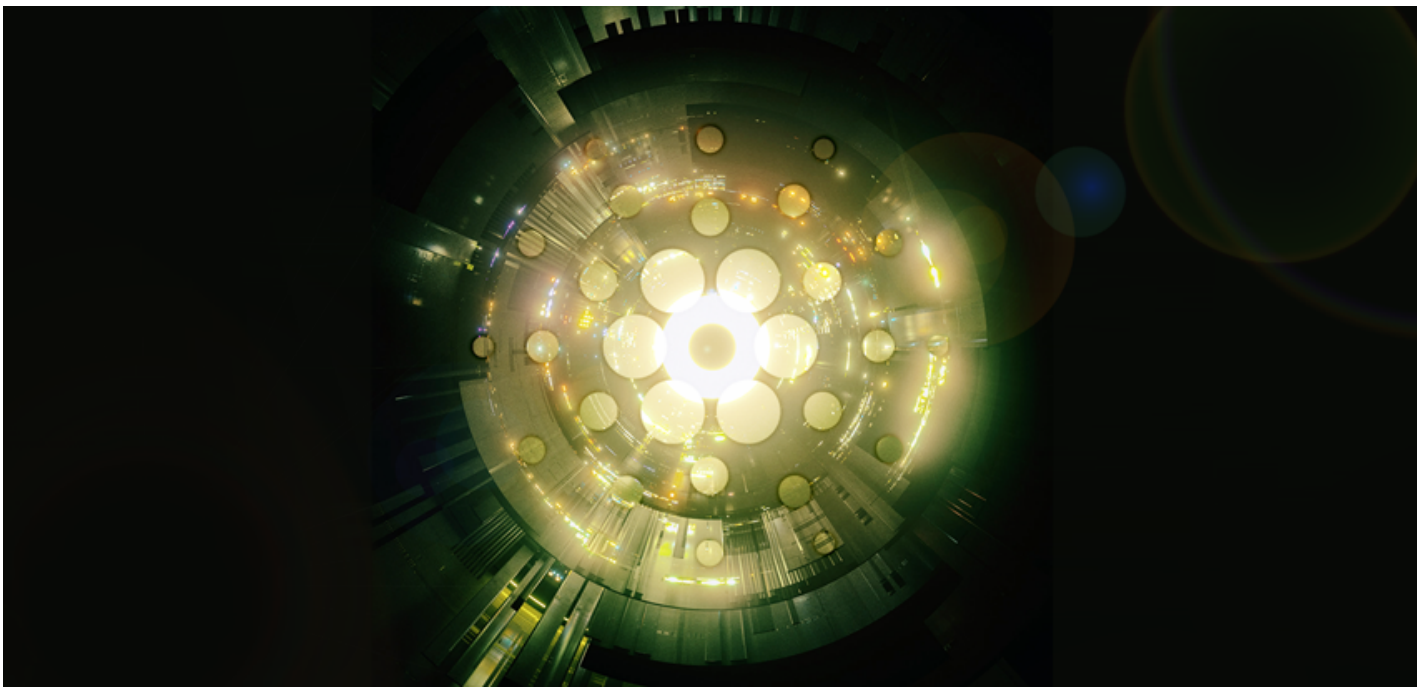
IOHK | BLOG

Cardano prepares to launch

Development during the past weeks has strengthened the network

SEPTEMBER 01, 2017 5 MIN READ



Developing Cardano is no small feat. There is no other project that has ever been built to these parameters, combining peer reviewed cryptographic research with an implementation in highly secure Haskell code. This is not the copy and paste code seen in so many other blockchains. Instead, Cardano was designed with input from a large global team including leading experts and professors in the fields of computer programming languages, network design and cryptography. We are extremely proud of Cardano, which required a months-long meticulous and painstaking development process by our talented engineers. With that in mind, I'm pleased to report that we are finally reaching the end of development.

We had originally planned to launch by the end of August, so there have been a few additional weeks of development. The extra time was partly due to our team uncovering a few unexpected bugs which delayed testing of the overall network. It also took longer to set up Cardano's internal test network than expected. But during those extra weeks, we have also been able to make enhancements to dramatically improve Cardano's performance. One of the things engineers did to improve Cardano's performance was to change the format of messages that are sent between nodes on the network. We upgraded our binary serialisation format from a custom version to one based on an open, common standard that means third parties, such as exchanges, will find it easier to build their own nodes, and our system becomes more transparent.

In recent weeks, engineers also made improvements to the network layer, rewriting code to make it run faster. The system is more stable under load and the number of transactions per second is higher. We are further improving the transaction speeds of the network and in the coming months after release will demonstrate our results. These two improvements took a few weeks to fully implement and test.

We have now added additional protection against DDoS, or distributed denial of service, attacks. The network's core nodes have been placed behind firewalls, so they are not accessible from the public internet. This gives us some protection against this type of attack, because potential attackers can't reach Cardano's core nodes. To do this, we surrounded the core nodes with proxies, called relay nodes, which by contrast are visible to the internet. As their name suggests, these nodes relay messages to the core nodes. Even if there was an attack, the blockchain would be protected because the core nodes are not directly exposed.

We have also made Cardano's delegation scheme quantum computer-resistant. With the predicted advance of quantum computers, public key cryptography that is commonly used today could be broken. So we had to think about how to future-proof Cardano's delegation scheme, which keeps the network running even if its end users are not online. To be resistant to quantum computers public keys cannot be published, only a hash of them. Cardano is based on proof of stake, so the solution is that Ada holders will have separate public-private keys for their coins and for their stake and the public key for the coins will not be published.

While all this work was going on during the past few weeks, the team has done a lot more testing, which is always good. We found bugs, which we fixed, and the testing gave us a better assurance of quality.

Recently, IOHK research – our Ouroboros and SCRAPE papers – were also accepted to two major conferences, ACNS in Japan, and Crypto 2017 in the US, and we were very proud our work has been recognised by the academic community and has been peer reviewed. A major exchange that has agreed to list Ada at launch has also been integrating with Cardano's network. As a result, we have been adding some recommended features and minor changes.

All this development work has meant that Cardano's code has changed, sometimes significantly. That means everything has to be retested. You can't simply update code and assume that everything will be fine. The process of releasing a new version of the software takes a couple of weeks because that is how long it takes to test, and fix bugs and carry out tasks such as preparing new installers.

Development has been a lengthy process but we are now very pleased to share a detailed plan showing the launch countdown. Cardano is a unique and very special product and we look forward to passing it into your hands.