ceocfointerviews.com

Issue: April 2, 2018

CEOCFO Magazine

Q&A with Rob Leslie, CEO and Founder of Sedicii Innovations Limited using the cryptographic protocol Zero Knowledge Proof to provide an Identity Verification Platform for Authenticating People to Websites, Call Centers, Social Media Monitoring and Authorizing Secure Card Payments

Rob Leslie
CEO & Founder
Sedicii Innovations Limited
www.sedicii.com

Contact:
011 353 51 302181
rob.leslie@sedicii.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Leslie, what is the concept behind Sedicii Innovations Limited?***

Mr. Leslie: Sedicii has developed a technology based on a cryptographic protocol called Zero Knowledge Proof (ZKP). The simplest implementation of a zero knowledge proof is where two parties who have a piece of information want to prove to each other they have the same piece of information, but neither wishes to disclose that information to each other. Therefore, I can prove something and keep all of my information private, but I am still able to prove to the other party that the information they have is what I have, or not, as the case may be. We have used this technology to essentially build an identity platform that allows organizations who hold information about people; your name, your date of birth, your social security number and so on, to prove to each other that they have the same information about you, meaning it is consistent, or they do not. The thinking is that there are organizations who have high trust, for example, Government agencies, the Social Security agency, Passport agency and the Driver's License authorities and so on. If they say to you, "Yes, what you have presented to me is the same as what we have," then I know that I can trust the information that I have.

CEOCFO: ***How does the technology work?***

Mr. Leslie: The technology works on a simple, twenty questions style process, but all in a mathematical, very fast process. In real terms, the process takes less than a second. However, it asks a series of questions and gets a series of responses to those questions. If, in every scenario, the answer to the question is "yes" I am able to deduce that what I am talking about is what you think I am talking about. It therefore, must be the same thing because a very high probability says it must be so. As a simple example, just imagine that what we are talking about is a yellow duck, so you are thinking about a yellow duck and I am thinking about a yellow duck. In order to satisfy both of us that we are talking about the same thing I would ask a series of questions that never expose the information about the duck. I would ask questions like, "Is it yellow," and you would say, "Yes." "Does it have wings?" "Yes." Does it quack?" "Yes." "Does it have a beak?" "Yes." "Could you use it in the bath?" "Yes." Gradually, the pool of possibilities is starting to shrink to the point where, hopefully, there is only one logical outcome, yet nobody has told anybody what we are talking about. Yet, we have been able to figure out, mutually, that it is a yellow duck without sharing the information itself.

CEOCFO: ***Would it be your own information, such as where your mother was born and some kind of security question you would typically get?***

Mr. Leslie: No. The mathematical process underlying all of this is cryptographic. For example, let's assume I need to confirm your date of birth. Our process turns the piece of information into something that looks like a Rubik's Cube; a randomized pattern that is completely unique to that piece of information. It does that for both parties who are claiming to

have knowledge of this piece of information. Essentially, the challenge is to prove that the pattern on the Rubik's Cube I have is the same as the pattern on the Rubik's Cube that you have. Yet, neither of us can exchange the Rubik's Cube in totality with each other. So, I prove that the information is the same by testing permutations. A permutation would be, "is the top left-hand corner on the front face yellow and the top right-hand corner on the top face blue." When I apply that challenge to the Rubik's Cube, the answer says, "Yes, it is," therefore the response to the challenge is true. If I send the exact same challenge across to you on your side and you test it with the Rubik's Cube that you have and you respond to say, "Yes, mine does the same thing." Therefore, I now know that I have got a partial match. If I repeat that process ten, twenty, fifty or one hundred times and every time I get a true answer back, the probability that those two Rubik's Cubes are the same rapidly approaches one hundred percent. It never gets there, but it gets so astronomically close that the only logical outcome is that the two things are the same, so the information on which both of them are based must also be the same.

CEOCFO: ***How much time would that take?***

Mr. Leslie: For the process to work, it happens in milliseconds. Therefore, it is less than a second for each check.

"The "a-ha moment" comes at different points, because different things resonate with different people. There is a ninety-nine percent chance that you will commit a cybercrime and you will get away with it Scott free. If we can crack it, I feel we will have left something behind that will last the test of time."- Rob Leslie

CEOCFO: ***Where are the best applications for this technology or is it virtually anywhere that an idea is needed?***

Mr. Leslie: It is useable virtually anywhere an identity verification is needed. However, at this moment in time, we are very focused on organizations who have a regulatory requirement to prove identity. Therefore, banking and finance would be one area of particular interest where I have to prove to my bank that I am who I claim to be. Today I do that by providing a copy of my driver's license, a copy of my passport or a copy of my national government issued ID with my photograph in it and maybe a utility bill that has my address recorded on it. Today, the bank will take those pieces of information, generally at face value. "It looks like a passport and therefore it is and I trust it." However, the problem is that there are many really high quality fake documents floating around. Equally, there are many stolen identities floating around. Therefore, how is a bank able to discriminate as to what is real from what is fake? The way we are looking at doing this is by being able to verify information that I give to my bank with the issuing authority using zero knowledge proofs. Therefore, my bank gets my permission to verify my passport or my driver's license with the driver's license issuing authority of the state, or the passport agency. After performing the check the passport agency says, "Yes, what you have is the same as what we have." Now the bank has confirmation that it is a verified, true ID. However, we go a step further. We also say that rather than the bank taking a photocopy of my passport or my driver's license, what if the state issuing authority created a digitized version of that document and made it available in the form of a secure, digital information token. Therefore, I am just sharing this token with my bank so they can get the information, whenever they want, through a secure, trusted interaction with the state agency. However, my information is not stored in the bank anymore. The only organization that has it is the state driver's license authority or passport agency, because they are the issuer and I have given them my permission to release it to the parties that I deem appropriate to have it. Therefore, there is a consent mechanism built in. There is 'privacy by design' built in. There is data minimization and because of that you now have massively reduced the risk that the information can be stolen, because it is now only held by the authorities. It is not held by all of the parties that hold it today. We have created an ecosystem that now works on tokens rather than real information constantly floating around.

CEOCFO: ***What is the buy in from the agencies? What has been the response that has to agree to this?***

Mr. Leslie: Right now, we are at the beginning of this process. We have had some trials here in Europe with a national passport office, for example. The passport office themselves love the technology for a number of reasons. The first is that they are able to interact with their customers. They have a consent mechanism through a mobile app that exists on the user's phone, where they are always able to communicate with their customer. The second is that they love the capability of being able to know who is relying on the official document. In the case that I just described, it would be a bank. Therefore, if something happened to the document, for whatever reason, they could just tell the bank, "Sorry, the customer's passport has expired or it has been reported lost or stolen, you can no longer rely on the document you have."

Then the passport office would just make available the new one when it is issued, with the consent of the customer, because the issuing agency can now talk to them.
The problem we have had is that, as we all know, governments work very, very slowly and they have lots of big bureaucratic processes. Therefore, if we can get the process in front of decision makers it is an obvious decision to want to do this. That is because it is in everyone's best interest. It is in the government's best interest, because they control the visibility of the information. It is in the citizen's best interest, because their information is now being passed only with their permission and they know who has it and from the customer's perspective, the information is being minimized in the sense that not everybody has it, if they do not need to have it. The risk of theft has been vastly reduced because it is not available everywhere to steal anymore. As I said, there is a win, win, win for everybody participating in the process. However, getting to the decision makers is a real challenge!

CEOCFO: ***You have been involved in a fair number of previous ventures. What have you learned?***

Mr. Leslie: Obviously, education and publicity is one. You have got to try and convince people that this is a good thing and that they need it to solve a real problem and I think we are doing that well. Being able to talk to people like you Lynn and getting our message out through publications and through social media and through other channels is an extremely important activity for us. Therefore, educating the marketplace has been tremendously important. Getting some advocates; early adopters who are batting for us, again, is extremely helpful. For example, as a Global Technology Pioneer with the World Economic Forum, who are a tremendous organization for putting global thought leaders together, I am working with a number of groups on collaborative activities to solve really, really big problems. The identity problem in the world is one of those. Through this forum I am able to talk to big technology companies, to governments and financial institutions about how we can work together to bring technologies like the zero knowledge proof we have created to help solve these problems. I am convinced that we are far stronger working in collaboration than we are at working in competition in this scenario, because it is in everyone's best interest to make sure that happens.

CEOCFO: ***How would you implement if an organization wants your service?***

Mr. Leslie: The first thing they have got to do is identify the data that they have. Do they have personal identity information that may be of value to their customer? Let us say it is a large retailer, Walmart for example, because it is the biggest, and they have lots of customer information. Do you know what information they have that is of value to you? I would say not but it would be great to know what they have. I am sure Walmart would be happy to interact with you, their customer, to be able to verify that information to help you manage your personal circumstances. Therefore, we provide a suite of tools that allows the conversion of the raw data into the abstract "Rubik's Cube" format that I mentioned earlier to allow verifications take place, for which you get paid. We abstract all of the information so that it is no longer sensitive. Essentially, it is a secure, cryptographic mathematical process. We do this for every organization that claims to have the same piece of information about you. We then use what we call a zero knowledge proof verification engine, or ZVE for short, that sits in the middle of all of this and learns what organization has what information about you; not what the information itself is, just where it is; and whether it matches the data that you claim to be the truth "Walmart has my first name, Walmart has my last name," so that I can match that piece of information with someone else who has claimed to have the same piece of information. The results are provided to whomever wants to verify the data, with your permission. One of the things that we are looking at is to try and create a commercial model that incentivizes the citizens, the consumer in this case, to want to participate. Therefore, just for arguments sake again, if Walmart was verifying my name and address with a utility company they might pay a small fee for that. Part of that fee would be paid to me, the consumer, as a royalty for my participation in the process. Over time, because there are an awful lot of these verifications happening, that small micropayment could turn into something more substantial. Then, for the first time I am actually deriving tangible economic value that I can spend, which might be in the form of coupons, it might be air miles, it might even be cash that I can take from an account and go and spend somewhere.

CEOCFO: ***Are you funded for the time and effort that is going on at the moment?***

Mr. Leslie: There is an awful lot of effort going on at the moment and we are definitely under-funded! To date, we have raised one million dollars and we are in the process of raising another two million dollars at the moment to keep activities going and to start this collaborative activity that I mentioned earlier. What we are trying to do is very big and very challenging, which means it is very risky. Investors like big problems because there are big returns to be made, but they are not so keen on big risks, so there is a trade-off there. However, if there are investors that are reading this article and would like to have a deeper conversation, I would love to have that conversation with them.

CEOCFO: ***When you talk with someone about what you are doing is there an "a-ha moment" when people understand? Are there typical questions that people have that you can get out of the way early?***

Mr. Leslie: Most definitely! However, the "a-ha moment" comes at different points, because different things resonate with different people. For you, you just said the security aspects of this resonated with you. For others, it is the opportunity to derive some form of meaningful, tangible value from their personal data; that resonates with them. For example, for governments it is the ability to know who is relying on a credential, a passport or a driver's license, that immediately resonates with them. Therefore, it is trying to create a suite of these sweet spots, where you have got a bit for the government, a bit for the consumer, a bit for the service provider, a bit for the relying parties and everybody gets something that is actually appealing if we can do it successfully. So far, we have been doing well. We just need to scale what we are doing to a much larger level and build an alliance. Eventually, when we have some big companies working with us, who have got a much broader reach than we have, we can cover many more people in a much shorter space of time.

CEOCFO: ***Given that it is a long haul, why did you decide to create Sedicii and go down this road?***

Mr. Leslie: That is because I experienced an online fraud about six or seven years ago, where I bought a camera and what I thought I was buying was not what came. I tried to get restitution and it did not work, but I had nowhere to go. Therefore, I just said, "The internet is broken." We fundamentally do not have enough trust in this system. I needed to be able to find who the retailer was who was selling my product and I had nowhere to go to actually find out who the person was. If you can create this identity layer that sits on top of the existing internet structures where, with judicial oversight and proper legal structures provided by the authorities, where, if they suspect malfeasance of some kind they can get involved and identify who the participants are, then we have solved a huge problem! Cybercrime is a massive issue and it is just getting bigger, because frankly, it is just too easy to commit a cybercrime. There is a ninety-nine percent chance that you will commit a cybercrime and you will get away with it. That is because it is just too hard to prosecute that crime today and to try and find out who the perpetrators of it are. This is why it is growing at an exponential rate. Therefore, we have got to address this problem as a society. I just felt, when I had this personal experience that I had to do something to try and address it. I had no idea when I started that it would turn out to be this big or this challenging! However, as more time has gone by, I actually feel even more strongly about it today than I did when I started, that what we are doing is absolutely in the best interest of the global community as a whole. If we can crack it, I feel we will have left something behind that will last the test of time, hopefully.