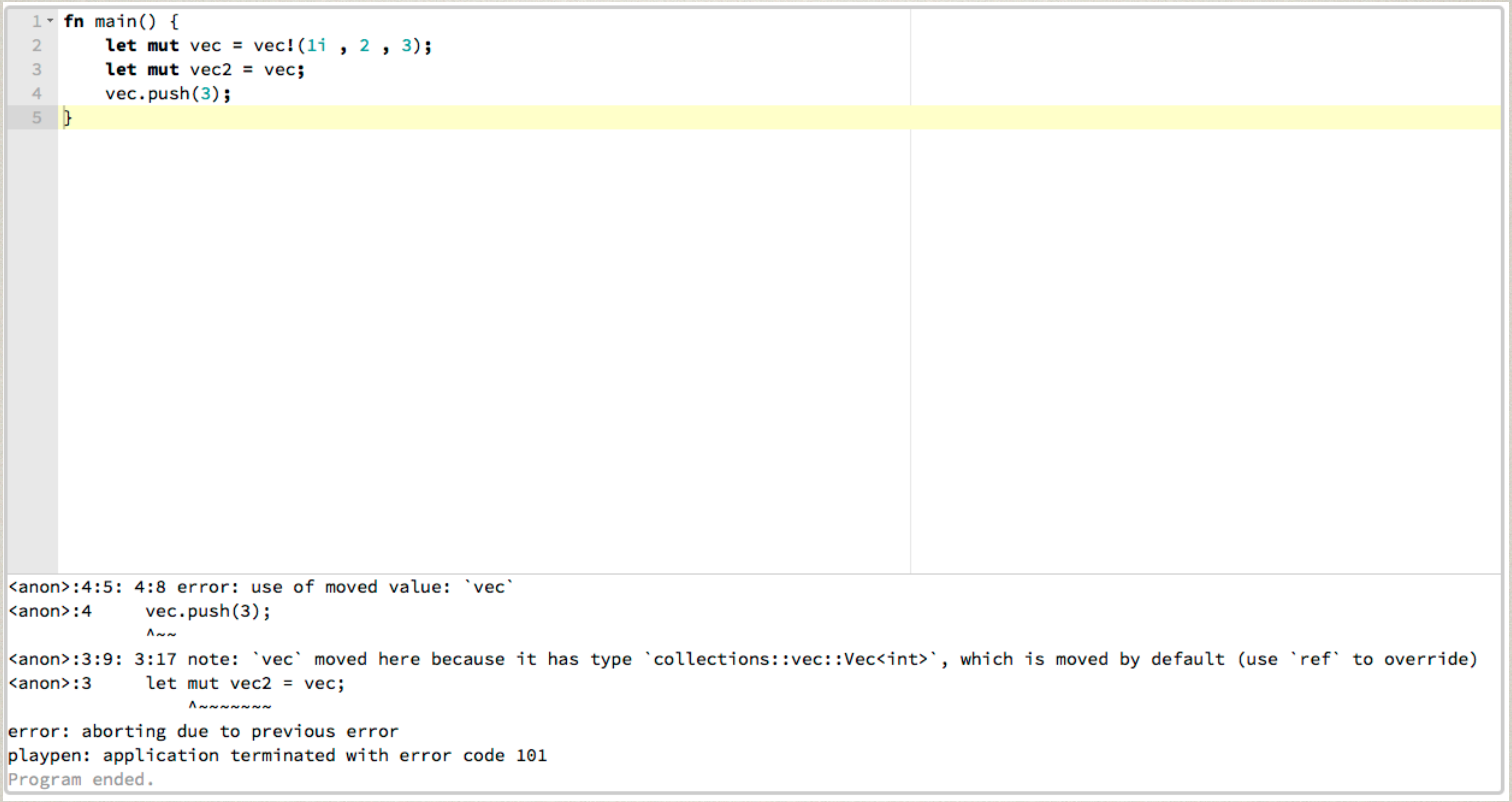
```
fn main() {
    let vec = [1i , 2 , 3];

    for v in vec.iter() {
        println!("{}", *v);
    }
}
```

```
1
2
3
Program ended.
```

Memory safety without overhead

- Lifetimes and ownership ensure memory safety
  - No garbage collection
  - No reference counting
  - No C++ “smart” pointer classes

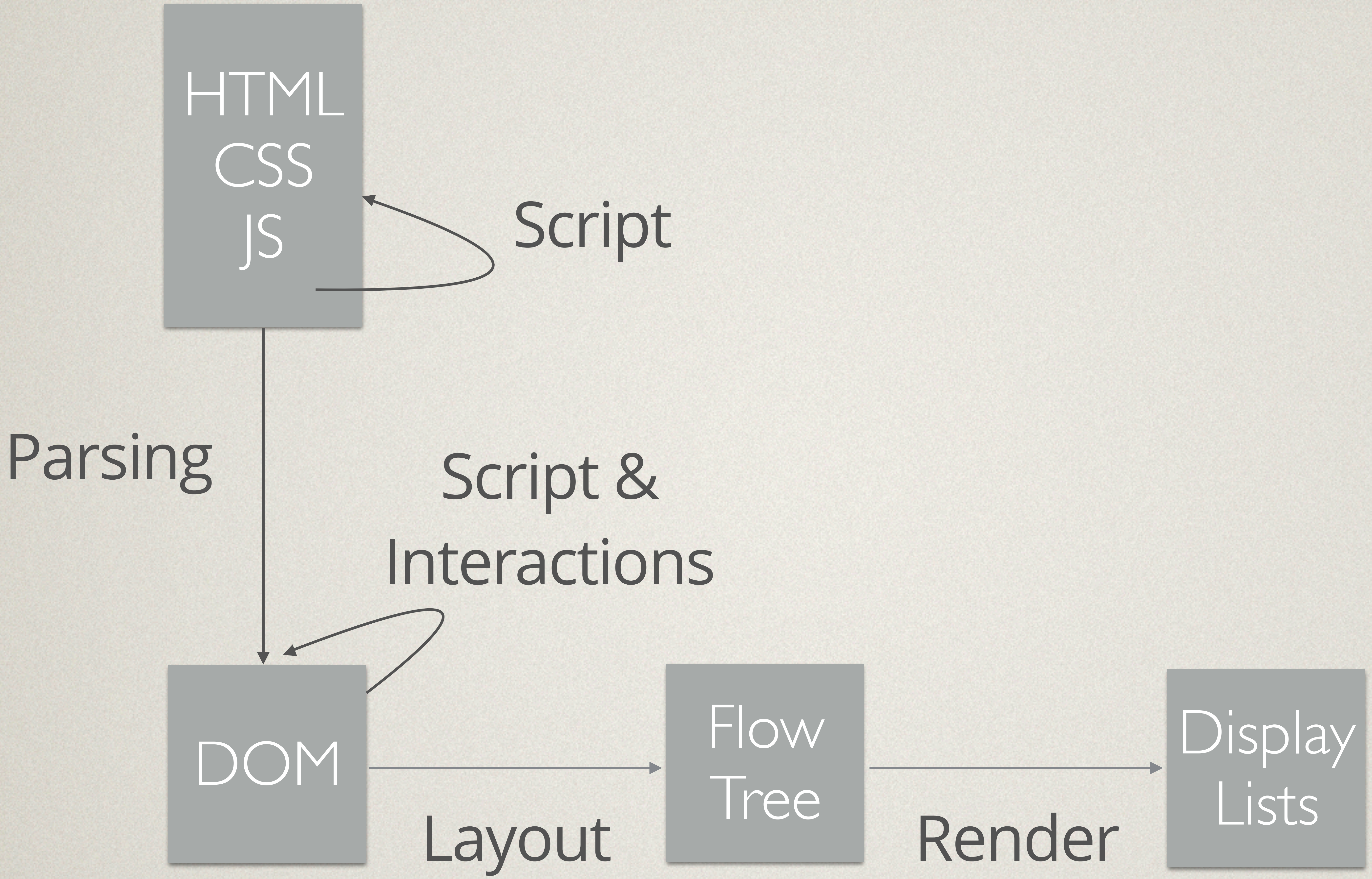
Example of code you can't write



```
fn main() {
    let mut vec = vec!(1i , 2 , 3);
    let mut vec2 = vec;
    vec.push(3);
}
```

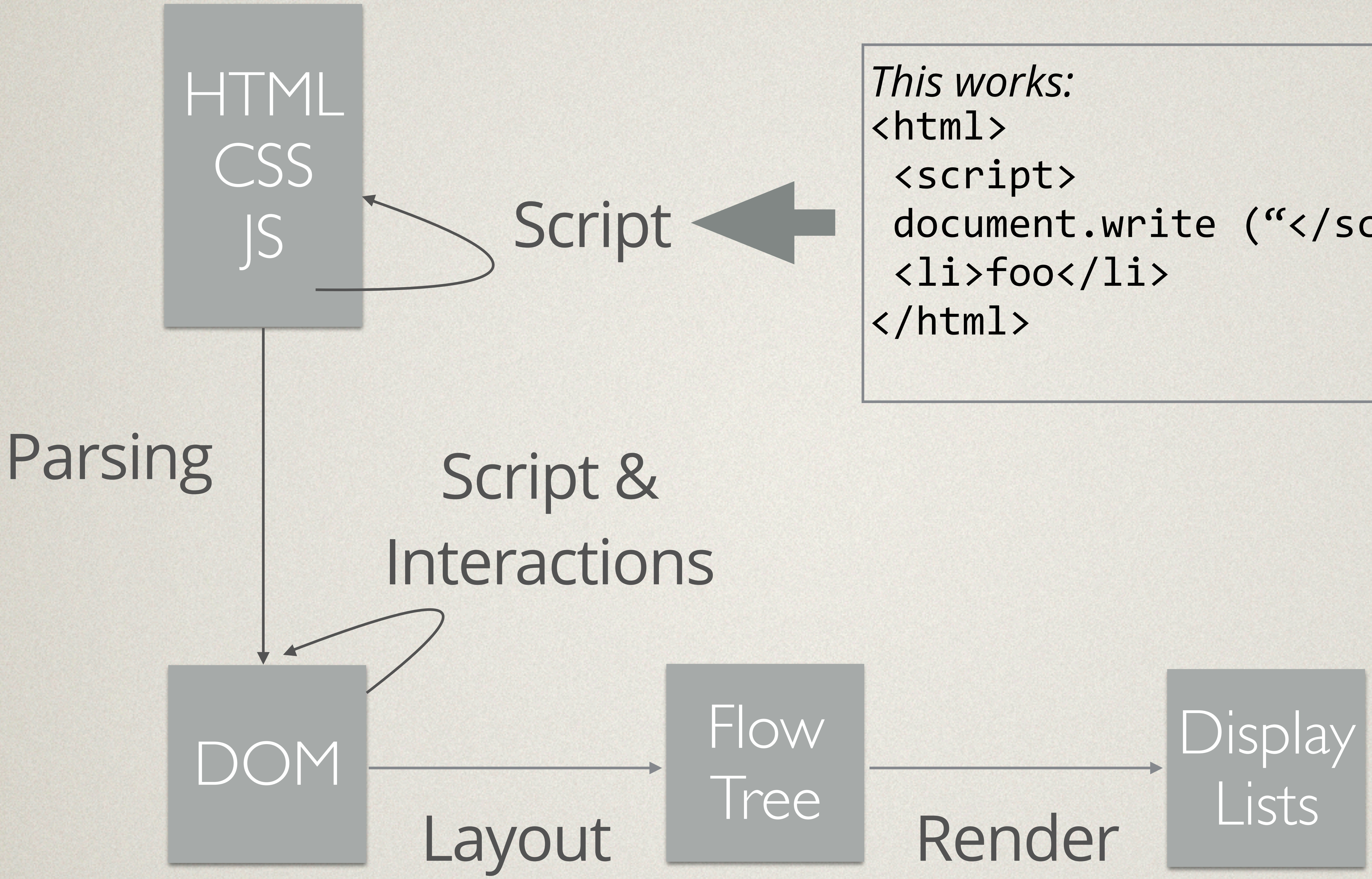
```
<anon>:4:5: 4:8 error: use of moved value: `vec`
<anon>:4     vec.push(3);
             ^~~
<anon>:3:9: 3:17 note: `vec` moved here because it has type `collections::vec::Vec<int>`, which is moved by default (use `ref` to override)
<anon>:3     let mut vec2 = vec;
                 ^~~~~~~~
error: aborting due to previous error
playpen: application terminated with error code 101
Program ended.
```

How a browser works



More details: http://www.html5rocks.com/en/tutorials/internals/howbrowserswork/

How a browser works



This works:

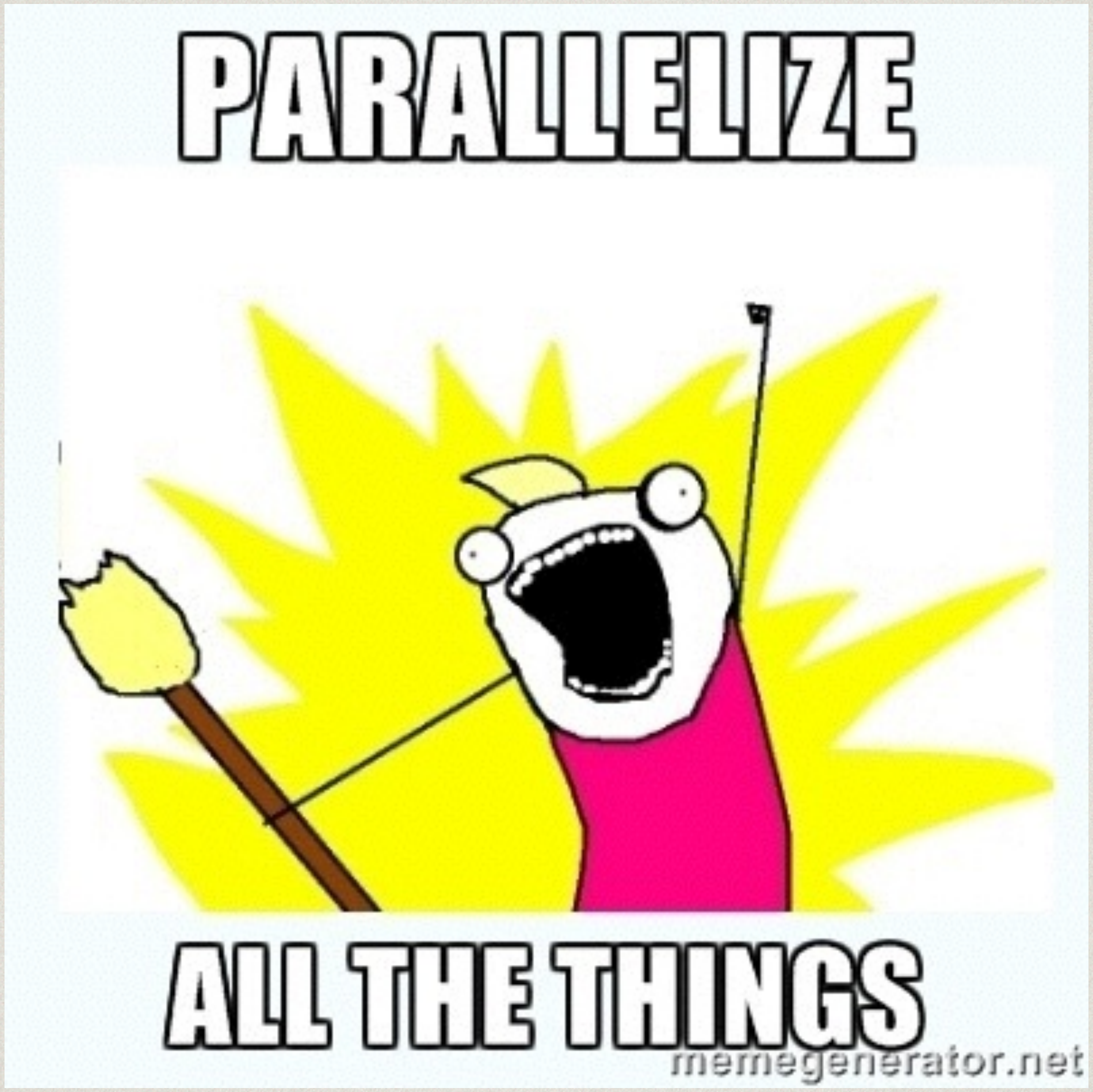
```
<html>
 <script>
 document.write (“</script>
 <li>foo</li>
</html>
```

More details: http://www.html5rocks.com/en/tutorials/internals/howbrowserswork/

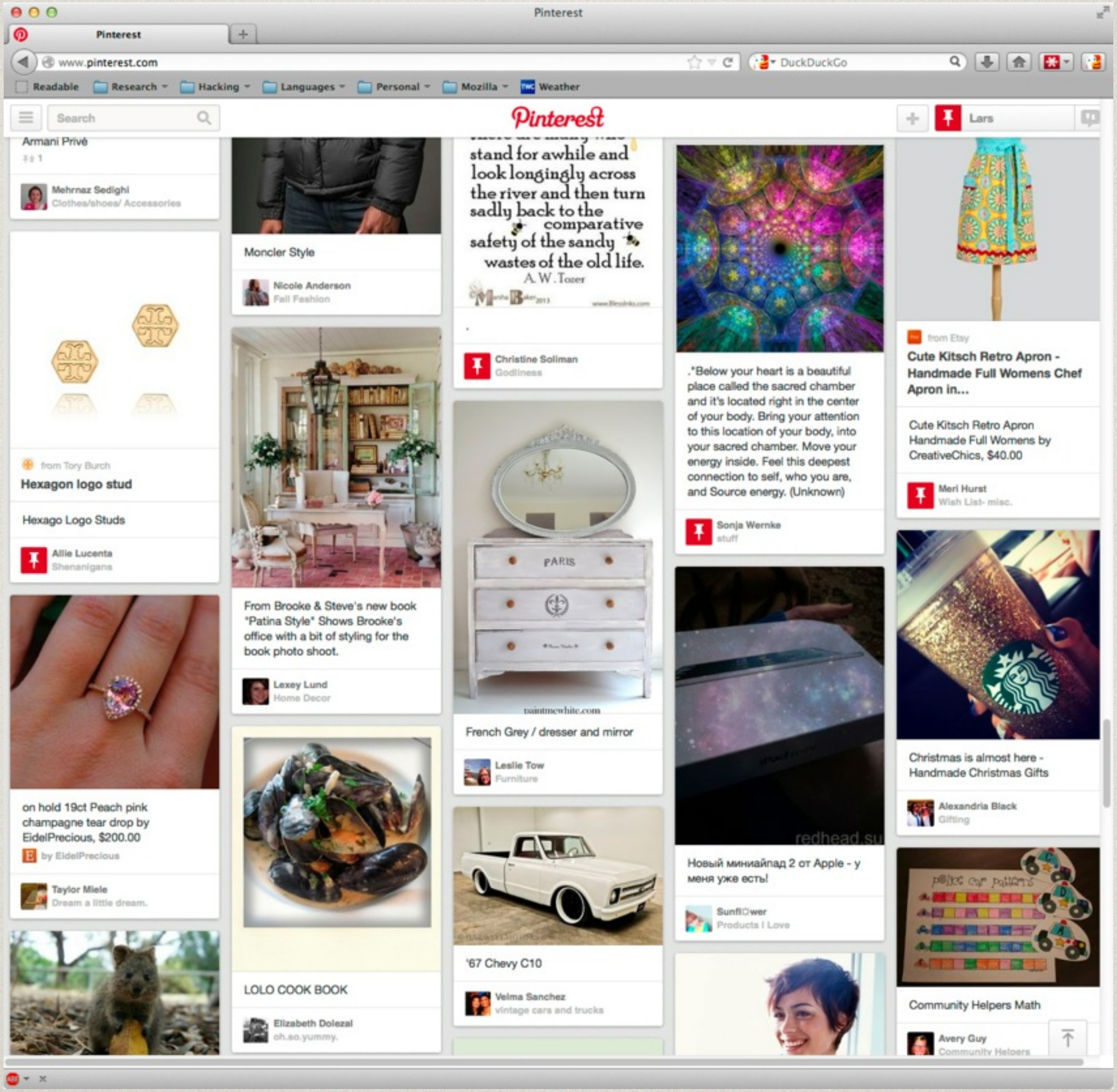
Timing breakdown

Task	Percentage
Runtime libraries	25%
Layout	22%
Windowing	17%
Script	16%
Painting to screen	10%
CSS styling	4%
Other	6%

Data from A Case for Parallelizing Web Pages. Mai, Tang, et. al. HOTPAR '12


PARALLELIZE
ALL THE THINGS
memegenerator.net

Websites already partitioned



Armani Privé
Mehrnaz Sedighi Clothes/shoes/ Accessories

from Tory Burch
Hexagon logo stud
Hexago Logo Studs
Allie Lucenta Shenanigans

on hold 19ct Peach pink champagne tear drop by EidelPrecious, $200.00
by EidelPrecious
Taylor Miele Dream a little dream.

Moncler Style
Nicole Anderson Fall Fashion

From Brooke & Steve's new book "Patina Style" Shows Brooke's office with a bit of styling for the book photo shoot.
Lexey Lund Home Decor

LOLO COOK BOOK
Elizabeth Dolezal oh.so.yummy.

stand for awhile and look longingly across the river and then turn sadly back to the comparative safety of the sandy wastes of the old life. A.W. Tozer

Christine Soliman Godliness

French Grey / dresser and mirror
Leslie Tow Furniture

'67 Chevy C10
Velma Sanchez vintage cars and trucks

."Below your heart is a beautiful place called the sacred chamber and it's located right in the center of your body. Bring your attention to this location of your body, into your sacred chamber. Move your energy inside. Feel this deepest connection to self, who you are, and Source energy. (Unknown)
Sonja Wernke stuff

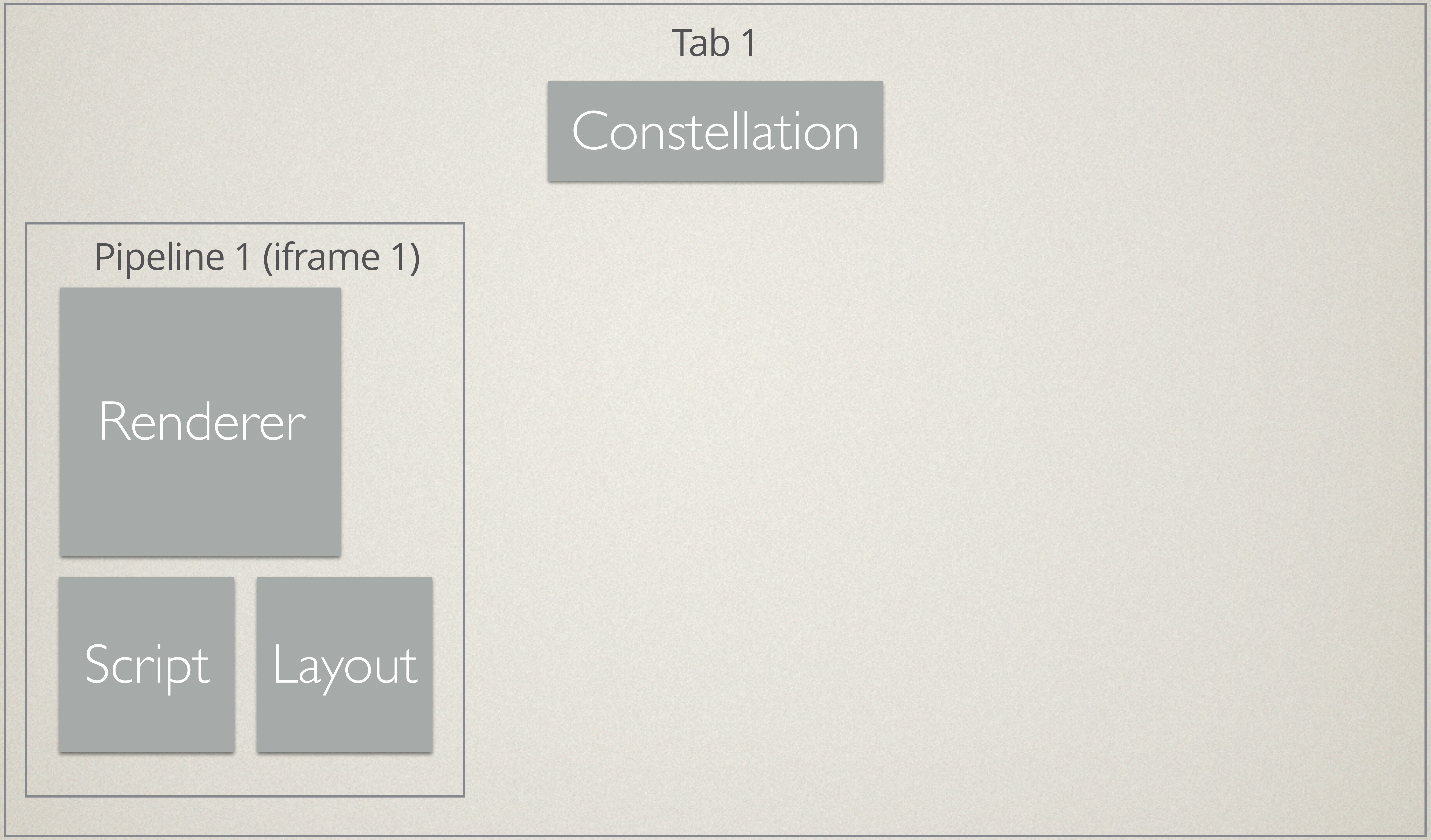
Новый минайпад 2 от Apple - у меня уже есть!
Sunflower Products I Love

from Etsy
Cute Kitsch Retro Apron - Handmade Full Womens Chef Apron in...
Cute Kitsch Retro Apron Handmade Full Womens by CreativeChics, $40.00
Meri Hurst Wish List- misc.

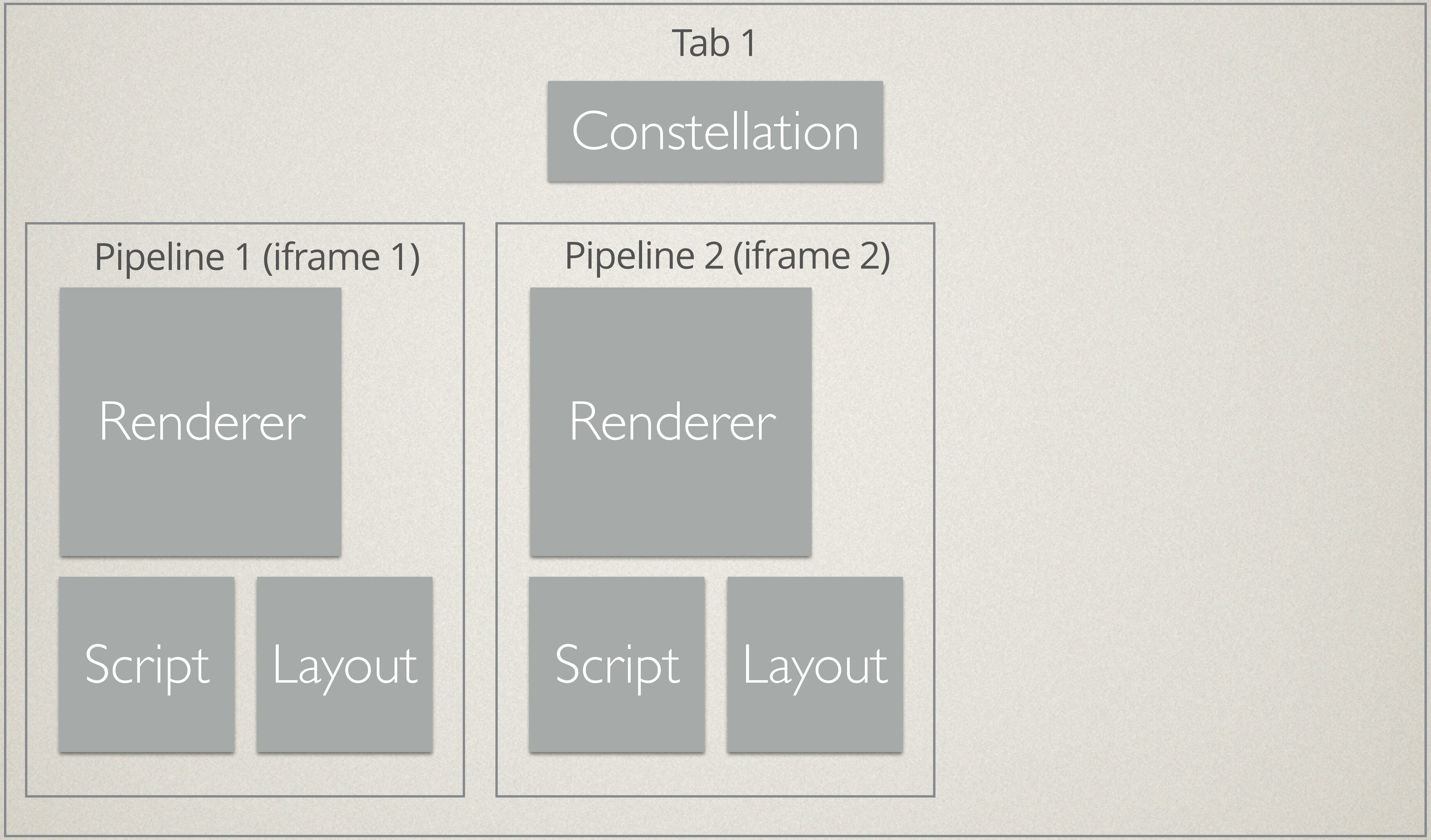
Christmas is almost here - Handmade Christmas Gifts
Alexandria Black Gifting

Community Helpers Math
Avery Guy Community Helpers

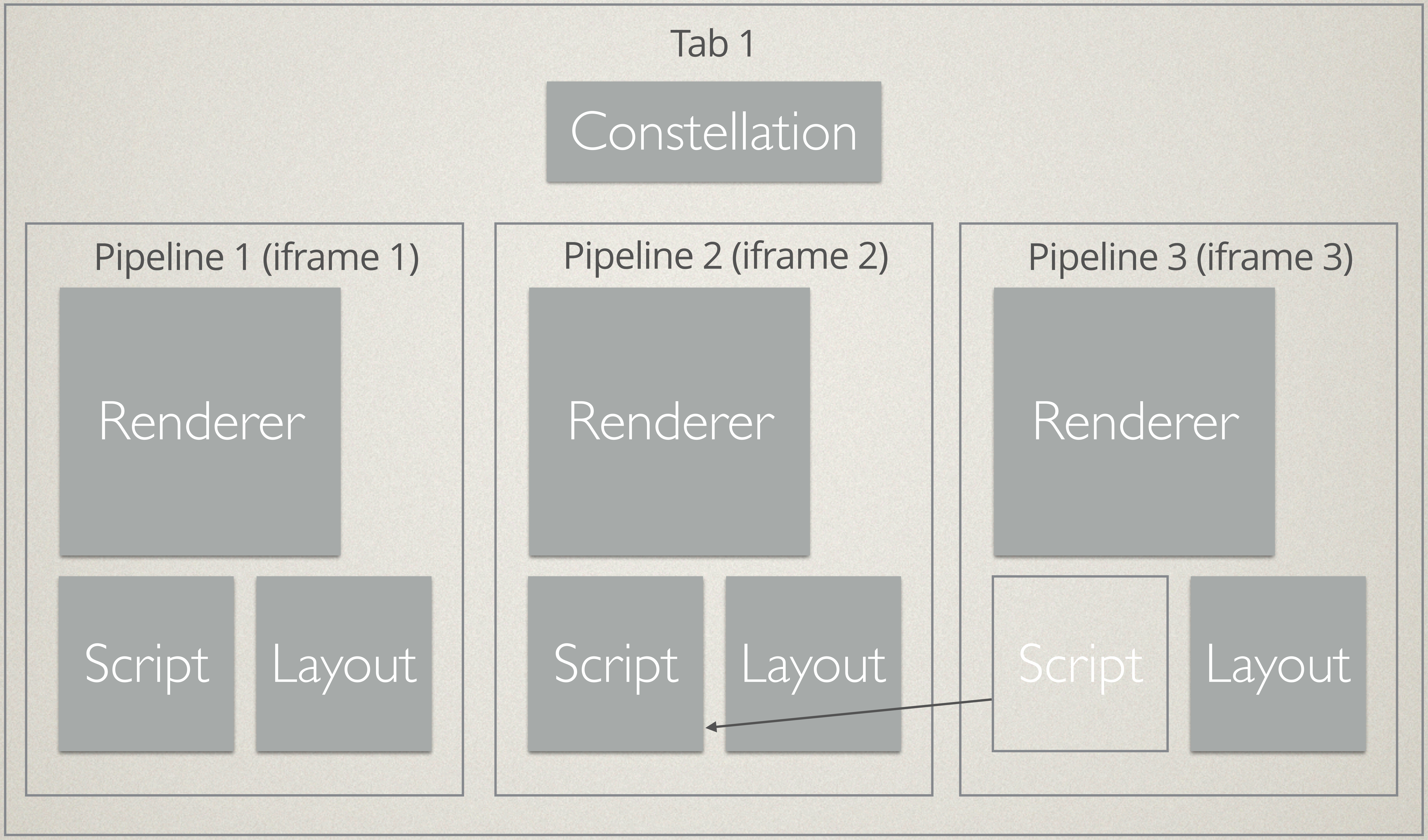
Servo's architecture



Servo's architecture



Servo's architecture



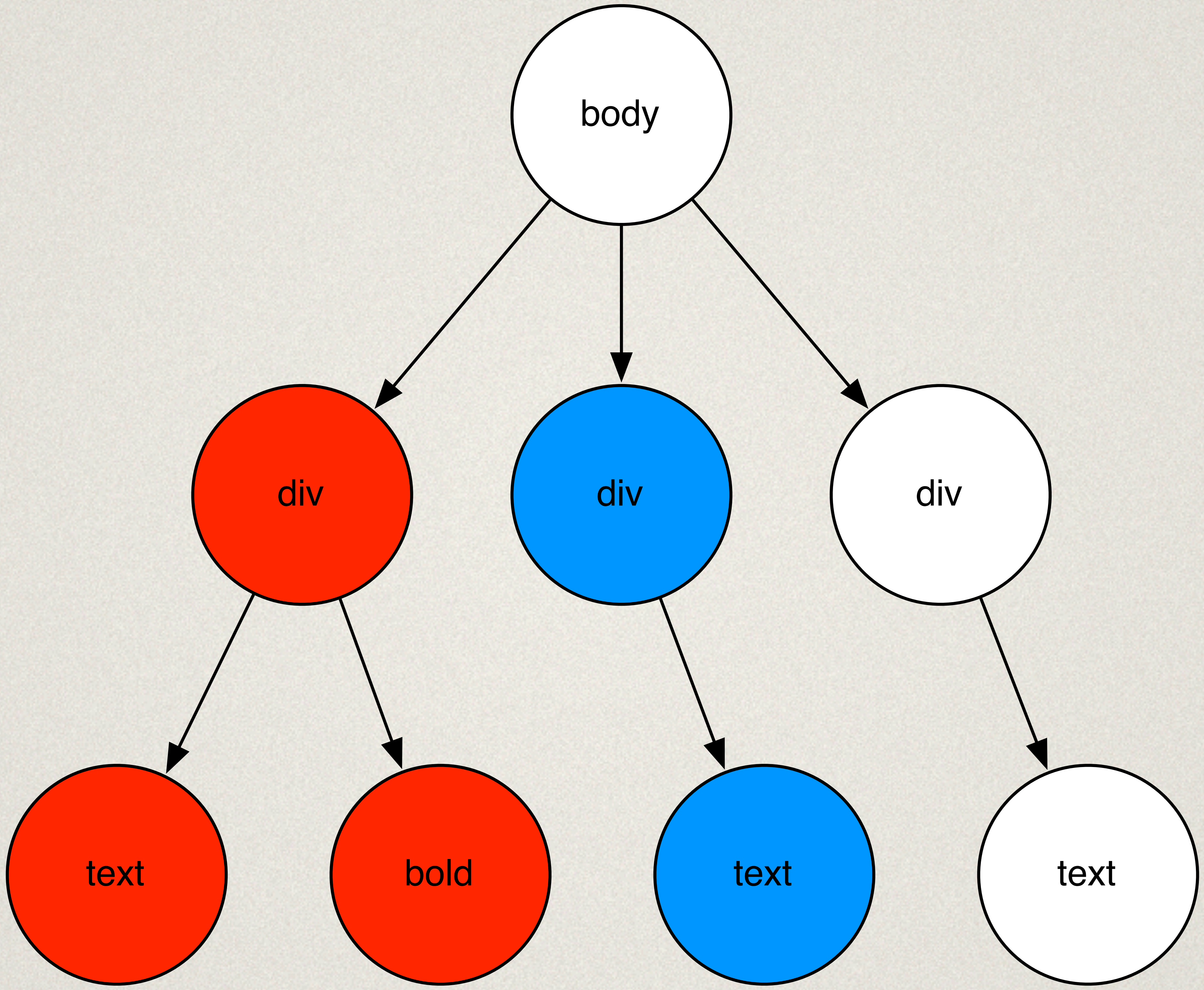
Demo: parallelism and sandboxing

Parallel layout

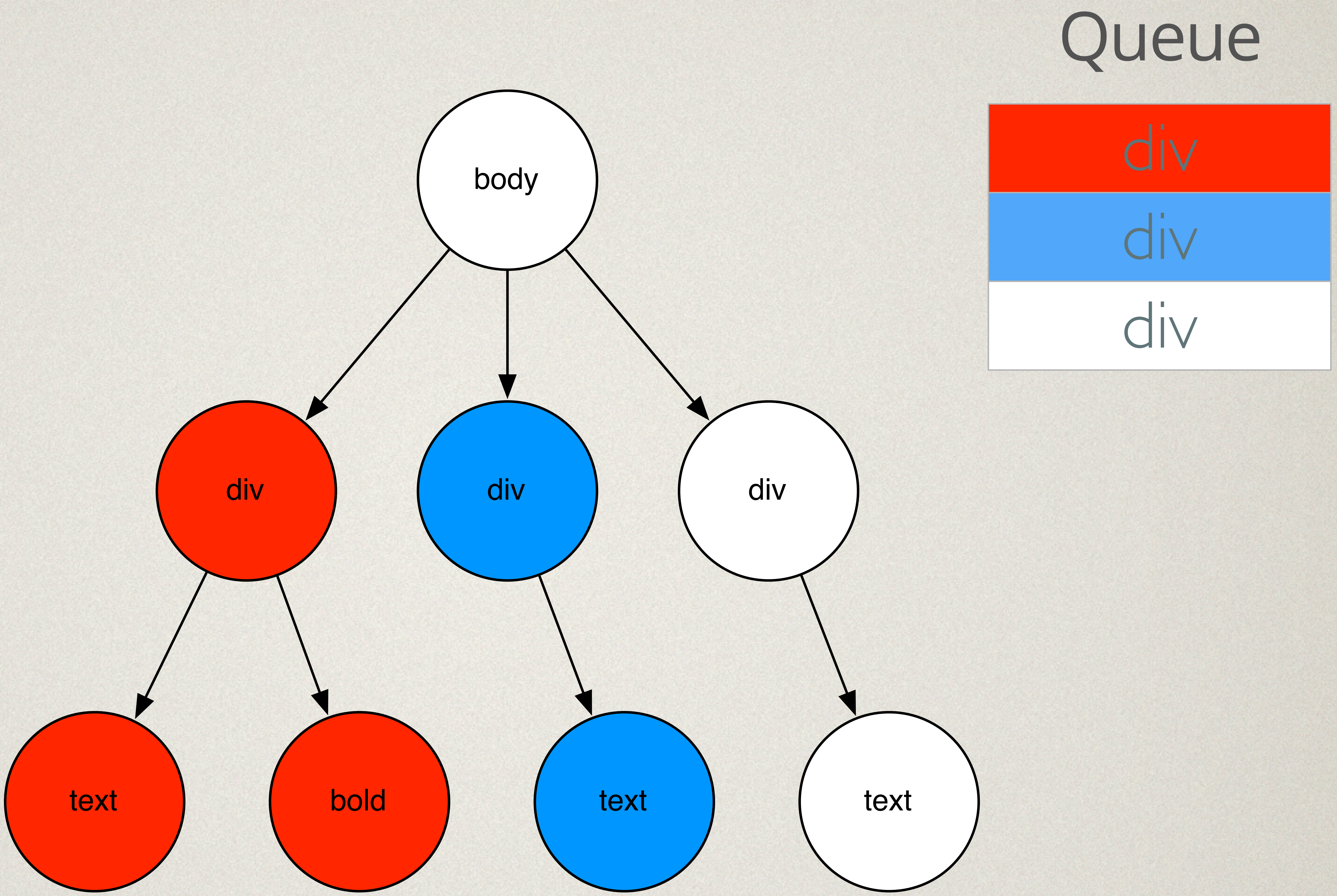
- Matters hugely on mobile platforms
    - Processors run at lower frequencies, but many cores
- Would enable more complicated pages on all platforms
- Implemented by work-stealing algorithm

See: Fast and Parallel Webpage Layout. Meyerovich and Bodik. WWW 2010.

Parallel layout



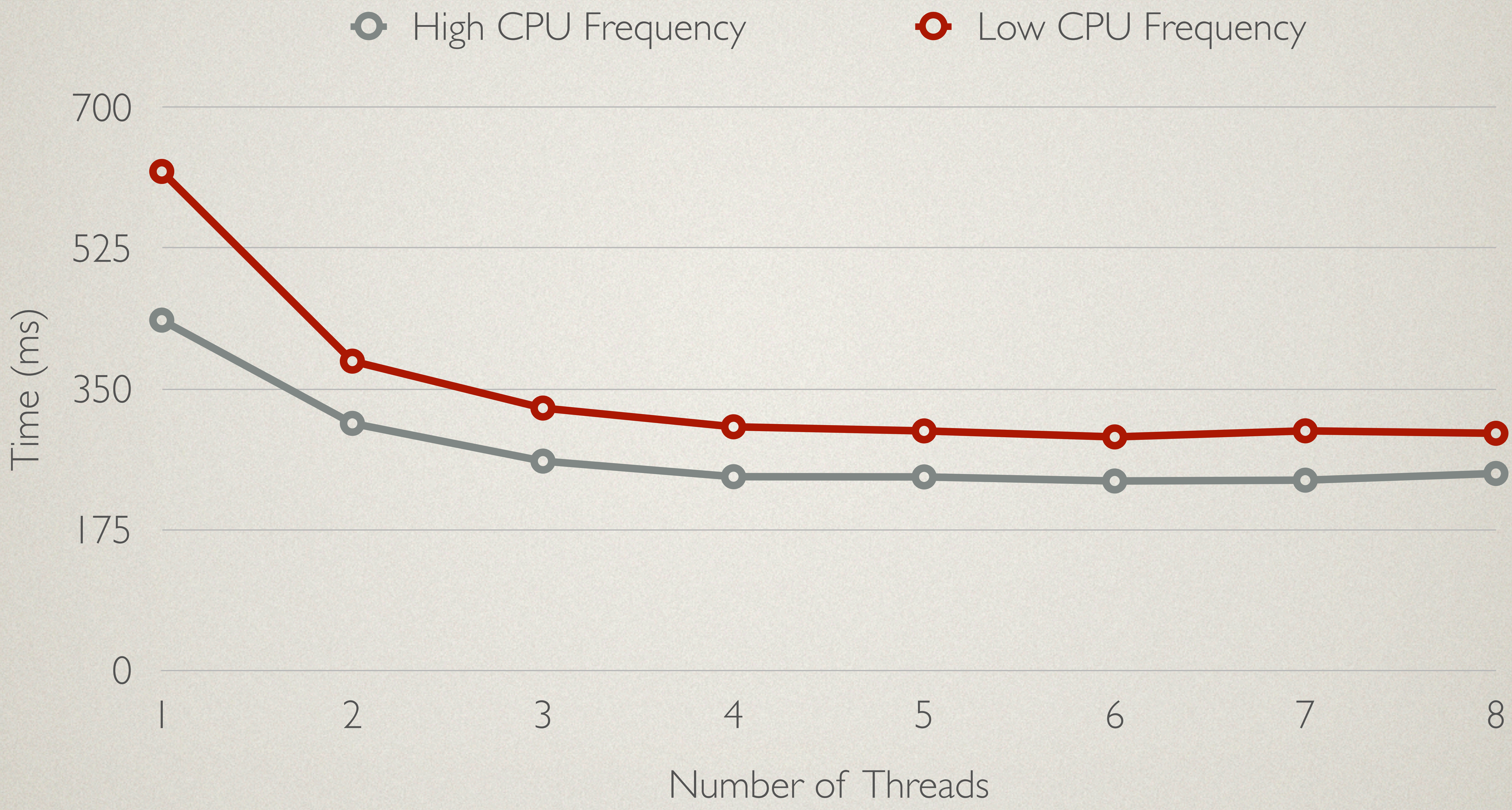
Parallel layout



Parallel layout challenges

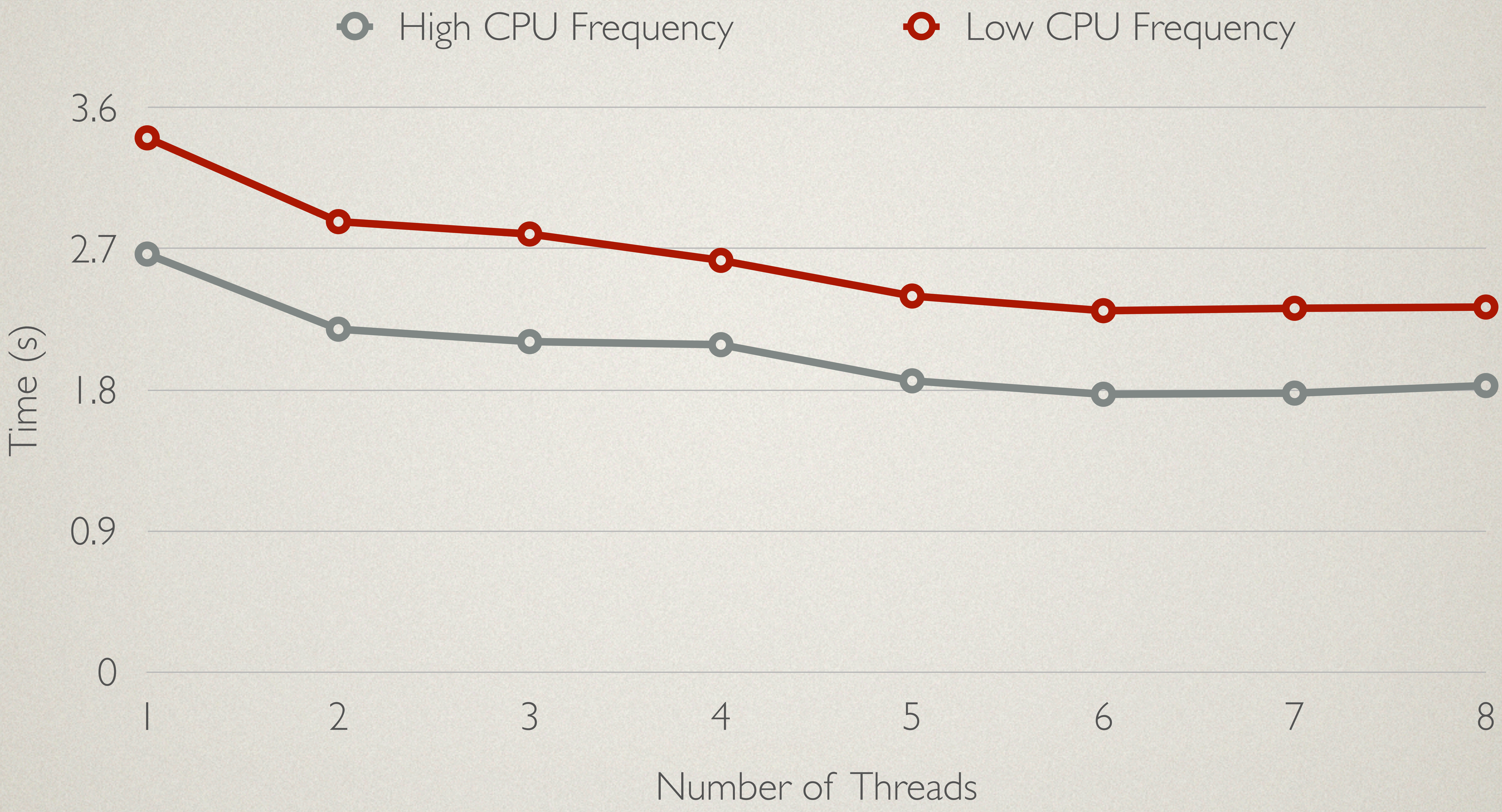
- HTML layout has complex dependencies
  - Inline element positioning
  - Floating elements
  - Vertical text
  - Pagination
- Considering adding speculation

Layout: parallel speedups

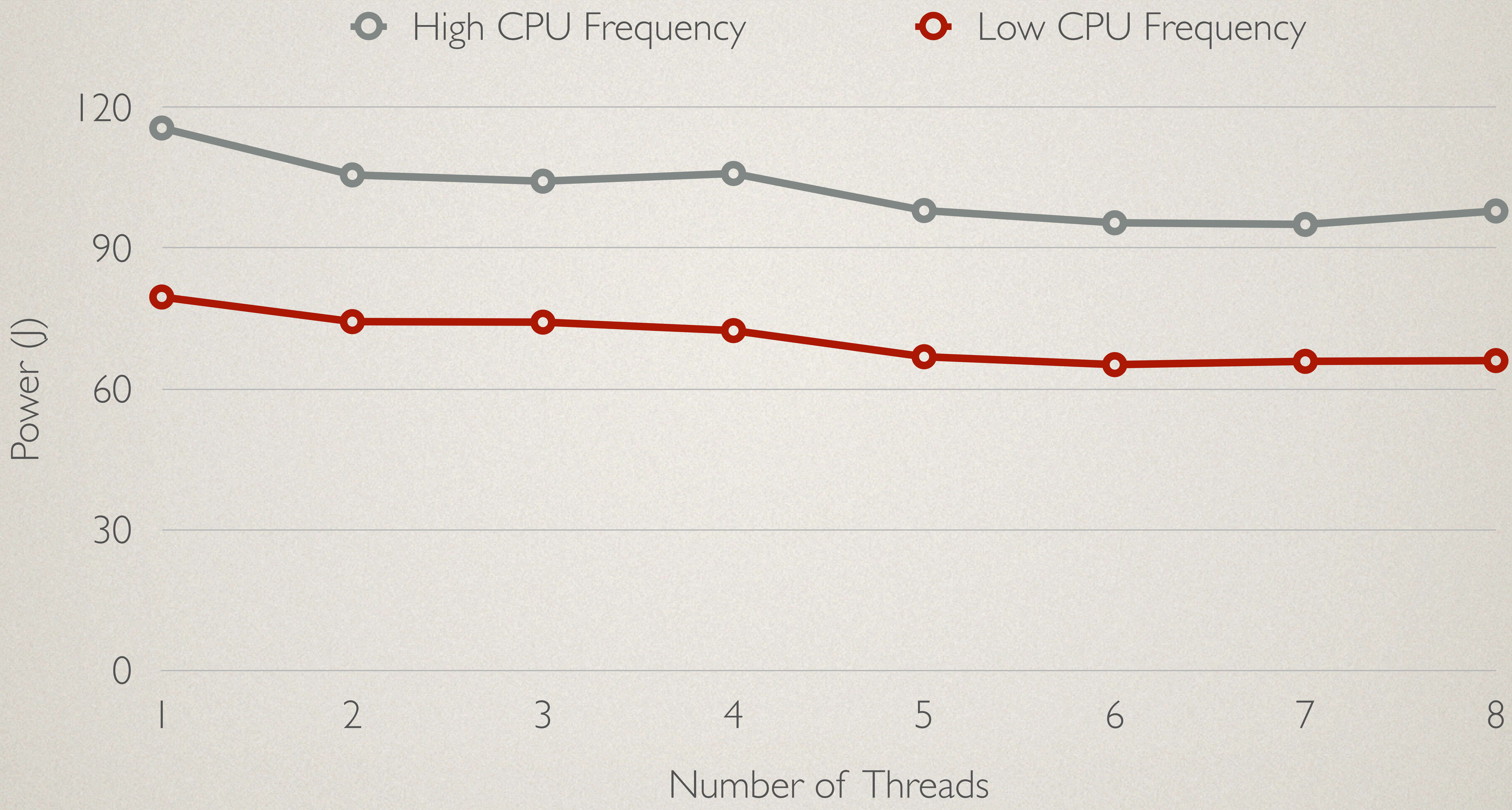


mozilla SAMSUNG

Total time with parallel layout



Total power with parallel layout



Measurements by Laleh Beni, intern from University of California Irvine

Punchline: parallelism for power, too

- Force low-frequency CPU setting
  - Above four cores, same end-to-end performance as single core at high-frequency
  - BUT, 40% of the power usage
- Could also parallelize more
  - Rendering, CSS selector matching, etc.

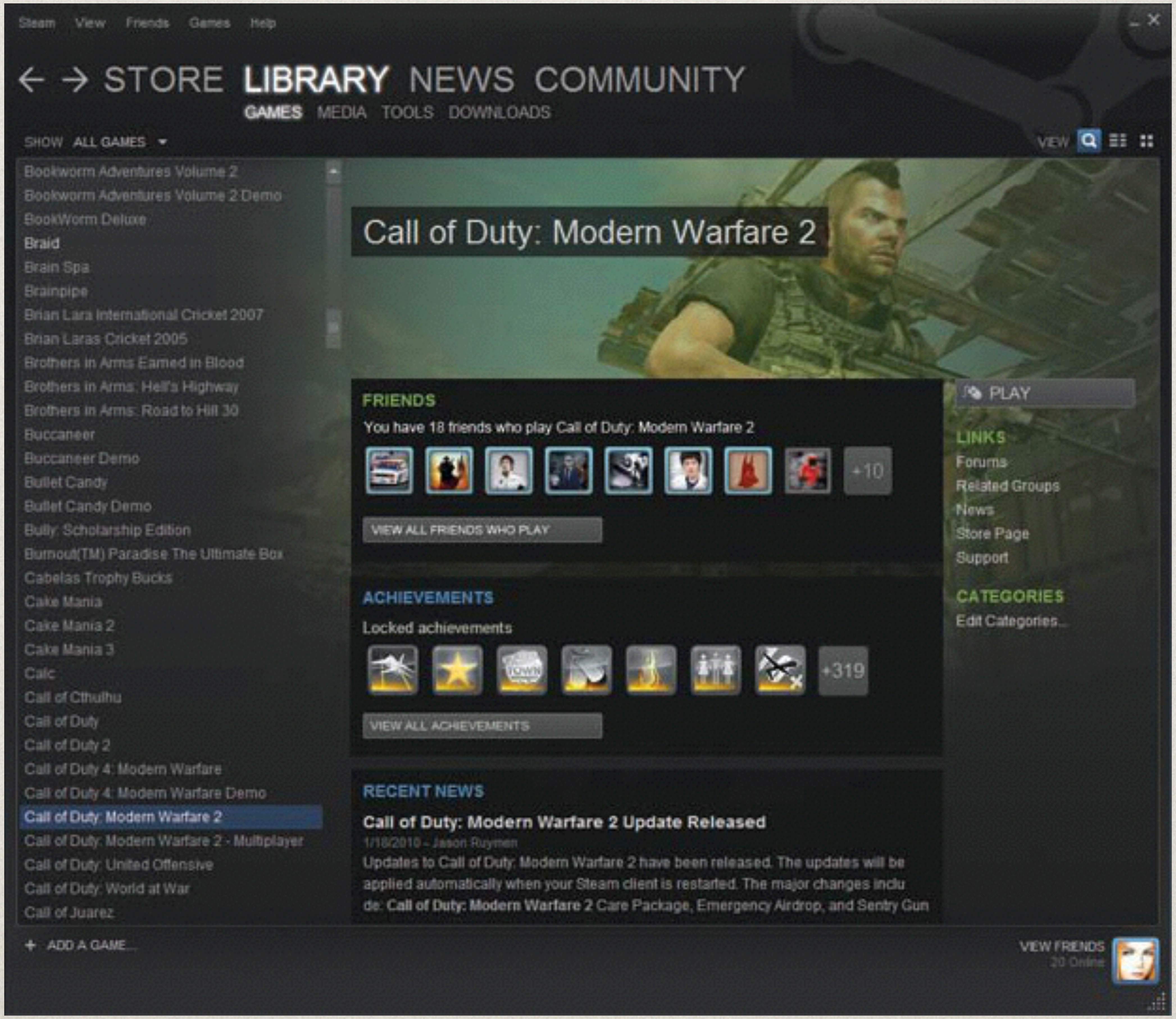
From engine to browser

- Servo just renders pages
  - Similar to the Blink and Gecko engines
- Designed to work in many browser shells
  - Firefox OS, over interprocess communication (IPC)
  - Android, by implementing a Java wrapper
  - On the desktop with…

mozilla SAMSUNG

What is embedding?

- Hosting web engine in native application


Steam View Friends Games Help
STORE LIBRARY NEWS COMMUNITY
GAMES MEDIA TOOLS DOWNLOADS
SHOW ALL GAMES
VIEW
Bookworm Adventures Volume 2
Bookworm Adventures Volume 2 Demo
BookWorm Deluxe
Braid
Brain Spa
Brainpipe
Brian Lara International Cricket 2007
Brian Laras Cricket 2005
Brothers in Arms Earned in Blood
Brothers in Arms: Hell's Highway
Brothers in Arms: Road to Hill 30
Buccaneer
Buccaneer Demo
Bullet Candy
Bullet Candy Demo
Bully: Scholarship Edition
Burnout(TM) Paradise The Ultimate Box
Cabelas Trophy Bucks
Cake Mania
Cake Mania 2
Cake Mania 3
Calc
Call of Cthulhu
Call of Duty
Call of Duty 2
Call of Duty 4: Modern Warfare
Call of Duty 4: Modern Warfare Demo
Call of Duty: Modern Warfare 2
Call of Duty: Modern Warfare 2 - Multiplayer
Call of Duty: United Offensive
Call of Duty: World at War
Call of Juarez
Call of Duty: Modern Warfare 2
FRIENDS
+10
VIEW ALL FRIENDS WHO PLAY
ACHIEVEMENTS
Locked achievements
+319
VIEW ALL ACHIEVEMENTS
RECENT NEWS
PLAY
LINKS
Forums
Related Groups
News
Store Page
Support
CATEGORIES
Edit Categories...
+ ADD A GAME...
VIEW FRIENDS
20 Online

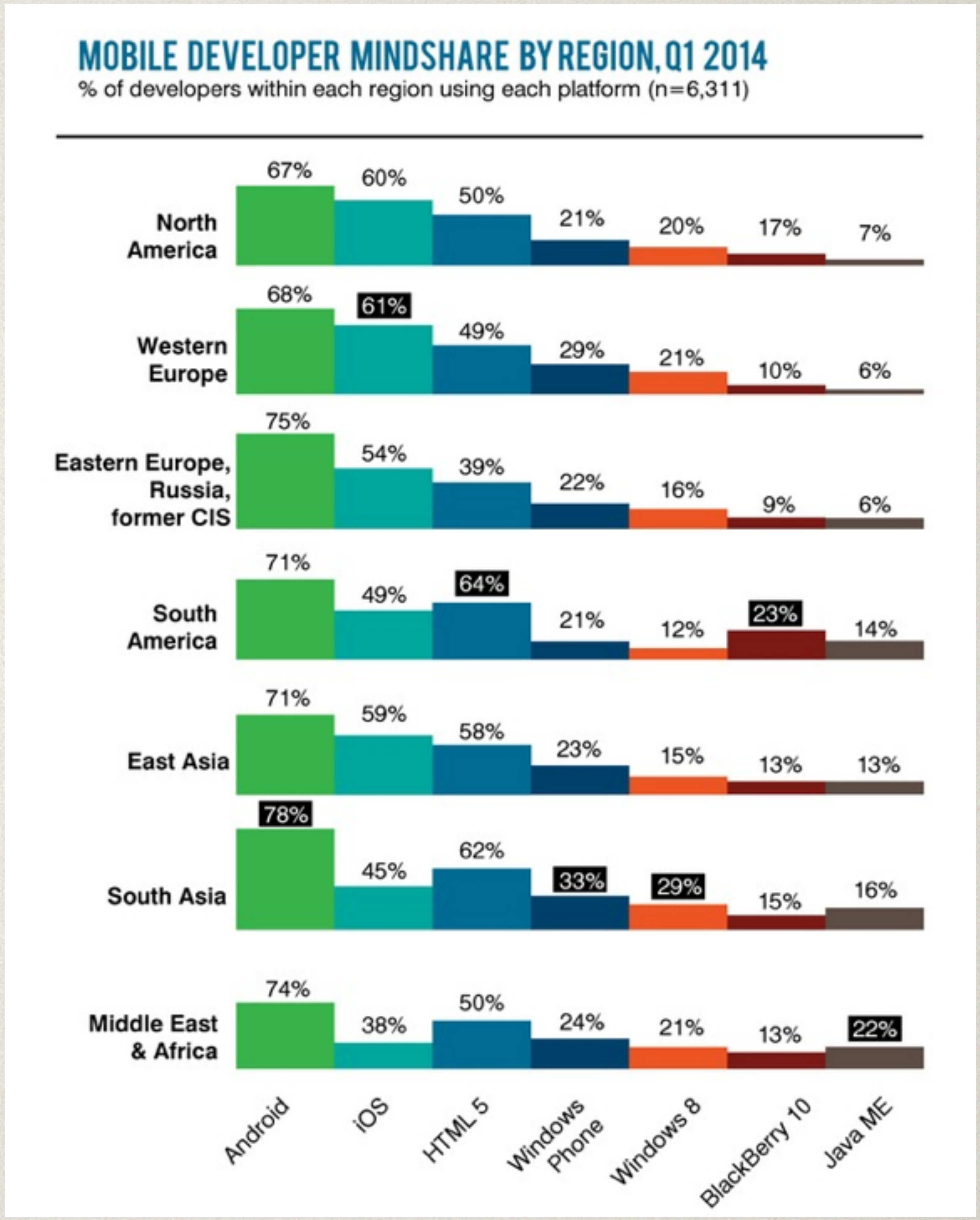
You have 18 friends who play Call of Duty: Modern Warfare 2

Call of Duty: Modern Warfare 2 Update Released
1/18/2010 - Jason Ruymen
Updates to Call of Duty: Modern Warfare 2 have been released. The updates will be applied automatically when your Steam client is restarted. The major changes inclu de: Call of Duty: Modern Warfare 2 Care Package, Emergency Airdrop, and Sentry Gun

mozilla SAMSUNG

Why embed?

- Reduced development time
- HTML5 popularity



% Highest regional Mindshare for the platform

vision mobile | Licensed under CC BY ND | Copyright VisionMobile
Source: Developer Economics Q1 2014 | www.DeveloperEconomics.com/go

How not to embed

- WebKit
- Blink
  - Both suffer from an unstable API
  - Application developer choices:
    - Ship full browser engine with application
    - Continually update to match breakages

How to embed?

- CEF: Chromium Embedded Framework
  - Isolates application developers from core API
  - C API with C++ extensions

Servo embedding strategy

- Stable API/ABI
  - Extensive API testing is a plus
- C-based
- Flexible
- Already designed

How to embed with Servo?

- Use CEF API+ABI
  - Removes need for YA embedding API
    - Less competition, more coding
  - Allows easy testing between engines
  - Servo: the pragmatic embedding engine

Servo embedding methodology

- Full symbol/ABI coverage
  - Every CEF function call resolves to a Servo function
  - Struct allocation sizes are identical

```
typedef struct _cef_string_utf8_t {
    char* str;
    size_t length;
    void (*dtor)(char* str);
} cef_string_utf8_t;
```

```
pub struct cef_string_utf8 {
    pub str: *mut u8,
    pub length: size_t,
    pub dtor: extern “C” fn(str: *mut u8),
}
```

C

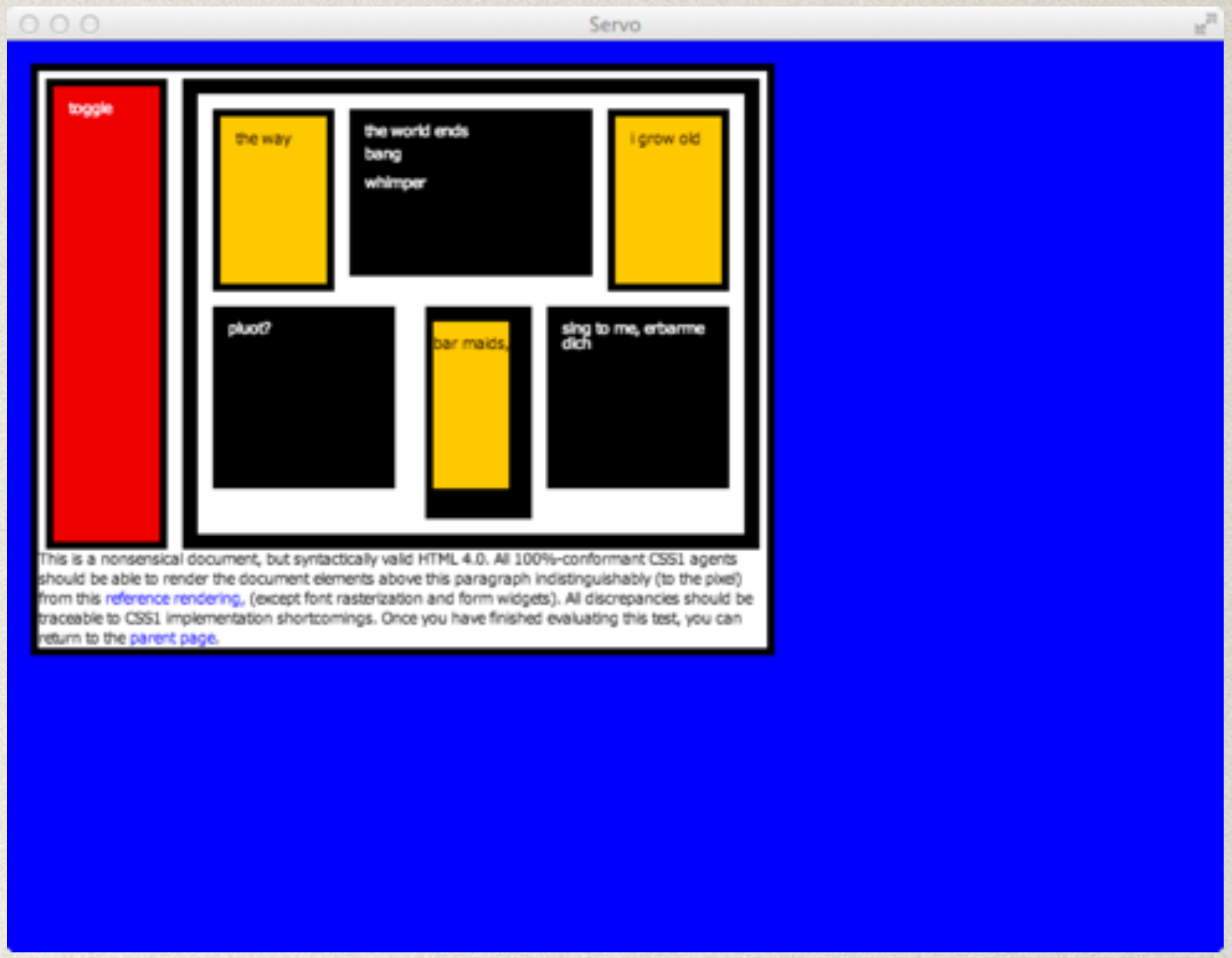
Rust

Servo embedding development

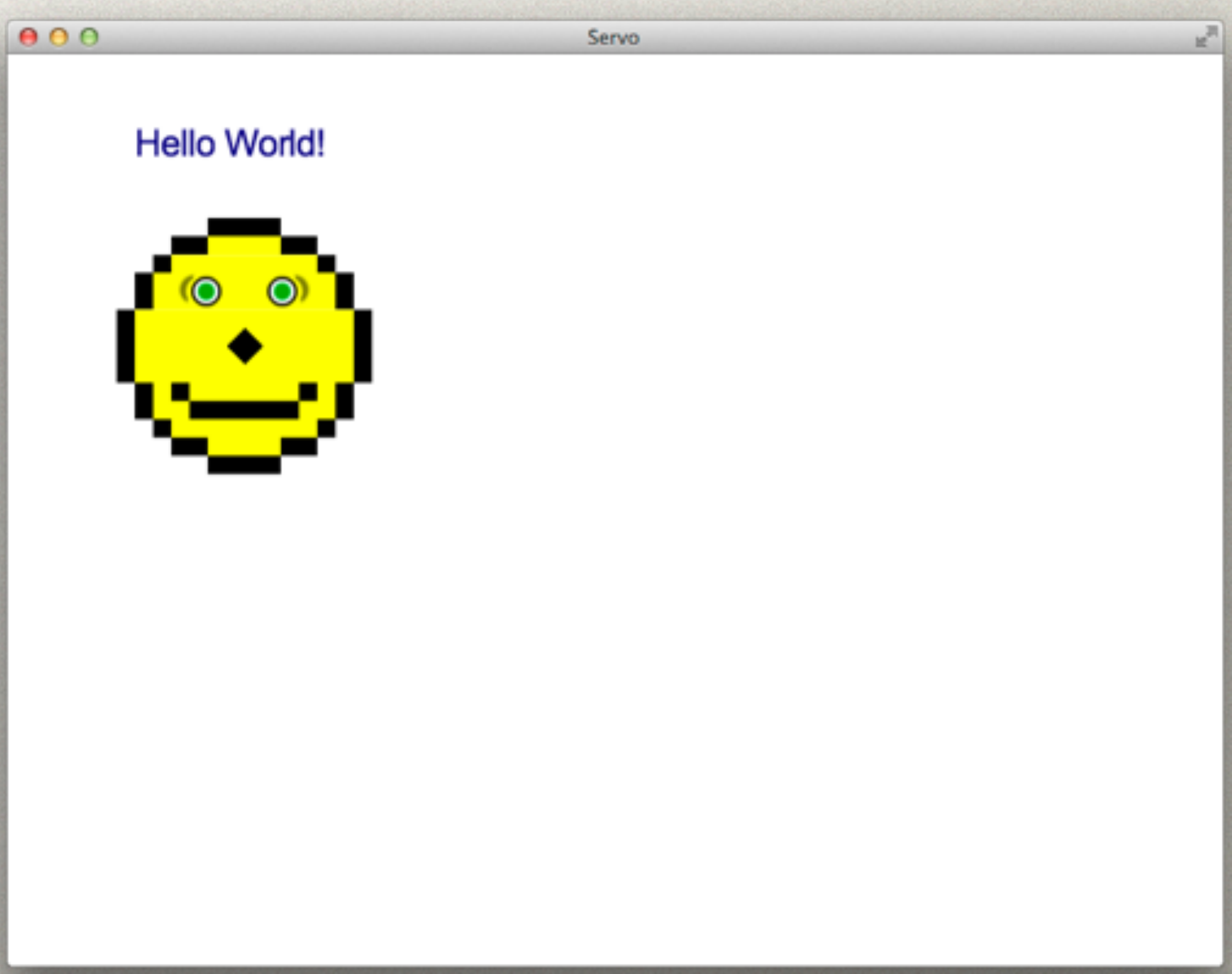
- Start with base set of symbols
  - `nm -u` on CEF applications
- Track function execution
  - CEF <-> Blink <-> Application <-> CEF ...
- Mimic CEF behavior using Servo equivalents
- Use preload hacks to test
  - LD_PRELOAD on Linux

Servo status

- Pass some tests
  - ACID1, ACID2
- Render basic web pages
  - Wikipedia, etc.
- Focus on design + challenges
  - Parallelism, latency, power, memory



This is a nonsensical document, but syntactically valid HTML 4.0. All 100%-conformant CSS1 agents should be able to render the document elements above this paragraph indistinguishably (to the pixel) from this reference rendering, (except font rasterization and form widgets). All discrepancies should be traceable to CSS1 implementation shortcomings. Once you have finished evaluating this test, you can return to the parent page.

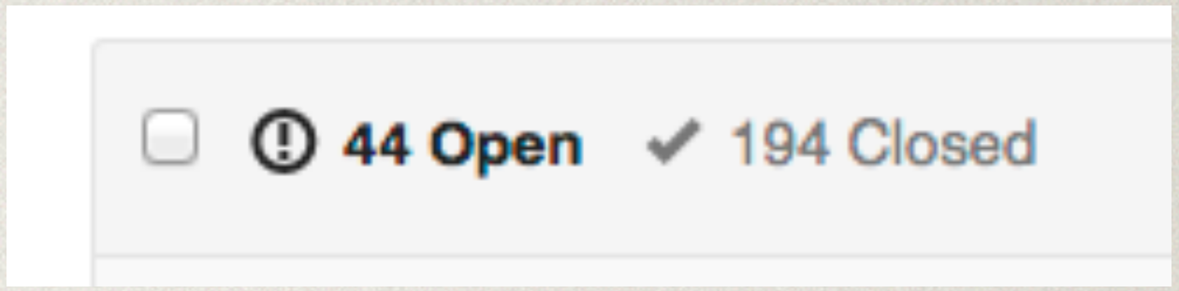


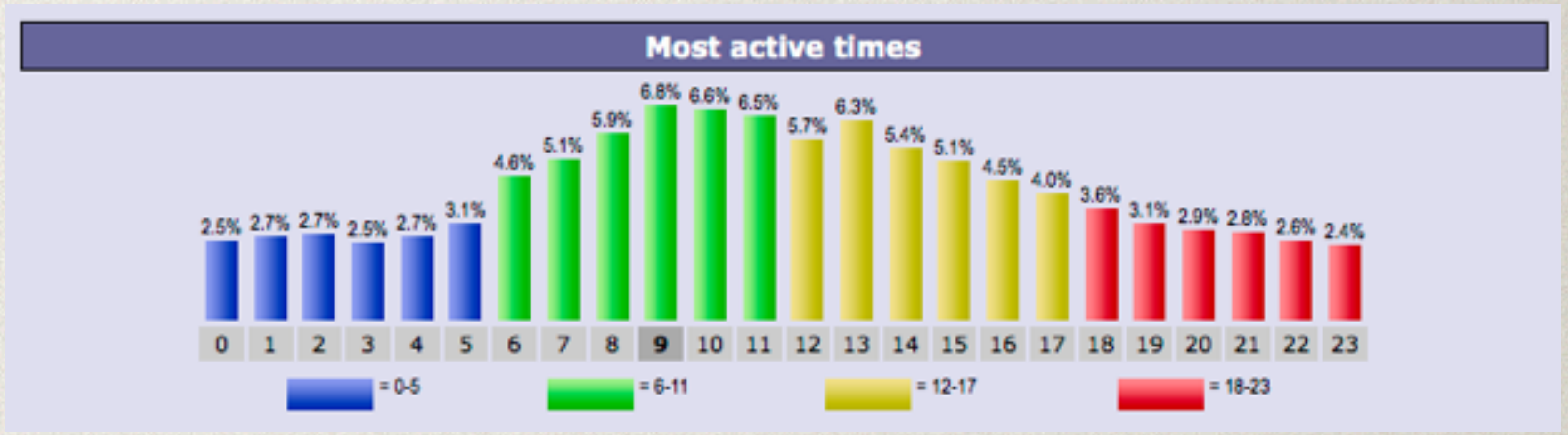
Servo roadmap

- https://github.com/servo/servo/wiki/Roadmap
- Q3 2014
  - Writing modes (vertical text)
  - DOM memory usage, perf, and features
  - Web Platform Tests & CSS Ref Tests
- Q4 2014
  - Very basic dogfooding

Getting involved with Servo

- www.github.com/servo/servo/issues
  - Filter for “E-Easy”
- irc.mozilla.org, #servo channel
  - Worldwide community
  - Looking for more partners and contributors
  - larsberg@mozilla.com


44 Open ✓ 194 Closed


Most active times
= 0-5
= 6-11
= 12-17
= 18-23