IOHK | BLOG

A Crypto on the Edge of Forever

DECEMBER 28, 2017 CHARLES HOSKINSON 7 MIN READ

Now that the dust has settled after travelling to more than 20 countries, dozens of conferences, major events and community meet and greets this year, I've finally had the time to reflect on the progress of the Cardano project as well as some of the lessons I've learned. It's honestly been the most challenging year of my life, filled with drama, stress, death and some unbelievably cruel people. It's also been one of the most rewarding and joyful years, having had the chance to meet thousands of passionate and kind fans, technologists and scientists – I can see the inspiration that Charles Dickens had when he said it was the best of times and the worst of times.

The reality is that the internet and in particular the cryptocurrency space can be a really toxic place if you allow it to get to you. There were times after reading some blog post or comment on Reddit that I seriously questioned if this effort was worth it. I can understand why Mike Hearn left Bitcoin.

But I've never been here for the short term, it's always been the dream of finding a way to get financial services to the three billion people who don't have them using technology that was only a dream a generation ago. And I think we are making great progress there.

In January of 2017, Cardano was still mostly in a very early alpha stage. We had tremendous engineering difficulty getting Haskell, our DevOps and the new protocols such as Ouroboros and Scrape to play nicely together. Rather it was a constant learning curve of how to tame the three headed dragon of research, decentralized teams and exotic programming languages while managing the expectations of a huge community.

As an aside, Cardano has one of the fastest growing and most intelligent fanbases. We actively invited people who care about formal methods, peer review and functional programming to come and see what we are working on. These people aren't swayed by jargon or flashy marketing. They were born with bullshit detectors in their cribs.

I've gained significant strength and a much needed boost in morale from interacting with our community. For example, one member asked about how we were verifying the proofs in the Ouroboros paper and I posted a link to Kawin's Isabelle repo. Most would simply say 'that's nice' and move on. This member took the time to read the code and mentioned we had a long way to go with specific examples.

For most people, Isabelle is a name followed by a lake in Minnesota. For our community, some can actually read the code and comment on it. That's a rare gift and it's the privilege of a lifetime to be in this kind of environment (we ended up hiring the person who commented on the code).

Moving through the months, Cardano moved from the lab to a series of testnets to eventually being released in September. Dealing with these transitions gave us a newfound appreciation for just how many different computer and network configurations exist. I can almost feel a Windows force ghost whispering "I told you so" in a smug voice.

We designed Byron (the September release of Cardano) to be the minimum viable product necessary to test the concepts Cardano is built upon. We wanted to run Ouroboros in a production setting to see epochs function properly. We wanted extensive logging of both the edge nodes and relays to see how our network is being used. We wanted to have third parties play with our APIs and tell us where we screwed up (boy did they ever!). We wanted to test the update system a few times.

Overall, the experiment has been a tremendous success. There are several thousand edge nodes concurrently connected to the network. There are several exchanges and other third parties using our software in the harshest possible way. There is a wealth of data flowing in that is giving us a much better sense of what we need to do to make Cardano better.

Since launch, we've already pushed three updates to the network without incident. We've started a very rapid redesign of our middleware and its associated APIs to make it easier for third parties to integrate. We've started a series of systematic improvements to our network stack that will be finished with the Shelley release that should dramatically improve things.

However, what excites me most about 2018 is that Cardano is starting to open up to the world. Delegation and staking will be rolled out all throughout Q1 and Q2 in coordination with the community. Soon we'll have a testnet running IELE allowing developers to play around with our smart contract model for the first time. And we'll be deploying our first verified protocol with Praos thereby engaging the formal methods community.

Constantly living in the moment, one tends to eschew Cardano's vast scope in exchange for the problem of the week. But looking at our ever growing Cardano whiteboard series demonstrates how many brilliant people wake up every morning thinking about how to solve the problems of scalability, interoperability and sustainability. These aren't just hypothetical lectures. They are backed by papers, funding and developers working full time.

Then there are the new things. The work by Professor Rosu and Runtime Verification on K and semantics based compilation isn't just really smart competitive differentiation, it's literally moving the chains of the entire field of programming language theory. The Cardano project is creating a financial incentive to have correct by construction infrastructure from virtual machines to compilers. Our success means you don't have to handwrite this code ever again – not just in a cryptocurrency context but in a general context.

Our research efforts at Tokyo Tech under Professors Mario Larangeira and Bernardo David with multiparty computation is rapidly bringing these protocols into practical use. Kaleidoscope and Royale are case studies on how to achieve everything that Ethereum does off chain, in a low latency setting, privately and at a scale of millions of concurrent users each in their own domain. Further abstractions will push this work into more useful domains like decentralized exchange. And eventually DApp developers will be able to integrate these protocols into their code via libraries.

Professor Bingsheng Zhang's research on treasuries and voting is groundbreaking. It gives our project the ability to open a discussion about how changes to cryptocurrencies should be proposed, debated, approved and funded. What's most special here is the interdisciplinary nature of the effort that can draw from political science, game theory, sociology, open source software governance and computer science. There is something for everybody.

Moving into 2018, we are going to open this discussion up by both engaging the community directly and by holding a conference in Switzerland. More details will be published later, but the basic idea is that this area isn't a Cardano problem. It's a cryptocurrency problem. And there are many great projects from Dash to Pivx who are trying to solve it in a novel way. We ought to talk to each other.

I could continue to enumerate our research efforts (there's a lot more to write), but I think the point has been made. Cardano isn't a cryptocurrency as much as it is a movement of minds who are frustrated with the way technology works in practice.

The functional programming community has for decades had great solutions to many of the problems plaguing modern developers, but they have been historically ignored. Our RINA guys, if given a chance, could build a much better and more fair internet. Layering protocol development with formal methods extracts a much cleaner and more meaningful design process where ambiguity and hand waving is slain.

What Cardano has given us is a chance to answer if only the world worked this way with why not? We have the freedom to dream again and the freedom to try new things without asking permission. I even have a chance to work with my heroes like Phil Wadler. 2018 is going to be one hell of a year.

Thanks for reading.