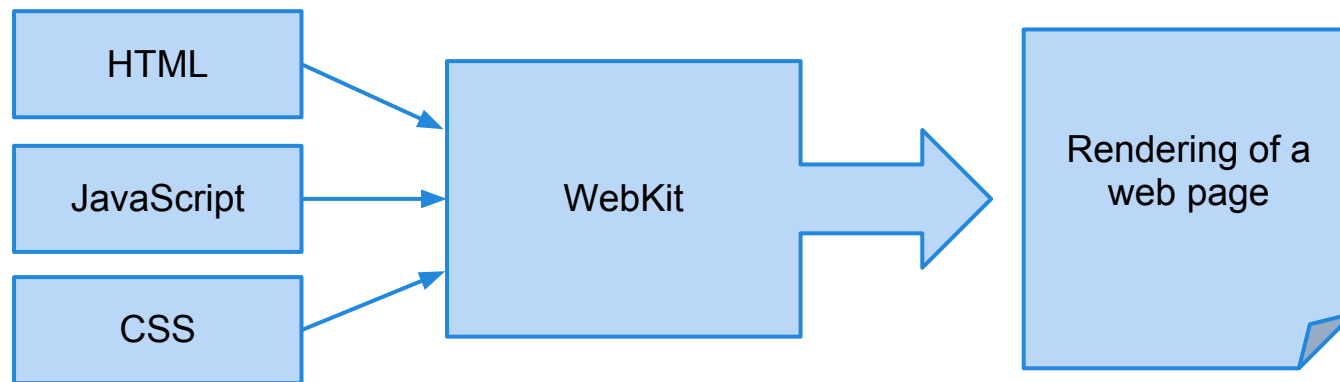


How WebKit Works

Adam Barth (abarth)
October 30, 2012

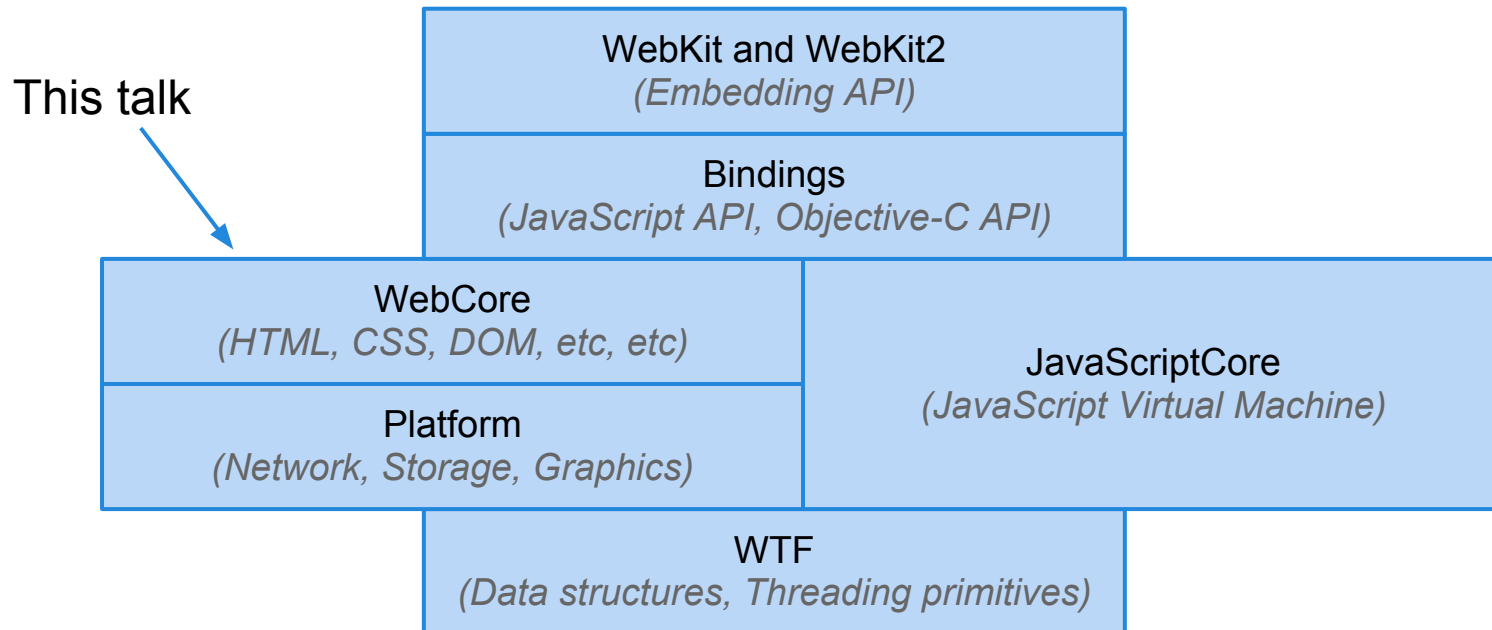
What is WebKit?

WebKit is a rendering engine for web content

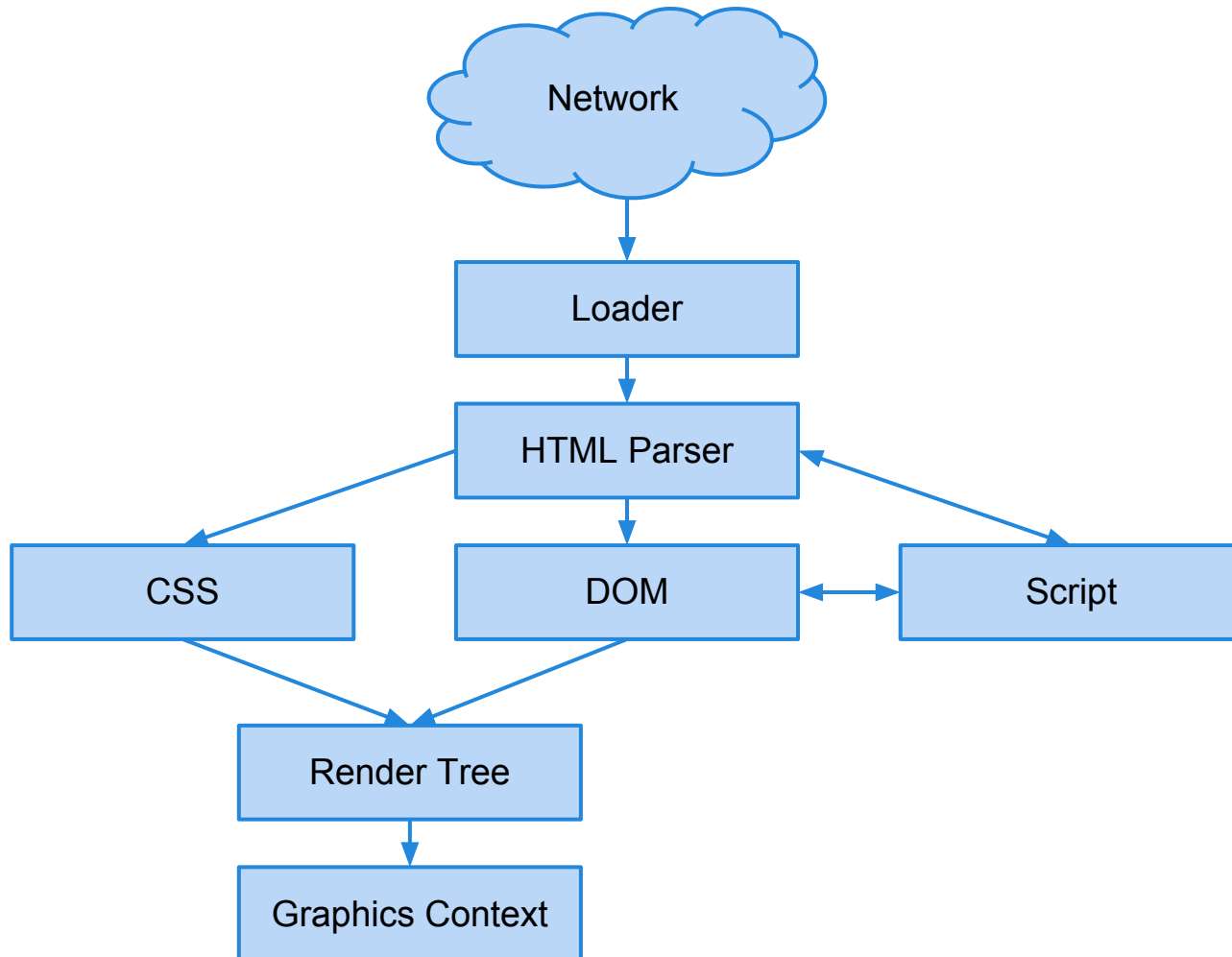


WebKit is not a browser, a science project, or the solution to every problem

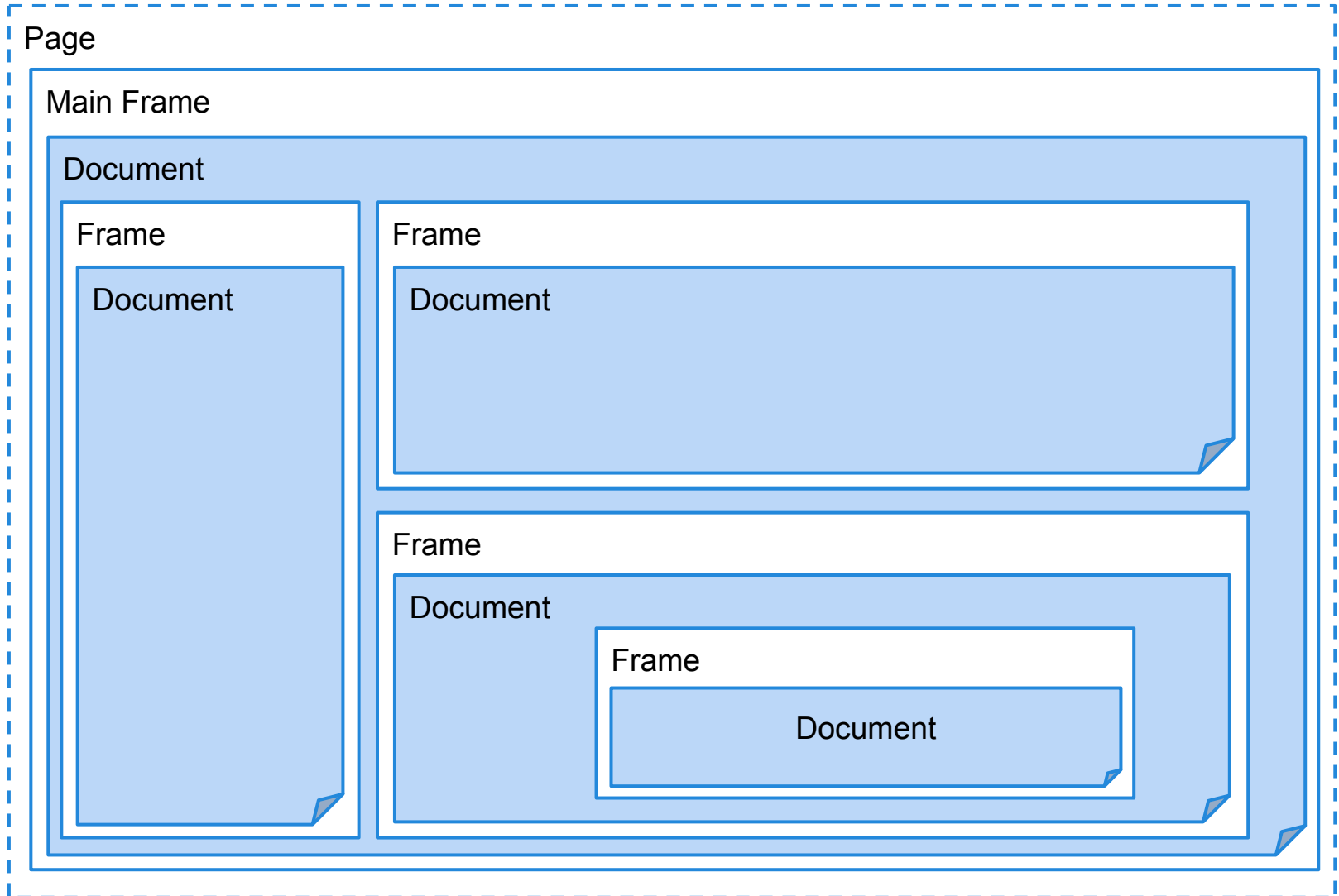
Major Components



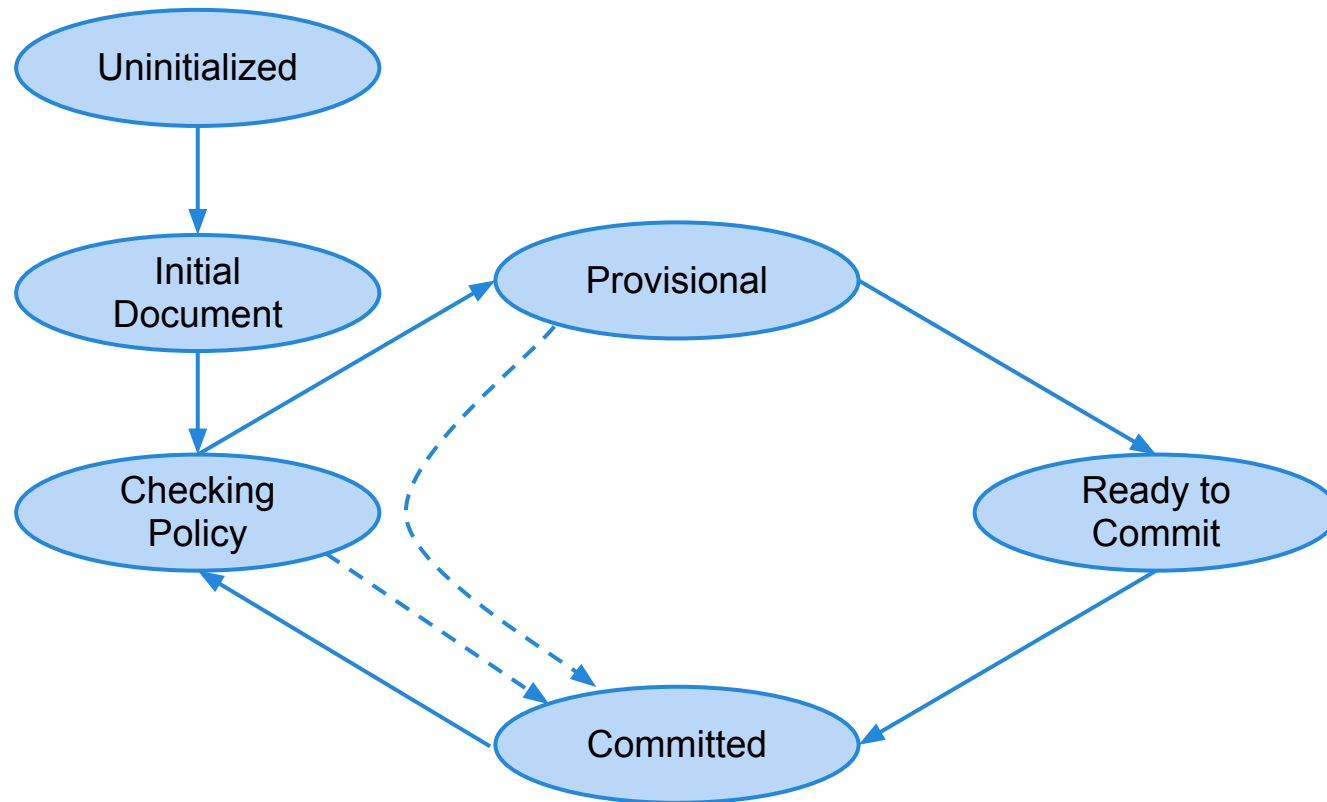
Life of Web Page



Pages, Frames, and Documents

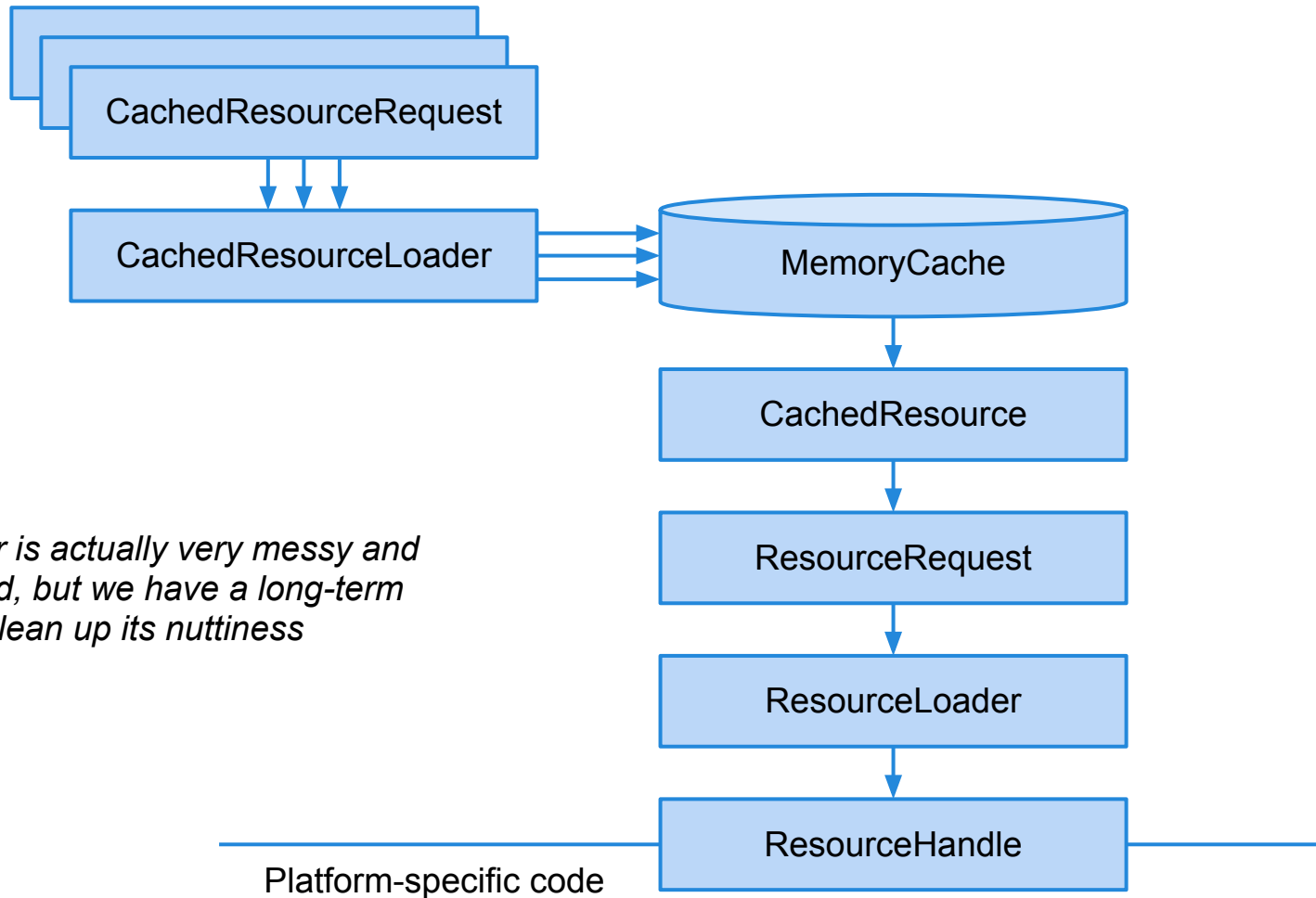


Lifecycle of a Frame

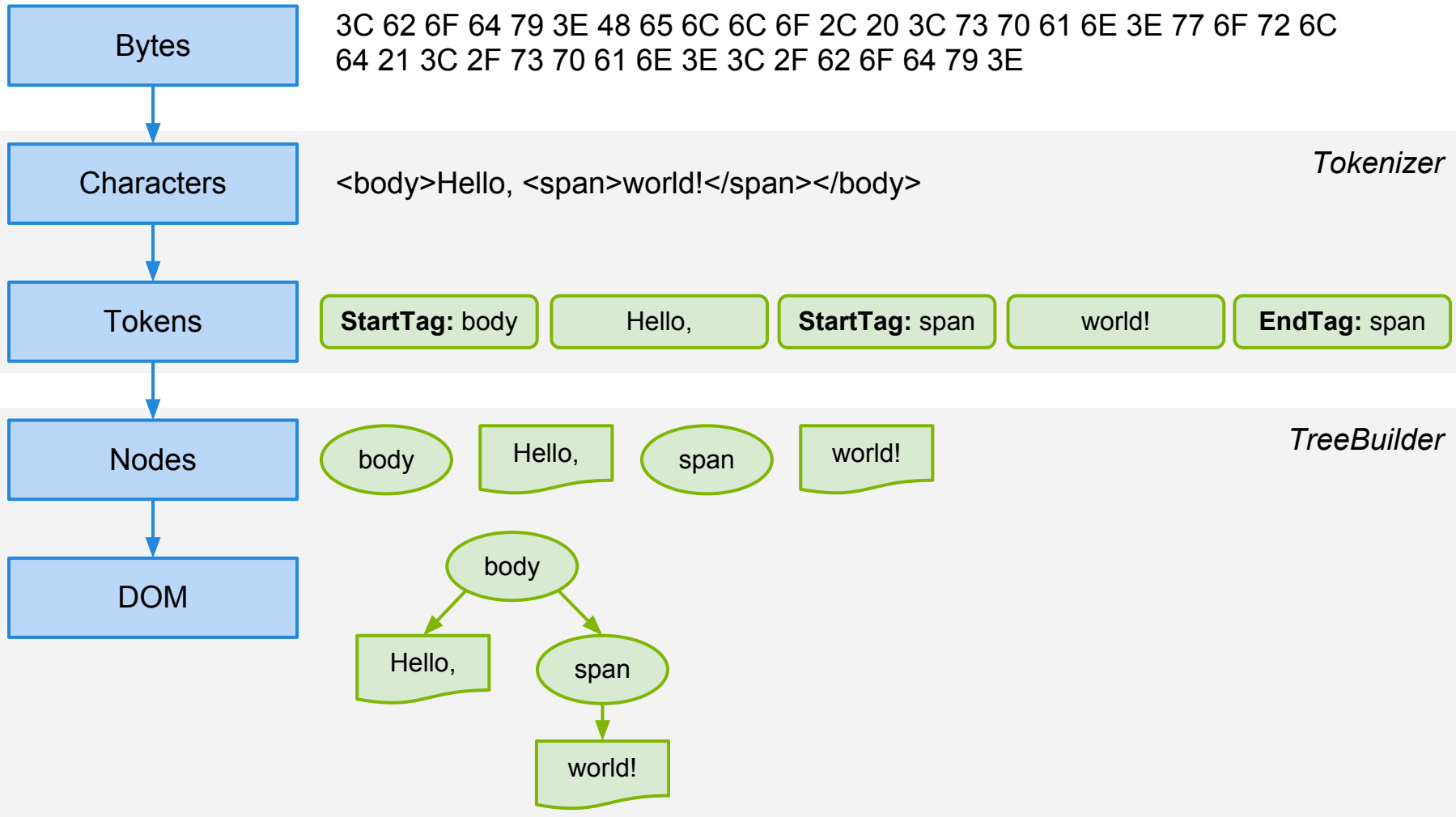


- Committed is the quiescent state

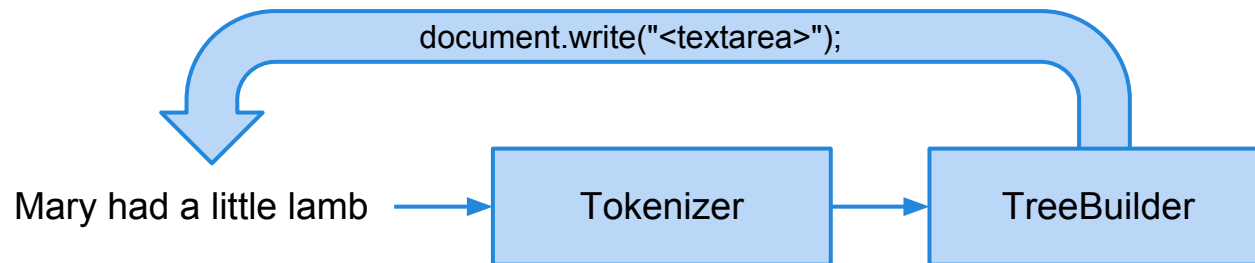
How the Loader Works (Idealized)



How the HTML Parser Works



Preload Scanning for Fun and Profit

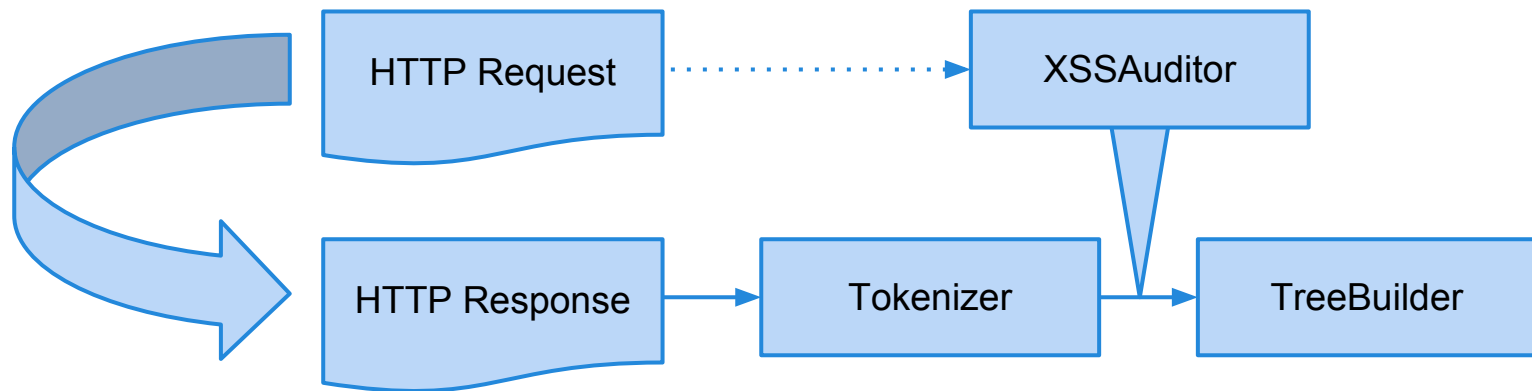


Script execution can change the input stream

Preload scanner tokenizes ahead

- When parser is blocked on external scripts
- Starts resource loads earlier

XSSAuditor



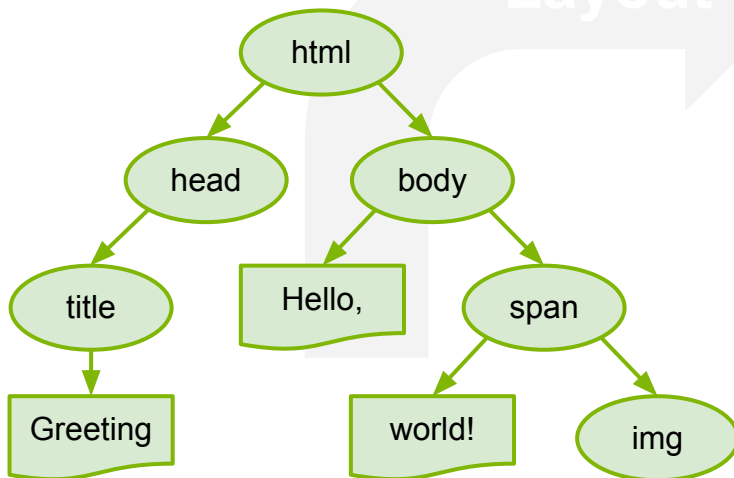
XSSAuditor examines token stream

Looks for scripts that were also in the request

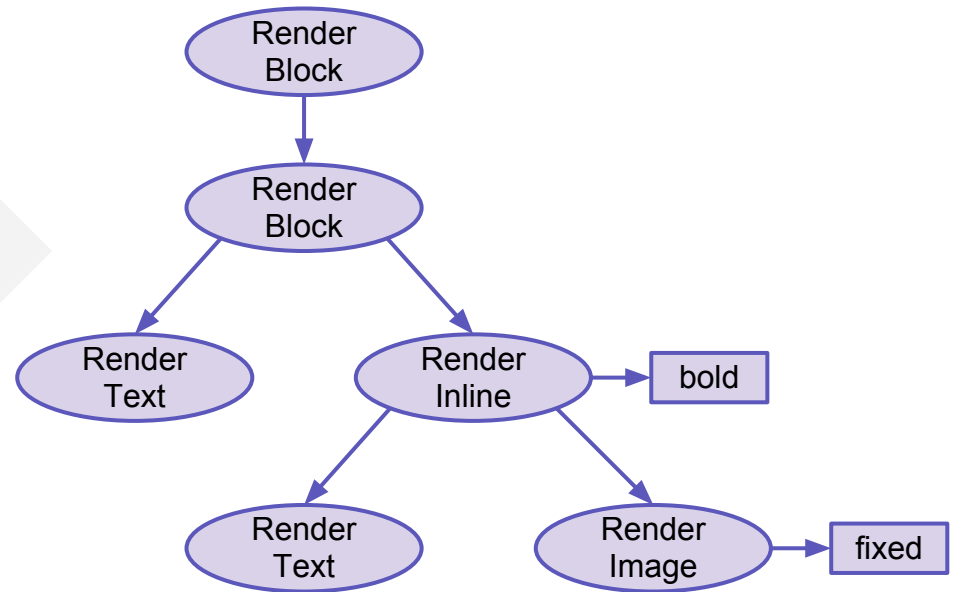
- Assumes those scripts were reflected XSS
- Blocks them

DOM + CSS → Render Tree

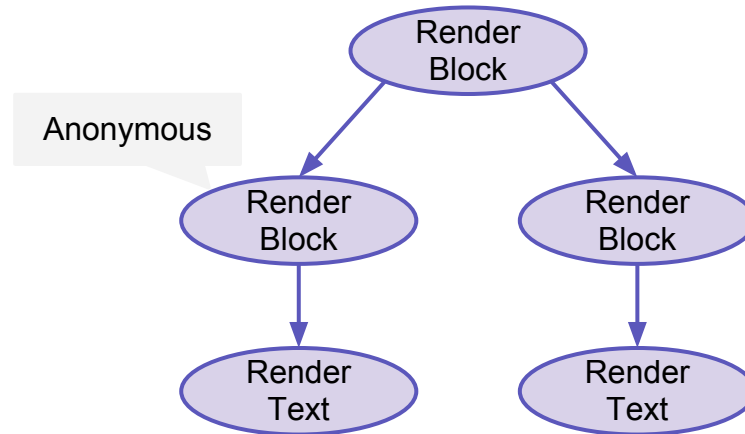
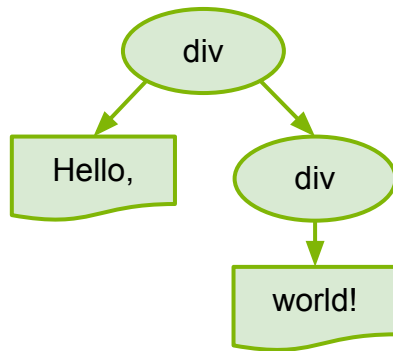
```
#footer { position: fixed; bottom: 0; left: 0 }  
body > span { font-weight: bold; }
```



Layout

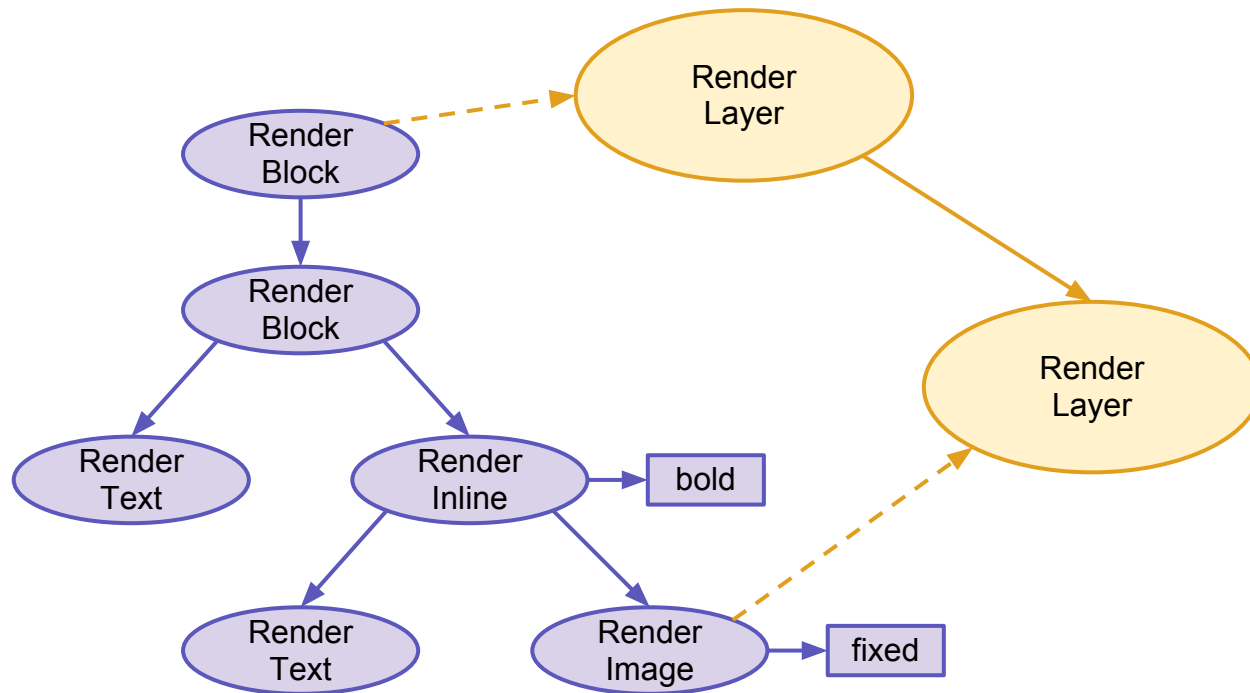


Anonymous RenderObjects



- Not every RenderObject has a DOM Node
- Every RenderBlock either:
 - Has *all* inline children
 - Has *no* inline children

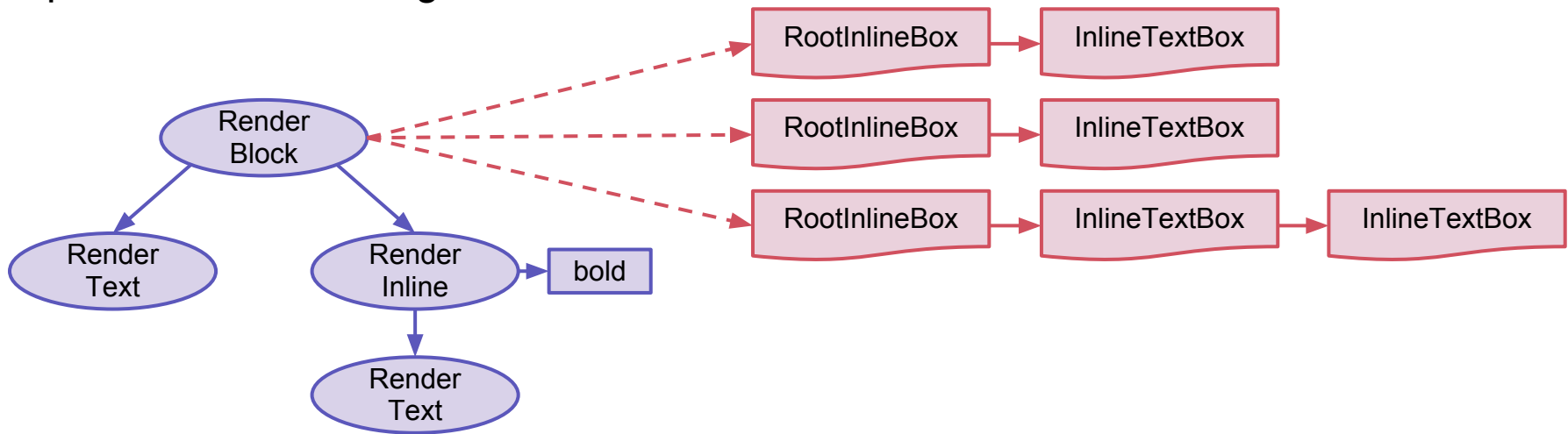
LayerTree



- Sparse representation of RenderTree
- Enables accelerated compositing, scrolling

Yet Another Tree: LineBoxTree

<div>An old silent pond...
A frog jumps into the pond,
splash! Silence again.</div>



- One RootInlineBox per line of text
- List of inline flow and inline text boxes

Conclusion

- WebCore's main processing pipeline:
 - Loader and Parser
 - CSS, DOM, and Script
 - RenderTree, LayerTree, and InlineBoxes
- Other major subsystems
 - Accessibility, Editing, Events, CSS, Web Inspector
 - Plugins, SVG, MathML, XSLT...
- Other components
 - WebKit, Bindings, Platform, JavaScriptCore, WTF
 - ... 1.5 MLOC of C++
- Learn more:
 - <http://www.webkit.org/coding/technical-articles.html>

Thanks!

abarth@webkit.org