What makes blockchains useful?

Dave Maher, EVP, CTO Intertrust

Its all about Hash functions

- One-way function that maps any document into a fixed length string:
- D —> H(D) = (3fa918d… 4e761)
- Standardized (such as SHA(256) defined by NIST)

- Easy to compute
- Infeasible to generate a document D with a given hash value H(D)
- If D and D’ differ in even 1 bit, H(D) is very different from H(D’)
- Infeasible to find collisions, ie. two documents D and D’ such that H(D) = H(D’)

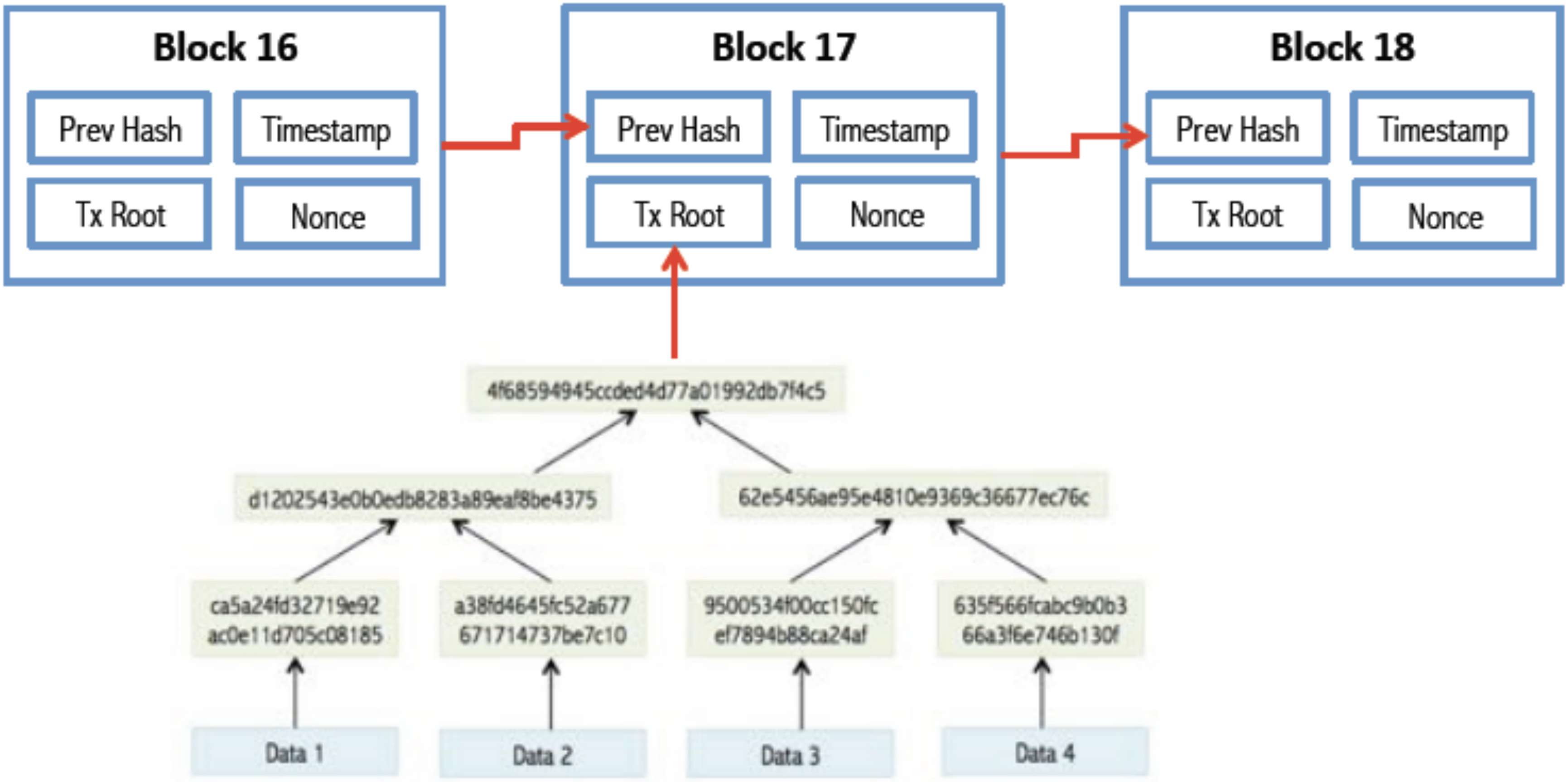
How big is 256 bit Hash space?

As many points as the number of *atoms* in the universe
(At least in the closest 100 *Sextillion* stars)

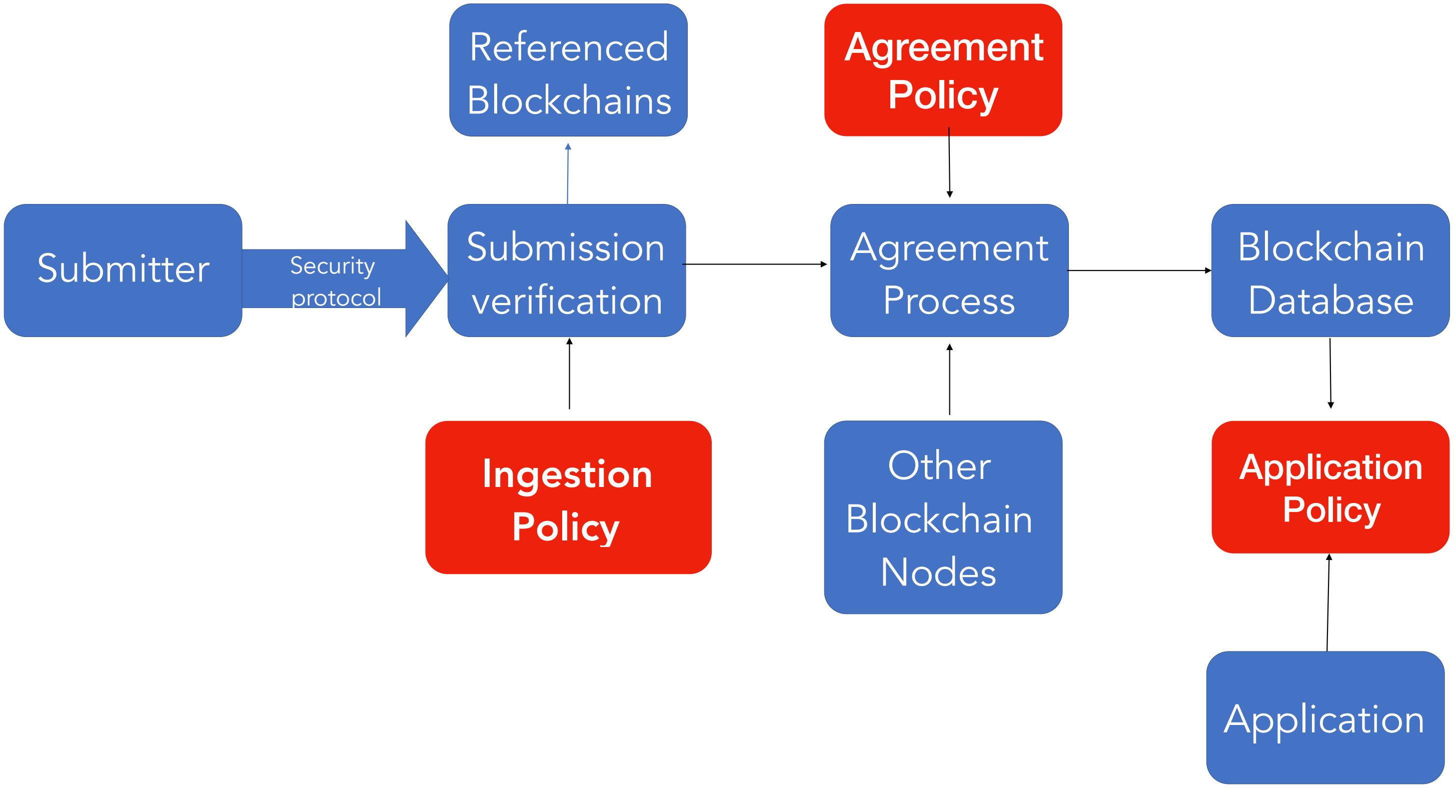
A good hash function (pseudo) randomly distributes values in this space

So, a Hash function can authenticate a document IF we can fix its value in time

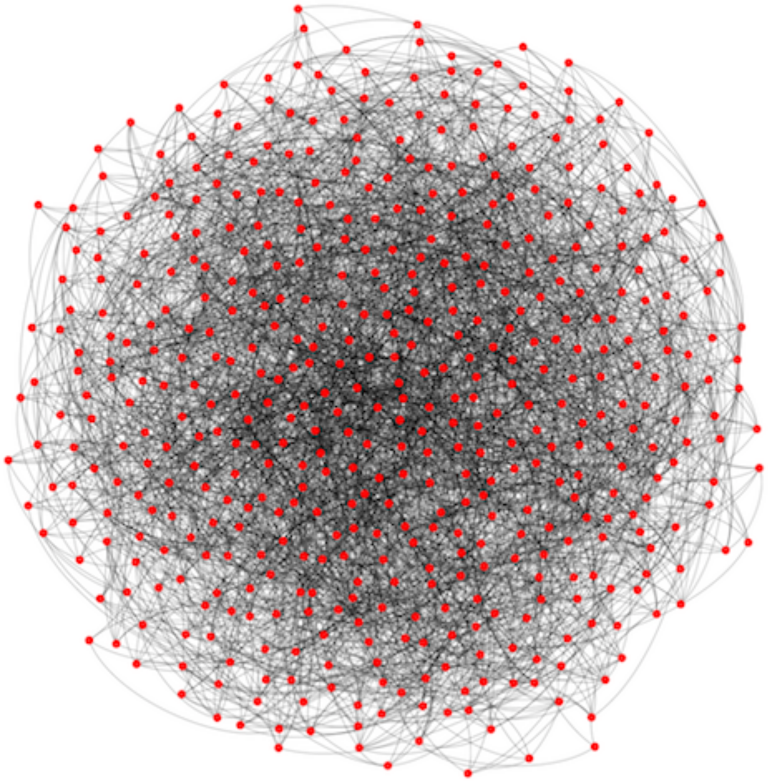
Blockchains fix documents immutably in time



Different blockchains can be distinguished by Policy



Thoughts on Trust and Agreement Policy



The thing that we need is a bee-watcher-watcher!. Well, the bee-watcher-watcher watched the bee-watcher. He didn't watch well so another Hawtch-Hawtcher had to come in as a watch-watcher-watcher! And now all the Hawtchers who live in Hawtch-Hawtch are watching on watch watcher watchering watch, watch watching the watcher who's watching that bee" -- Dr. Seuss

Every one in Hawtch-Hawtch can be "a bee watch-watcher and watch the other bee watcher-watchers

Blockchain submissions can be:

- Transactions
- Assertions (for example about identity)
- Smart contracts
  - Programs with verifiable inputs (events), automated outputs
- Permissioned or non-permissioned
- Publicly readable, or private: Documents private, Hashes public or private