Stefan Thomas Follow
Open-source developer and distributed systems advocate. Currently working on @Ripple and @In...
Aug 18 · 5 min read

“Let’s take extra care to follow the instructions or you’ll be put to sleep.
...and don’t forget Taco Tuesday’s coming next week!”

The Subtle Tyranny of Blockchain

Re-learning old lessons about shared state

The past months have become a new chapter in the evolution of blockchain technology. Ethereum’s fork in the wake of the DAO hacks. Bitcoin’s almost-fork in the wake of the (still unresolved) block size debate. All of this is leading to the growing frustration and even disillusionment of key figures in the crypto-currency community.

I left the Bitcoin community in 2012 for very similar reasons. In 2011, I was part of the group that helped Gavin Andresen design the Pay-to-Script-Hash (P2SH) feature. The design wasn’t very complex, it was backwards-compatible and provided crucial building blocks for improving Bitcoin’s security and performance.

> *In a blockchain, everyone has to think the same.*

Unfortunately, getting it deployed turned out to be very political. It was easy to extrapolate from this change to more advanced functionality still on the roadmap and get depressed about our chances to make important progress in the future. As the Bitcoin price rose, the number of stakeholders expanded and the amount of money at stake increasingly dominated the technical discussion.

Blockchains are systems of central state

With this context in mind, the recent situation with Ethereum is not surprising in the slightest. As a blockchain grows, the larger and highly vested user-base becomes more and more difficult to shepard. When combined with time pressure (i.e. the 27-day DAO split creation period), something had to give. There wasn't enough time to get the sort of buy-in and preparation needed to safely hardfork a system like Ethereum.

At the root of the difficulty in updating blockchains is the need to maintain shared state. In any protocol, everyone has to *act* the same. But in a blockchain like Ethereum, everyone has to *think* the same. Everyone's memory (also known as "state" in computer science terms) has to be exactly the same and evolve according to the same rules.

Shared state adds tremendous complexity and that has a big impact on developers: Blockchains are a pain to work with. Everyone who has done it knows what I'm talking about. The fact that blockchain has been largely ignored by major tech companies and embraced by the financial industry is partly because that industry has a relatively high tolerance for arcane and complex systems.

Harmony and consensus are valuable. If we didn't agree on who is president or how much money is in anyone's bank account, society would be unable to function. But harmony taken to the extreme becomes a detriment. In the Lego Movie utopia, "everything is awesome" only on the surface. Behind the scenes, there is tremendous diversity and a rapidly changing world, which doesn't match the established consensus.

So how do we find the right balance between too much consensus and too little?

Xanadu and the Web

I expect that almost everyone is familiar with the World Wide Web. That's probably where you are reading this very article. What you may not know is that there was a much older project, started all the way back in the 60s called Project Xanadu. Not only had Xanadu been around for longer, it also had a

significantly more ambitious feature set than the Web. There would be no broken links in Xanadu and two-way links would be possible as well.

There are many reasons why the Web won in the end, but I believe its stateless architecture was critical to its success. Both Xanadu and the web are decentralized, but the web was much simpler. All it required was a minimal protocol and simple data format. No interaction was needed between websites, which meant that they could evolve independently from each other, and rather than waiting for the Xanadu creators to add a feature, many features that users cared about could be created just by changing a website or a client.

> *Instead of blindly replacing centralized functions with blockchains, we should be thinking about ways to avoid having those functions be centralized to begin with.*

As active participants of the W3C and IETF, we're always fascinated by the process by which the technology powering the web is updated. For instance, HTTP 2 was implemented under the name "SPDY" by Google who happened to control a number of web servers (Google Search, Gmail, etc.) and clients (Google Chrome). The fact that one corner of the system can be updated and good ideas can eventually spread to the system as a whole has been essential for the Web's ability to keep pace with technological innovation.

A better way

What can the blockchain industry learn from Xanadu and the world of Web standards? Instead of blindly replacing centralized functions with blockchains, we should be thinking about ways to avoid having those functions be centralized to begin with. We need to build stateless protocols like the Web that can be incrementally improved upon in different corners of the system.

To illustrate what I am talking about, let's consider the example of payments. Bitcoin is a replacement for existing centralized ledgers like the credit card networks. This is arguably a great idea. But Bitcoin still has a lot of shared rules that participants **must agree** to. I need to be on board with using proof-of-work as the consensus mechanism. I need to agree to the currency distribution function. I need to be ok with the block size limit. I need to accept the lack of anonymity.

By contrast, in adding one more layer of abstraction, the Interledger Protocol allows me to choose a ledger that has the consensus mechanism, the currency, the performance characteristics and the level of anonymity that I like and still

seamlessly transact with someone who has made different choices in each of these categories.

"My ledger is going to be powered by love and rainbows!"

That doesn't mean that Interledger doesn't require any agreement —we still need a common data format for instance. However, these choices aren't going to affect me economically or politically nearly as much, which makes it easier to compromise. And, crucially, we don't share global state, so at least our thoughts can be—once again—our own.