Fenbushi Interview with Dominic: the great vision of DFINITY's internet computer

Remington from Fenbushi Capital had a conversation with Dominic Williams from DFINITY. The following is the content of the interview.

Rem: DFINITY is known as a more volatile sibling of Ethereum, a more revolutionary version of it.

Dominic：The Internet Computer — stewarded by the DFINITY Foundation — represents the third major innovation in blockchain. Ethereum is a marque example of building a simple blockchain in an open source manner. Since the Internet Computer is a new type of advanced blockchain computer with infinite capacity and performance that rivals the traditional cloud, we cannot crowd source cryptography on GitHub — we need to build a world class R&D organization with the world's best cryptographers, distributed systems engineers, programming language experts, etc.

Rem：What are DFINITY's technical advantages compared to the public chains that challenge Ethereum (EOS/Polka/Algorand/ETH2.0, etc.)?

Dominic: Most of today's blockchain infrastructure projects are attempting to build a faster Ethereum… and we're confident only the Ethereum community will build a better Ethereum with ETH 2.0. Bitcoin created a magical financial ledger in cyberspace via simple script attached to coins (aka, digital gold), and (2) Ethereum created programmable crypto currency by having coins attached to units of code called smarted contracts. Now, DFINITY created the Internet Computer and will spin it out as part of the public internet, providing the world a revolutionary blockchain hosting unlimited data and computation "on-chain" to easily build scalable dapps, DeFi, websites, enterprise systems and open internet services of the future.

In its application, the Internet Computer differs from Ethereum, as we aim to host all of humanity's software.But, Chain Key Technology makes this all possible — something Ethereum doesn't have.

Rem：When DFINITY breaks through the boundaries of the blockchain, it seems to be subverting the traditional Internet. We see that DFINITY has made progress in benchmarking traditional Internet applications (LinkedIn, TikTok), with Linkup and CanCan respectively. From the perspective of users and developers, what are the advantages and disadvantages of these apps compared with traditional Internet apps?

Dominic: On the head because you will find easier to create a high scale internet service like a TikTok on the internet computer. Then you will build it on Amazon web services using traditional legacy IT technologies. And I like to say you're gonna be able to create hyper scale internet services in less than a thousand lines of code. And indeed, there are many lines of code in CanCan that works similarly to TikTok. So all of those things are great. I think the first of all,internet computer is a very compelling platform when comparing against legacy IT. However, if you're entrepreneurs/ teams of developers/ investors, there are even more compelling reasons to build on the internet computer. Namely you can do a whole lot of new things that you cannot do if you build in a traditional way.

So first of all, if you build something on the internet computer, you can create open internet services. You can create something like CanCan in a form where it runs autonomously as part of the fabric of the internet as it is controlled by a tokenized governance system. Now there are lots of reasons that's cool. Users may like the fact that the internet services controlled by an open tokenized governance system because it makes the service transparent and they can gain confidence . For example, we all know about the scandals relating to Facebook and its practices of exposing data to people. Open tokenized governance system provides users with guarantees that is not gonna happen. But from the developers and entrepreneurs perspective, there are enormous benefits. For example, you can sell the governance tokens to raise money.

It's fact that vast majority of the world's technical talents reside outside silicon valley. I'd probably say that 99% of the world's technical talents reside outside of silicon valley. And outside of silicon valley is much harder to raise venture capital. I know because i've been an entrepreneur for some decades And I was an entrepreneur in Europe before I moved to California some years ago from now. And I can tell you it's much easier to raise venture capital in silicon valley against based in London. And I'm sure if you're based in other parts of the world, it's even harder. So if you're an entrepreneur, investor or team of developers, and you want to develop an exciting new internet service, I would suggest you look into open internet services on the internet computer, because if you create a fantastic prototype, you can make that prototype into an open internet service. You can now raise money for further development by selling the governance tokens. And you can do that from anywhere in the world.

So one of those exciting parts of this whole project is we think we're going to unleash worldwide technical talent by giving access to funding. So that's already a very compelling proposition for entrepreneurs, investors, and teams of developers because if they produce something that's compelling, they can get something. That's just the first thing. The second thing is that you can do new things on the internet computer that give you really substantial competitive advantages. So perhaps the most obvious of these is tokenization. Okay, so let's say you wanted to create an open Uber or an open Didi, let's call it open rights. One of the challenges is how you gonna get early drivers and early riders on to your Open internet services. Tokenization provides a solution.One of the simplest ways you might approach the problem is dispersing open governance tokens to early riders and early drivers. But you can workout by using much more imaginative and effective schemes. But even the very simplest scheme is pretty compelling. For example, if you don't stop offering rides on the open internet service, you may be rewarded through governance tokens.

There are other advantages, too. Since internet computer as part of the fabric of the internet is created using autonomous software and its control configured and upgraded by the open tokenized governance system, and it's not owned by any particular person or company, If you create something like open rides, it provides other advantages. For example, my hometown in England, Uber can't provide services. And the reason is that the local municipal government banned Uber to protect the local taxi monopoly. And I was made acutely aware of this a few years back when I had to go somewhere in the rain and I couldn't just press a button to bring Uber to me. I actually had to run half a mile to the taxi rank and stood there for a few minutes and arrived at my destination completely soaked.

Now if you create something like open rights, open internet service equivalent to Uber, first of all, you can use tokens to motivate early drivers and early riders. You can also go into territories where are traditionally difficult to operate because these municipal councils cannot sue the internet and can't sue something that's equivalent to blockchain. And in fact the municipal council would have to focus their attentions on the riders and drivers themselves, which is a much more difficult thing to do. So certainly that can be an advantage. But there are many other ways you can do really cool things.

I'll give you another example. I don't know if you use Google photos, but it popped me up. Google already said, they would never lock your photos. And you can upload all the photos you wanted to Google photos and they never locked them in. That was their promise. That was a pretty good deal has to be said. And all my photos from Google photos, however, you may realize that sort of started to change how things work. And until recently you could actually sink your photos to your drive, so you have one copy of your photos in Google photos, another copy on your laptop. Now, Google has stopped that. So for that was stage one, stop people to sink their photos to the computer. The only way of getting your photos is to download individually.

The second thing is, if you get Covid and find yourself in hospital for a while. And if your credit card expired while you're in hospital, when you come out, you could find all your photos disappeared. This kind of things become already a big problem where somebody dies for some reason and their relatives won't get access to photographs in their accounts. There's some really sad stories where people have just lost their entire set of family history as recorded by photographs. So what could you do with an open internet service? This is where blockchain creates just a much more interesting platform for building new internet services. Let's say you wanna build Open Photos. What you could do is to integrate with Defi system that enables people to make one deposit that gives them lifetime or infinite host. For example ,as a user,I want a terabyte of photo storage. Once you made that deposit, you've got that terabyte storage forever. How would that work? Essentially, when Open Photos received the deposit, it would use marginal lending schemes to earn interest; and the interest would be used to pay the cycles which are about underlying hardware costs. That's a really cool feature.

Another example is on the internet computer, you can non-revokably share APIs. That means you can trustlessly share functionality and data with other services using something called permanent APIs. This means something called service composability. Essentially, Open Photos can provide APIs that other developers and entrepreneurs can trust. So those other developers and entrepreneurs can create extensions that enable uses of Open Photos to apply a much wider range of fields/ filters because one team can never do everything and that's why permeant APIs support. Another important aspect is security. So the internet computer doesn't work like a traditional blockchain. Private data stays private. You don't have to worry about hackers looking at your photo collection. And you may have heard just a few weeks ago some white hackers got into apple and they were able to see everything in icloud. That's a particular concern to a lot of young people. They don't want their private photos looking out onto the internet. Open Photos is able to provide this kind of guarantees to its users not only because Open Photos cannot be hacked, but also because even developers and designers of Open Photos themselves, cannot see users photographs. That's pretty compelling.

Lastly, give you the full picture. we actually moved Linkedup to CanCan, which is a tTikTok clone. And the reason we did that is we wanted to show how the internet computer can store extra bytes of user data on chain and expose the internet computers and network of blockchains under the skin. And it has very clever technology that makes it possible for these different blockchains related. But anyway, we decided to develop CanCan because it was more challenging. We wanted to show people how it's possible for users to update and upload exa bytes of data to this blockchain system and therefore this blockchain app can stream that data back to users and show people how the programming framework on the internet computer made it much easier to develop something like TikTok. But actually, the next set of features that we're putting in now are related to tokenization.

So very basically it works like this: every user of CanCan can super like up to 10 videos every 24 hours.If a video of CanCan goes viral, CanCan examines the ordering in which super likes were made. So users who are very good at super like content, their content will become viral earlier on and collect a lot of reward points. What can they do with these reward points? There's something called a drop day. On a drop day, you can exchange rewards points for CanCan governance tokens. And you could probably further exchange those governance tokens for cash.In addition, you can exchange those

rewards points for prizes offered by sponsors. So you can imagine clothing brand will offer prizes in exchange for reward points. And then those brands that are offering prizes can use those reward points to pay for advertising.

Finally, this is an idea we just stole straight from China.Users can show their appreciation for producers of videos by sending red letters for reward points. So if you see someone doing some extreme sports and you want to encourage them, you can press the red letter button. It sends red letters for award points. Or if you see someone do a dance and you wanna courage, you can do the same thing. So we think you can only do this kind of thing on the internet computer, because open internet service that's autonomous is akin to a blockchain which runs autonomously as part of the internet. You can use this type of advanced tokenization strategies. And we believe by applying tokenization strategies into CanCan and incorporating things like defi, something like Open Photos can give people eternal photo storage in exchange for the deposit. Using tokens as incentives for something like open rights can motivate early drivers and early riders to take part. And we think these kind of features combined with better guarantees that the internet computer can help people stay private from hackers. We think all of these things together make the internet computer extraordinarily competitive.

Rem: I don't know about other developers that maybe watch this at some point, but you just really blew my mind with all the sort of different possibilities of what can be built on the internal computer. I think developers will be able to build scalable internet applications directly into the fabric of the internet, be able to build open governance systems and be able to raise money. As you said, small entrepreneurs will be able to get access to funding, security, privacy, and storage capabilities.

And there is some stigma around building on traditional blockchains because for the average user, there's a lot of friction about the user experience. And you mentioned something earlier about reverse gas model, where a user might not necessarily need to have deposit. I was wondering if you could share a little bit more about the mechanisms that may make Dfinity help developers build applications more user friendly and make it easier for mass adoption?

Dominic: Yeah, I think the reverse gas model is very important. There are some challenges with using traditional blockchain architectures to create compelling consumer apps. I think Crypto Kitty is a good example. First of all, Kitty is very popular within the block chain community. As a result, usage went up, but the capacity of the ETH chain is fixed. Once the capacity of the ETH chain was exhausted, it took people several hours to get their transactions through Crypto Kitty And the project faded away after that-the lack of scalability created a very firm ceiling on how far crypt kitty could go.

I've had experience of building a massively multiplayer online game that grew to some millions of users. And it wasn't a world beater by any definition, but include some millions of users. It was pretty successful and it gave me a taste of how competitive the game industry is. And if you want to create a game that scales to millions of users, you have to optimize what we call the funnel. The funnel is a sequence of events that occur when a user hears about your game, then visits your website or downloads the app, then tries engaging with right the way through becoming a paying customer.

What i learned is that you've got to remove friction from the funnel. And in very competitive consumer industries of games industry, people spend a lot of time just optimizing that funnel because they know the smoother the funnel, the less friction, the more viral their game will be. But can you imagine what would happen if you had to ask the average consumer to acquire tokens before they play your game? So you should create the best game in the world and stick it on blockchain, a scalable blockchain. But if players had to acquire tokens before they could play, you just wouldn't be able to compete and grow. It seems to tell the user you can stop playing before you actually could start playing. You have to Binance to buy some tokens, work out to sign ledger wallets and such kind of stuff.

that's why the internet computer has reverse gas model .So, on the internet computers, smart contracts are charged with these things called cycles, which are equivalent to gas. And they pay for their own computation and memory, which is where data is. And that means you can create services on the internet computer that the user can interact without having tokens. Now, if you're using tokenization mechanism, as we just talked about,actually you can introduce tokens. But you don't actually introduce in a straight way. You can allow users to interact with your service over the web or via smartphone and get comfortable, or create an account and get engaged on and later on engage with tokenization features.

Rem: I think this concept of variety is probably a sensitive word this year. But applications sort of being viral really depends a lot on on reducing friction, making it as easy as possible and getting as many users as possible on board with the least numbers of efforts. So I think this reverse gas model definitely solves one of the big pain points of existing blockchain.

You can also provide users with a variety of ways to authenticate themselves. Since the internet computer has obviously a 3rd case cryptographic signature which is difficult to use, you can allow users to choose traditional username and password, the jobs script inside the web browser or the apple smartphone. User apply seed phrases to these name passwords to generate a key pair, which signs messages. That's one option. So if you want, it's possible to create internet services on the internet computer, whatever it is social network, game, crypto exchange.you can create something that allows users to login user password, which behind the scenes is converted to a cryptographic key.

Or you can enable them to use web3. And web3 is a new standard that's integrated with the hardware of phones and laptops, and also can be used for things like Ledger wallets. For example, you can have internet service and open internet service on the internet computer where users sign in by biometric on the phone or laptop. And in this case, the private key pair they're using to authenticate is kept inside a trusted execution environment, like a hardware on clave, some special temp-proof chip inside their device, which is equivalent to a ledger wallet. So for example, if you've got a MacBook laptop, you're probably familiar with using the fingerprint sensor to authenticate certain things. For example,if an open internet service is a social network, and when users dedicate themselves just by pressing the fingerprint sensor which locks there.

For us, it's very important that not only you can build all these kinds of things on the internet computer blockchain network, but also set new standards. Like for developers, we want to provide them with a better environment for developing these things in which they could ever get on Amazon web services using legacy IT. We also want to enable developers and entrepreneurs to provide better user experiences and supporting things like tokenization and so on, these you can't get in legacy IT. The way to make the user experience smoother, for example, is enabling people to get user names and passwords passed and login by pressing the fingerprint sensor on their laptop or do the equivalent on that pixel or iPhone. It is not only easier to use, but also more secure. I think that kind of thing is very central to the internet computer project.

Rem: Absolutely. I think this is a very important aspect that a lot of people don't think about. I think having the convenience of a standard of Google and hanging with Facebook bottom are such cool things. I think that will be a huge breakthrough for any application for replacing passwords and so forth. I think the most exciting milestone coming up is Mercury. I think this means that Dfinity will be formed in watching to the public and share with the listeners and viewers. What does this milestone mean for the internet computer project? And what will come after Mercury? what are the next steps on the road map after it passed this important milestone?

It's tremendously exciting that we got this far, and it's taken a lot of effort. We found we did decentralized fund raising in February 2017. So it's taken a long time and it's glad that we're finally getting to this point. But we know things are still happening slowly.

The internet computer is many times more complex than a normal blockchain. And that's why we've got this huge team of the world's best research scientists and engineers. So Mercury is important. So that's actually a process. There are several sub stages: the sodium network is gonna become Mercury network this year in December at some point, that will involve some parties being given what's known as neurons. We've got the single network nervous system that manages that way and some independent parties been given neurons and control of the network will pass over entirely to nervous system.

Nervous system （BNS） is capable of fully managing the network and can create sub networks. It can split sub networks, decide on which sub network are assigned work, repair some networks and so on. The neuron system is gonna take over responsibility for the network. Now, that doesn't mean the Dfinity Foundation is in anyways stopping work. So that's just the first phase. The second phase of Mercury will happen sometime in February next year. In the second phase of Mercury, we're gonna declare what we called The Alpha public network to be the beta public network. Something called the genesis contract will be activated, which will allow people to claim tokens and withdraw them to neurons. It is very likely that the token will go live on financial exchanges around the world, and that will be the bigger launch. I think the Mercury, which is in December, will happen quite quietly. It'll still be important for people because once we've passed that point, the network will no longer be reset.

So if you're building things on the internet computer, they won't be reset when we pushing upgrade. So one of the absolutely extraordinary things about the internet computer network and technology is that we can update it in place. For example, new iterations of the software that encapsulates new version of the protocol can be proposed to the network nervous system. You can actually roll that out across nodes in data centers around the world without interrupting service, which is really incredible. And that gained into technical details. That's one of the most complex pieces of the technology. The reason why it is important is that other organizations are gonna be enabled to continually push improvements into the network. The foundation is not for profits, its only purpose is to develop internet computer technology and promote the success of the network. And according to what we are allowed to do, our aim is to increase spending every year. And we're obviously already have the best team and the best cryptography team in the world, even compared against massive organizations like IBM. But we intend to continue scaling out foundations. And there are duties of other new organizations that are coming into being ever more aggressive with our spending. For us, this is just the beginning. So Mercury is a very exciting milestone because it's taken a lot of work just to get the point that we can actually hand over the reins of nervous system.

The Alpha networks launching is gonna transition to the Beta network and the genesis contract will be activated. But that's just the beginning. We're not gonna stop. In fact, we're actually going to continuously expand our efforts forever as far as we can.

Rem:Yes, absolutely. On one hand, Mercury marks the combination of sodium for five years' tremendous amount of work. And i am glad to hear Dfinity will be able to launch Alpha network into open governance system. On the other hand, you're absolutely right. It's just the beginning. I think that's all the sort of endless possibilities that we discussed earlier in this call,will be able to build on open and scalable internet computer. I think there's such a lot of possibilities ahead that we're all very excited about what comes next and where the network takes us after the launch. I'd like to thank you so much for taking the time and sharing today. I think that it's always good to catch up, hopefully next time we can do this in person. But I would like to say we're all very excited to see Dfinity reach this important milestone and look forward to all endless possibilities to come.