New technology will fight infectious diseases by outing fake diagnostic tests

July 24 2018, by Karl Gruber

Credit: CC0 Public Domain

Some shady people are profiting from making fake tests to diagnose disease like malaria or HIV. Now new technology is providing a level of protection.

Infectious diseases are still a big problem in some parts of the world. A recent study estimated that, in 2016, more than 8 million people died because of infectious diseases like HIV or malaria.

Most of these deaths occurred in developing countries, and one important way to combat these diseases is through prevention. In fact, it has been estimated that 1.2 million deaths from malaria, tuberculosis and syphilis could have been prevented each year in these countries if accurate diagnostic tests had been used.

Portable diagnostic tests allow for the quick identification of major diseases like malaria, tuberculosis or HIV. They are life savers in many parts of the world where infectious diseases are still a major problem. They help detect infected people quickly and prevent the spread of the disease by providing quick and accurate information to decision makers.

Sadly, a lot of these tests are now being falsified in different ways by people wanting to make a quick buck.

Anything from blood glucose test strips, blood tests and even vaccines are counterfeited by crooks in different ways. They might change the expiration dates or sell an HIV test as tuberculosis test.

But now there's a new technology, developed by IBM in Switzerland, offering hope for a safer future. The technology, which is nothing short of amazing, ensures the origin and content of virtually any consumer product from diagnostic tests to medicines to food.

Intelligent diagnostics

The new security technology, called crypto-anchors, involves the use of microfluidics—a technology that uses microscopic amounts of liquids to perform all kinds of functions.

The idea is to create a unique security code that is very hard to falsify yet easy to apply on any diagnostic device, such as those used for malaria or HIV detection. It can be attached to anything from a malaria test to a pill. For example, crypto-anchors can be embedded into edible magnetic ink used to dye a pill, then the code could become active and visible with a drop of water. This lets the consumer know the pill is the real thing. Good luck to any crook trying to copy that.

"Crypto-anchors integrate a security code in the test area of the diagnostic devices that is unique to each device and non-reversible. The test area then has a dual function in that it performs the biochemical test and simultaneously authenticates the device," says Dr. Emmanuel Delamarche, a scientist at IBM headquarters in Zurich.

In addition, this security code can also be scanned by a smartphone to track the history of the device being used.

The new security measure is different and more secure than traditional methods, such as product numbers, barcodes and QR codes, Emmanuel explains. These security approaches are commonly falsified.

"Among fraudsters, it is common practice to falsify labels and expiration dates on diagnostic tests for diseases such as HIV, malaria, dengue fever or Ebola and resell them on the black market," says Emmanuel.

So how does it work?

Imagine you are doctor in Kenya who needs to do a blood test for malaria and you have one of these fancy new devices.

The first thing you need to do is get your smartphone and scan the code on the device. Then, using your phone, you send the code to a remote database, called blockchain. This will verify the validity of the data on

that code.

The blockchain is online and is managed by all parties involved in the use of these diagnostic devices. This means extra protection if anyone wanted to make changes to the device.

"To make any changes to the blockchain requires consensus. So if one party wanted to change the expiration date for the malaria test, all parties would need to agree, which isn't likely. That is how it can't be faked or altered," Emmanuel says.

Once you have scanned the code on the diagnostic device, the blockchain will confirm the validity of the device, providing all kinds of details. For instance, it would tell you when the device was manufactured and in what country it is supposed to be used.

Now that you have verified the device, you do the blood test. As soon as the blood enters the device, the crypto-anchor code does the rest.

"If someone tries to recreate the pattern, it will not pass verification from the blockchain," Emmanuel explains.

The technology not only works but is also cheap. It doesn't cost more than a few cents per device, according to IBM. As long as you have access to the internet or a mobile phone network, you are good to go.

Crypto-anchor diagnostic devices are not yet available, but according to IBM, they are currently discussing their development with major manufacturers.

This article first appeared on Particle, a science news website based at Scitech, Perth, Australia. Read the original article.

Provided by Particle