Hi this is Charles Hoskinson, the chief executive officer of IOHK. This recording's purpose is to talk a bit about the Cardano project, where we're currently at, talk about some of the delays that have happened, as well as where we're going in the near future with more information to be released in text form soon

So first we're getting ready for the 5th version of the testnet, it's a major update, it's the first time that anybody has done an HD wallet using curve Ed25519 (elliptic curve). It also implements TLS (Transport Layer Security), some new transaction formatting, and a whole bunch of other features under the hood, and a tighter integration between daedalus and cardano itself. The purpose of this testnet release is to get testnet as close as possible to mainnet so we can begin the process of getting the mainnet prepared and launched.

Currently we are calling mainnet launch "Byron", and we're hoping to get the mainnet launch out sometime during the month of july to the month of of august. That's our best estimate with our current development resources. We're a bit behind schedule and I wanted to get this recording out to explain what's happened over the last months, some good, some not so good, but we've been able to overcome all of it.

First off, the Cardano sale that Attain put on which was audited by the CF was a tremendous success. There were over 14,000 sales, with about 10,000 unique people who went through KYC and AML. In the process of going through that, an enormous amount of data was generated so the databases that retained all this information had to be checked for accuracy, things like duplicate accounts or inaccurate information and so forth, and when the sale came to an end in january most of the month of february was spent doing a post-mortem on the sale, cleaning up the data, as well as closing up the 4th tranche's sales audit. Once this was done we moved on to the month of March to actual vending.

So what was Vending? Vending was a process where we launched the cryptocurrency, in this case it was RScoin, and we used it to issue tokens so that ppl would have balances connected to actual cryptographic assets. Usually this is done with Ethereum tokens like ERC20 but at the time Cardano was proposed Ethereum had yet to have been launched, so our original vending strategy was to use a smaller blockchain that was built for this specific purpose. That's why we implemented RScoin. We managed to get it operational in early March and we spent most of the month of March vending people. Approximately 93% of the buyers went through vending, and the other 7% were what were called force vended, where we simply generated the certificate on their behalf and sent it to them.

From that point we had to verify that the vending was done correctly and that people could indeed redeem their certificates. So the next version of the testnet was loaded with the genesis block that will be loaded into the mainnet, and we sent out numerous emails asking our buyers to go ahead and redeem their vouchers that they vended. In about mid april this version of the testnet was launched and since that time almost 3,000 people have redeemed their ADA purchases on the testnet. We've also some integrity checking and other such things.

We're about 8 weeks behind where we wanted to be in the development lifecycle. We were originally planning to have Cardano's mainnet ready around March to may was our initial estimate. Several factors caused the delay. The first factor was a research factor where we invested more resources in benchmarking, stress testing, and refactoring our whitepaper and ultimately the design of Ouroboros, the heart of our system, so it would be suitable for academic publication and also that we could survive peer review, and this endeavor was successful. So part of the good news is that Ouroboros is the first cryptocurrency protocol to ever be accepted as a PoS algorithm to Crypto 17, and we'll be presenting that at Santa Barbara (California, USA) in August.

Second, the code language that we used to create Cardano is called Haskell. Haskell is a very complex language. It is mostly used for academic projects although it has in the last decade found industrial applications. We chose Haskell because we feel that ultimately it will give us the fastest and easiest pass towards formal verification and specification of our underlying protocol. While this is of course true, the downside is that Haskell is still a bit immature for certain libraries and certain core technologies, especially on the development ops (operations or devops) side. So we ran into many hurdles over the last few months as a consequence of this and we've had to clean up and improve libraries, we've had to clean up and improve development processes, and we've also had to refactor our devops to make things work, well especially while deploying clients to the windows environment because unfortunately this is where Haskell has its greatest degree of immaturity. The good news there is that while it has cost us additional time, we've managed to overcome those problems and build up a really robust set of processes, better software, and a pretty good team that's been able to overcome most of the challenges.

Another delay was in respect to some cryptographic primitives. With Cardano we chose to use a different elliptic curve than the one that was used with Bitcoin. Bitcoin uses a curve

called secp256k1. It's a great curve and it has many applications and many libraries and it has been very successful. Unfortunately, this curve is not optimal for some applications that we wanted to use so we decided to use a different curve called Ed25519. No one had ever created an HD wallet for Ed25519 although there exists a very good specification that appears to be reasonable. So part of our delay was actually doing the hard work of implementing an HD wallet for this particular curve and then getting that implementation properly audited. As there are only a small handful of experts who are capable of doing this, we had to wait for those experts to become available to look at that code. Those experts were based in a place called RPI sec, it's Rensselaer Polytech Institute. So given that that took some time, we spent that time to get this done for the assurance of the ADA users and we're very confident that the work has been done correctly. The upcoming testnet will be the first release of the HD wallet, as well as a release of some new network improvements as well as TLS and a whole bunch of other things that we've put into the protocol.

A final delay stems from the architecture that we've chosen for Cardano. The architecture was a three tiered model where we'd have a Haskell based server running on the backend, we'd have a pure script type bridge, and then we'd run a copy of what's called electron which is a combination of both Chrome and Node. This architecture is incredibly robust because it gives us the ability to leverage everything in the Chrome and Node ecosystem, to use Javascript for our user experience as well as a lot of our user interaction logic, but then it also allows us to use Haskell for all other mission critical software. The challenge though was combining this architecture together you have to make everything talk correctly. This took quite a bit more than we had anticipated, especially because the developers themselves have different domains of competencies.

The developers working on the Daedalus side are mostly javascript developers, and the developers working on the Haskell side are mostly Haskell developers and there are cultural, knowledge, and technological differences between these two sets. We had to bridge that gap and bridge those cultures, yet we were able to find a way to do that. Now all that has been said, we've overcome a lot, we've grown tremendously. IOHK now operates three research centers: one at Tokyo Tech, one at University of Edinborough, and one at University of Athens. These centers have many great cryptographers who do phenomenal research and that research is focused on Cardano and we're really excited to see where that's going to take us.

So where do we go once the mainnet has been launched? What does the mainnet mean?

First it means that people will be able to redeem and trade the ADA that they have purchased. Second, they should be able to download, install, and send transactions with ADA using the Daedalus wallet and also verify those things on our blockchain explorer and other assets. But more broadly it means that we're now in a position to iterate on a live cryptocurrency. The way we develop software, the processes we have, all of these things will change over time, and throughout this year we'll continue to add more robustness and value to the Cardano ecosystem. We're going to publish a roadmap shortly which will outline major milestones. We've named the milestones on Cardano SL, that's the layer where ADA lives, after poets, so we have Byron being the release for the mainnet, and the next release this year will be Shelley, which will contain a lot of upgrades that allow interoperability and vast improvements to scalability. And then later next year we have two more upgrades which will serve as completing the SL layer, whereas the computation layer (CL) which is where smart contracts will run as well as things like gaming and gambling, as well as regulated activities, we anticipate two releases next year. One close to the beginning of the year we're calling Backus and that will focus on our next generation EVM, adding special purpose MPC for games and gambling, as well as a full version of our new programming language we developed for high-assurance smart contracts called Plutus. The second version which is called Milner will focus on trusted hardware as well as scalability improvements and also improvements to the standard library and the App development experience.

Our roadmap will cover these things in much more detail but the purpose of this recording is to assure everybody that we are now finally executing really well. I'm sorry for the delays. I know they're tough. I've been there, and believe me it's been tougher on me than anybody else because we've been coordinating a team in more than 10 countries and we're incredibly eager to get Byron out and get something before everybody. I will also remind everyone that we've only had so far 3.000 people redeem their ADA on the testnet. We would really love for as many people as possible to download Daedalus, redeem their voucher on the testnet, because this gives us a higher assurance that their certificate is OK, that nothing hurt during vending, and they can actually install and use the software. If they can't install and use the software it would be better to know that now than later when the mainnet launches because we have less options and opportunities to fix things. For example if there are corrupted certificates and the buyer did not choose the recovery option, there is no way to get the ADA back. So it's incredibly important, especially for those buyers, that they go ahead and redeem their certificate on the network, the testnet, to verify they can because this will be their only opportunity to do so, and have us potentially be able to do

something about it prior to the launch of the mainnet.

The other thing is that we'd really like to know user stories as well as user configurations, so we'd like to know how many mac users we have, linux users we have, windows users we have, the version of windows, the underlying hardware and so forth because this gives us better data on the systems we should focus on, as well as what our devops team needs to plan for as we get closer and closer to mainnet.

I hope that answers and addresses some of your questions and again we'll be releasing more information soon, as will the Cardano Foundation, and this month is going to be a busy one and next month will be even busier. Thank you so much for your time and your patience and I'd like to thank you all and have a nice day.