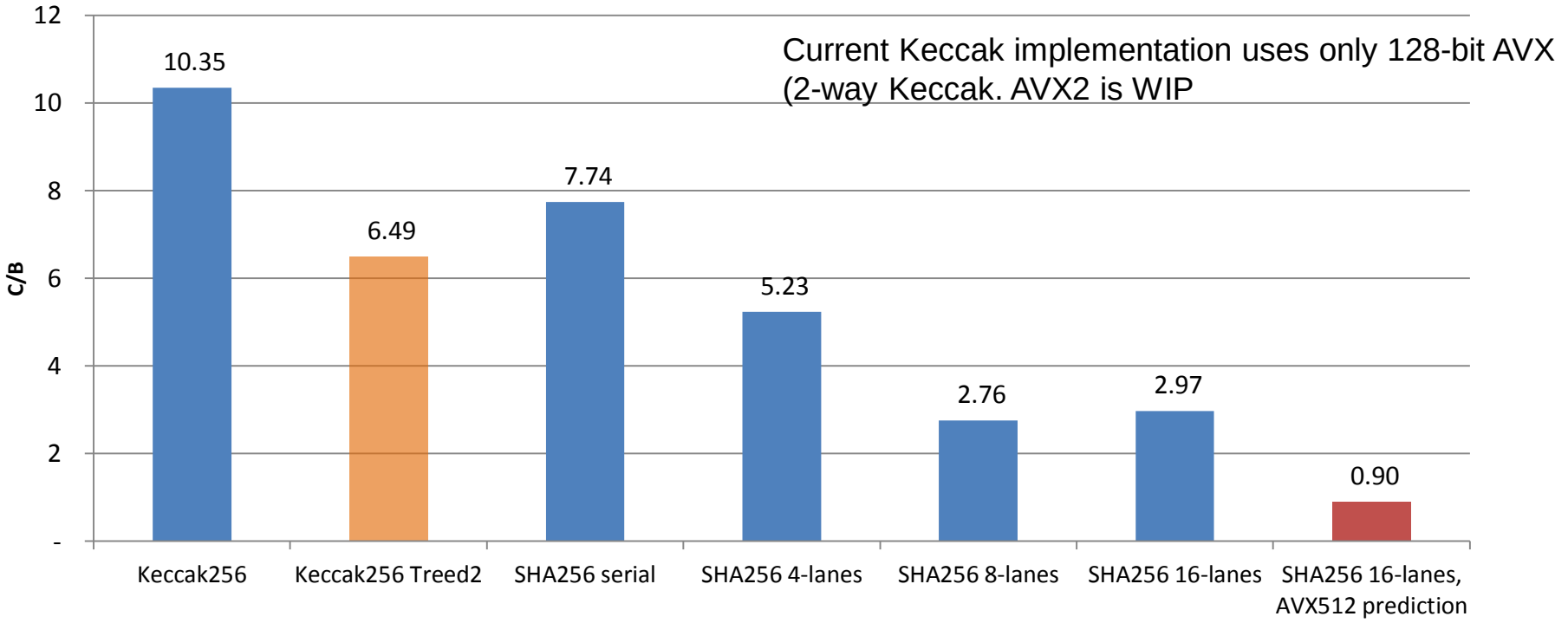
Current performance comparison:
Keccak256, Treed Keccak256, SHA-256, j-lanes SHA-256
Haswell microarchitecture (AVX2)



Keccak numbers from http://bench.cr.yp.to/results-hash.html, wintermute machine ("long message")

- j-lanes SHA-256 has a significant performance advantage
  - Even with "less-then-optimal" j=16 on current architecture
- Expect AVX512 with j=16 to improve further

Summary, conclusions, and call for action

Conclusion:

- j-lanes hash & j-pointers offer a significant performance advantage on current and future architecture. It would be a useful standard

Options to consider:

- Best to allow full flexibility:
  - Any j (=4/8/16), both j-lanes and j-pointer, any underlying HASH function
  - j+1 Prefix values (1 Prefix might suffice?)
- If only one j can be standardized: suggest j=16
  - Small performance compromise on current CPU's & high forthcoming potential

Call for action:

- Standardize j-lanes / j-pointers hash as a hashing mode