I remember a while back reading a paper I think about Hyperledger and ‘proof-of-elapsed’ time. The idea was something like using trusted processor features to create the holy grail of verifiable delay functions: creating a function that verifiably runs for exactly the amount of time it says it has. Independent of any advances to hardware speeds. It obviously relies on the security of the trusted hardware features – be it enclaves or the AMD equivalent. But its an interesting concept… which got me thinking:

Registering a ‘name’ is basically just the earliest possible point in time that a name existed. If you want to prove who really ‘owns’ a name, then you just need to prove how long a person has ran a VDF on that name for. The longest run-time is accepted as the owner. The downside to this is that you can’t transfer names. But not every use-case needs transferable property records. On the other hand: if you adopt this scheme there’s some pretty massive benefits to it.

You actually don’t need any kind of ledger, database, or key-value system for this to function. Records can be completely distributed among peers since their validity is inherently verifiable (subject to an optional refutation protocol.) So that makes the name system highly scalable over a blockchain-based consensus system like ENS that needs history chains to function. All such existing name systems either rely on a centralized server (which costs money) or need coins to use them. This idea could be adopted p2p without the need for dedicated servers to maintain the naming system. Although the peers would need to keep their ‘clocks’ running inside the enclave – potentially something that can be outsourced if longer-term names are required.

I see this being a good use-case for quick named addresses in peer-to-peer applications. Where you want to use addresses in applications with friends instead of dealing with large scale IPs and meta-data.