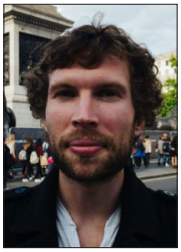
FRONTIER TECH INVESTOR
CRYPTO WIRE

ISSUE NO. 6 SEPTEMBER 2018

In this issue:

Moment of clarity

Harry Hamburg, Editor



"I was sitting here eating my muffin and drinking my coffee and replaying the incident in my head, when I had what alcoholics refer to as 'a moment of clarity'."

– Samuel L Jackson, playing Jules in *Pulp Fiction*

If you've seen *Pulp Fiction*, you'll know exactly what "incident" Jules is referring to.

If you haven't, well, I won't ruin it. But suffice to say, it was serious enough to make him rethink his most closely held views and decide to change his path in life.

As he said, usually this "moment of clarity" happens to alcoholics or addicts. But it is actually much more universal than that.

These profound moments surface in all our lives. Something happens – usually something that could have ended your life – and it gives you a whole new perspective on the world.

These moments of clarity tend to be life changing. It may cause a person to end a marriage, change careers, start a family, give up destructive behaviours or relocate to another country.

I'm sure if you haven't had one of these moments of clarity yourself, you'll certainly know people who have.

The one thing they all have in common is they cause a paradigm shift in a person's behaviour, which usually blindsides many people who know them.

My question for this month's *Crypto Wire* is, what happens when an organisation, an industry, or even a whole society has a moment of clarity?

Because over the last few years, and the last few months in particular, events have been lining up, pointing to a potential paradigm shift in the way we view our privacy.

And, as I'm sure you can guess by now, a number of crypto projects are laying the foundation for this shift to take place.

When it does, the way we interact with businesses and institutions will be forever changed.

And as you'll see today, that time is fast approaching.

Privacy is a dirty word

The only people who need privacy are paedophiles and terrorists. If you want privacy you must be one or both of those things.

This is the standard rhetoric of all mainstream political parties.

If our lives are kept private, if the government cannot pry into them at will, we will be subject to more terrorist attacks and more innocents will be abused.

These arguments are absurd, but they work. They work so well, in fact, that they are effectively unchallenged.

And every time a new terrorist attack takes place, or a new abuse scandal surfaces, it sets up the stage for even tighter controls on our lives.

Just this month, Five Eyes – which couldn't sound any more like a hellish organisation from a dystopian nightmare if it tried – demanded backdoors be put into encryption.

If you're not familiar with Five Eyes, it's an intelligence alliance between the UK, the US, New Zealand, Canada and Australia – the Five Eyes.

Here is what Five Eyes said:

> *Many of the same means of encryption that are being used to protect personal, commercial and government information are also being used by criminals, including child sex offenders, terrorists and organized crime groups to frustrate investigations and avoid detection and prosecution.*

Can't forget to mention those child sex offenders and terrorists now, can we Five Eyes?

Its statement continues (emphasis mine):

> *The Governments of the Five Eyes encourage information and communications technology service providers to voluntarily* ***establish lawful access solutions to their products and services*** *that they create or operate in our countries.*

Translation: tech companies need to start putting backdoor access into their encryption to give us access.

And what will happen if these tech companies don't "voluntarily" create backdoors in their encryption?

> *Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions.*

They will be taken to court. Who will win those inevitable court cases, it's hard to say. But I would hope it wouldn't be Five Eyes.

Big Tech is having a hard time this year, people have woken up to how their data has been harvested and used against them (as I wrote about in last month's issue). But if Five Eyes got its way and broke encryption, things would get a whole lot worse.

When the only tool you have is a hammer, the whole world looks like a nail

I don't believe organisations like Five Eyes are inherently evil.

I'm sure the people that work for them truly believe they are "the good guys". And I'm sure they would argue that by taking away our freedoms, they are actually protecting our freedoms.

When your entire existence is based around thinking up and trying to stop potential security risks and terrorist attacks, you will inevitably think anything that makes this easier for you is good for society in general.

I'm sure they would argue that if putting backdoors into encryption means they can stop even one terrorist or catch even one child abuser, it will be worth it.

And on one level, they would be entirely right.

However, this kind of thinking misses the bigger picture. What these agencies don't realise is that by putting backdoors into encryption, they would bring entire industries to a halt.

In fact, scratch that. They would bring the entire world to a halt.

Do not temp me, Frodo!

What Five Eyes and others like them don't realise, is the very systems they rely on to do their important work rely on encryption. If backdoors were put into encryption (which would be a virtual impossibility in itself) they would no longer be able to do their jobs.

All their intelligence and top secret documents would be out there for the world to see.

Terrorists would have access to location data on government figures.

Money would be drained from bank accounts because hackers would have easy access.

And IT systems around the world would go down.

Emails would be leaked, money would be stolen, criminal records changed, court rulings edited, cash machines hacked... you get the picture.

The problem is, these agencies are operating under a false assumption.

Here's what they don't seem able to grasp. If backdoors are created for them, hackers *will* eventually get access to those backdoors. And once they do, any system that uses that encryption would be hacked.

And given that our systems are all so interlinked, once hackers get access to one system, the next one becomes even easier to get into.

The whole situation reminds me of a passage from *The Lord of The Rings*.

When Frodo leans how powerful and dangerous the "One Ring" is, he tries to give it to Gandalf, so Gandalf can take care of it. But Gandalf knows that even he could not resist an evil like the One Ring.

> *"You are wise and powerful. Will you not take the Ring?"*
>
> *"No!" cried Gandalf, springing to his feet. "With that power I should have power too great and terrible. And over me the Ring would gain a power still greater and more deadly."*
>
> *His eyes flashed and his face was lit as by a fire within.*
>
> *"Do not tempt me! For I do not wish to become like the Dark Lord himself. Yet the way of the Ring to my heart is by pity, pity for weakness and the desire of strength to do good.*
>
> *"Do not tempt me! I dare not take it, not even to keep it safe, unused. The wish to wield it would be too great for my strength. I shall have such need of it. Great perils lie before me."*

The power to break encryption at will, to be allowed a backdoor into the structures that hold our essential IT systems together... that is like wielding the One Ring.

And whether you trust Five Eyes or not, if that backdoor was breached by hackers – which it eventually would be – they would wield a power "too great and terrible."

The trouble with central control

And it's not just me that knows hackers would eventually get though. It's an opinion also held by the head of the UK's National Cyber Security Centre, Ciaran Martin.

While being interviewed about the British Airways hack on Radio 4 last week, he stated: "You've got to assume that some of these things are going to get through."

If you're not aware, British Airways was hacked this month and thousands of customer details were stolen. Not just names, addresses and passwords, but people's credit and debit card numbers, too.

Customers have been told to cancel any cards they've used to pay British Airways recently, which is a huge headache.

Although the British Airways hack was small potatoes compared to last year's Equifax breach.

Hackers obtained personal data on more than 150 million Americans and 15 million Brits held by the credit-rating agency Equifax.

And not just basic data. This was in many cases social security numbers, names, addresses, driving licence details and phone numbers.

All that personal data was sitting in one centralised database. Compromise one key computer and you get access to everything.

Incidents like this are why when, Mark Carney, the governor of the Bank of England, was asked what he believes are the biggest threats to the financial system, he stated cybersecurity.

Why?

"Because financial systems are so interconnected," he said.

Now let's connect some dots.

Look at what Martin said and look at what Carney said. Put them together and we have the following.

Hackers are going to get through, and when they do they will be able to wreak havoc on the financial system because it is so interconnected.

And why is this? Because all this data is centralised and because none of it is really private.

You break into one database, say like British Airway's or Equifax's, or any governmental one, and you get access to thousands of people's personal details.

In the case of British Airways, that will be credit card and maybe even passport details.

In the case of Equifax it can be names, addresses, social security numbers, etc.

And in the case of the government – well, thanks to the Investigatory Powers Act, it may have records on every email, text message and website you've visited in the last few years.

Privacy's moment of clarity

Okay, so we've established why privacy is so important. And that it's not really about keeping our communications away from prying eyes, but about keeping our societal structures in order.

Now let's bring it back to the idea I opened with, the moment of clarity.

The "incidents" have been piling up.

It's not just data breaches, but also how our data is being used.

I wrote last month about the problem of online advertising and how our data is harvested, sold on and used against us.

But it's not just advertising. It's the very systems we all use in our day-to-day lives.

A year or so ago barely anyone thought about all the personal data they had granted Facebook access to. Now you can't move for hit pieces exposing Facebook, Google, Amazon et al's shady data practices.

The tide is changing.

People are taking a step back and gaining a different perspective on privacy.

With every hack that happens, with every data scandal, with every Big Tech misstep, the need for a different approach to privacy is highlighted.

Basically, we need to stop sharing our personal information with companies and institutions alike.

That way, when *they* get hacked, it doesn't matter to *us*. They lose money, but we don't lose anything. We don't end up paying for their mistakes, as we currently do.

Here's how it will work.

Proof without proof

One of the key developments in crypto is zero-knowledge proofs.

These basically let you prove you have certain data without ever showing anyone that data.

So, say you want to prove you're allowed to leave the country to British Airways, but you don't want it to have your passport details on file, in case it gets hacked again.

Instead of giving British Airways your passport details, you give it proof that you own your passport and are able to fly.

Without giving your actual passport details, this may sound impossible, but it's not.

Or say you ring a call centre to transfer money between your

bank accounts.

Instead of giving the call operator your name, address, account number, etc, you just give them proof you have all of that information, but you never give them any of the information itself.

If the call operator is looking to steal your money or sell your information on, they can't. They don't actually have any information on you.

This proof all happens automatically, you don't have to do anything. You just log in to your identity app.

This means you can prove your identity to any company without ever giving them any information about yourself.

If they get hacked, it doesn't matter. They don't actually have any of your personal information, just a line of computer code that proved you are who you say you are. The hacker can't use it for anything.

It sounds like magic, but it's actually very simple.

How zero knowledge works

This is the simplest example I've seen on how zero-knowledge proofs work.

From Wikipedia:

> *Imagine your friend is colour-blind and you have two balls: one red and one green, but otherwise identical. To your friend they seem completely identical and he is sceptical that they are actually distinguishable. You want to prove to him they are in fact differently-coloured, but nothing else, thus you do not reveal which one is the red and which is the green.*
>
> *Here is the proof system. You give the two balls to your friend and he puts them behind his back. Next, he takes one of the balls and brings it out from behind his back and displays it. This ball is then placed behind his back again and then he chooses to reveal just one of the two balls, switching to the other ball with probability 50%. He will ask you, "Did I switch the ball?" This whole procedure is then repeated as often as necessary.*
>
> *By looking at their colours, you can of course say with certainty whether or not he switched them. On the other hand, if they were the same colour and hence indistinguishable, there is no way you could guess correctly with probability higher than 50%.*
>
> *If you and your friend repeat this "proof" multiple times (e.g. 128), your friend should become convinced ("completeness") that the balls are indeed differently coloured; otherwise, the probability that you would have randomly succeeded at identifying all the switch/non-switches is close to zero ("soundness").*
>
> *The above proof is zero-knowledge because your friend never learns which ball is green and which is red; indeed, he gains no knowledge about how to distinguish the balls.*

Within blockchain these zero-knowledge proofs have moved on and can now work without any interaction between the person providing the information and the one verifying it.

If you want to know more about how this works in detail, you can read Zcash's page on zK-SNARKs here.

There is no data to hack

And now to come back to Mark Carney saying that cybersecurity is one of the biggest threats to the financial system because of how interconnected everything is.

Well, zero knowledge solves this problem. With things like zK-SNARKs, institutions can work together and process transactions without ever putting each other at risk.

If one got hacked, it would only be its data at risk. It would have no knowledge of other institutions' data.

With blockchain and zero-knowledge proofs, data breaches become virtually impossible.

I'm sure eventually, people will work out ways to hack even these systems. But one thing is for sure, they are a whole lot more secure than what companies are using right now.

The need for privacy in cryptocurrencies

As I said zK-SNARKs can be used to prove information without handing over any information.

These were first developed by Zcash, and Ethereum is working on integrating them into its protocols.

This would mean you could transfer Ethereum anonymously, which is essential for any kind of payment system.

As it stands, when you pay for something with, say, bitcoin or Ethereum, the vendor would be able to see your full account balance and every other account you've ever used in conjunction with that account.

This may be fine when you're working with a big, reputable store. But what about an eBay seller, or a pop-up bar, or a street vendor?

Your entire wealth is basically out there for anyone to find and then come and come and take from you with violence.

This is why anonymity in cryptocurrencies is vital if they ever want that "real world adoption" we hear so much about.

Secret smart contracts

Okay, now here's where this all gets really interesting.

As I've written many times before:

- Blockchain 1.0, like bitcoin, enabled trustless transactions.
- Blockchain 2.0, like Ethereum, enabled smart contacts.

Smart contracts mean you can build entire systems on the platform. You can program it.

And last year, one crypto startup called Enigma promised the next step in this evolution. Private smart contracts.

This essentially means companies can compute and manipulate data, without ever really gaining access to it.

So, for instance, people's medical records could be used to help with medical trials, without the company conducting the trials ever getting access to the records.

How does it work?

Enigma has a fairly succinct explanation in its white paper:

> *Enigma is private. Using secure multi-party computation (sMPC or MPC), data queries are computed in a distributed way, without a trusted third party. Data is split between different nodes, and they compute functions together without leaking information to other nodes. Specifically, no single party ever has access to data in its entirety; instead, every party has a meaningless (i.e., seemingly random) piece of it.*

So basically:

- The data is split up into such small pieces that it is meaningless.
- These pieces are distributed to nodes on the network.
- When all the nodes work together they can perform computations on the data.
- But on their own, they can do nothing with it.
- And if one or more nodes were hacked, the data hackers would get would be meaningless.

This would mean you could, for instance, send your medical data to a drug company, and get paid for doing so, while remaining anonymous.

We are still so early

All the new developments in crypto inspire each other.

First, we had bitcoin. The main issue with using bitcoin as a currency – other than the bottleneck in transactions per second – is that it is not private.

Now we have Monero, Zcash and others which offer privacy, and solve this major issue.

In terms of privacy coins, by far the best implementation I've seen is Monero. If you never read my long *Exponential Investor* article on Monero, you can find it here.

However, Zcash's privacy system, although not as good for currency as Monero's, has other uses – as I have shown earlier.

So, Ethereum is now implementing Zcash's privacy functions into its blockchain. As with most things Ethereum – scaling solutions, proof of stake, sharding, plasma, etc – this is "coming soon".

I have no doubt all these things will be implemented. But they are taking longer than many people had hoped and this is one of the reasons Ethereum is struggling right now.

(Just as an aside, as I'm writing this Ripple has once again become bigger than Ethereum by market cap.

Just as it did for a brief period last December, Ripple is sitting pretty at the number two spot on coinmarketcap.com. By the time this issue goes out, I imagine Ethereum will have taken back second place. But maybe it won't have.

Still, it's good to see a top ten crypto gaining 60% in a day again. It almost feels like the wild price rises of last year. Almost.)

And now we are even getting secret smart contracts, with Enigma. The possibilities for this technology are ground-breaking. Secret smart contracts could finally allow us real ownership of our own data. Plus, the ability to lease it out for a profit.

Meanwhile, most of the world still thinks of all cryptos as merely bitcoin. It's true the average person on the street has now heard of bitcoin. But a smart contract? No way. And a secret smart contract? Not a chance.

It's going to take a while for the mainstream to catch on to all the possibilities cryptos offer. When it does, I fully expect the highs we saw in early January will be easily surpassed.

But, for now, we should remember just how early we are.

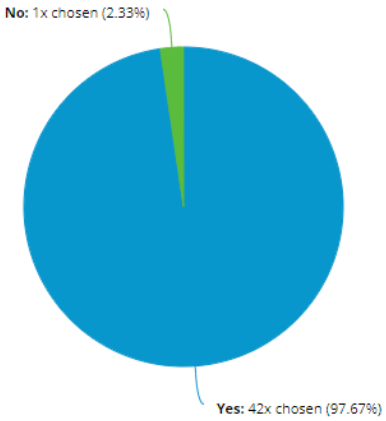
Blockchain will change almost every computer system we use today, in almost every area of industry. But it's not going to happen overnight.

You could see being this early as either a bad thing or a good thing. A bad thing if you despise uncertainty. And definitely a bad thing if you've invested more money than you're okay with losing.

But a good thing if you see all

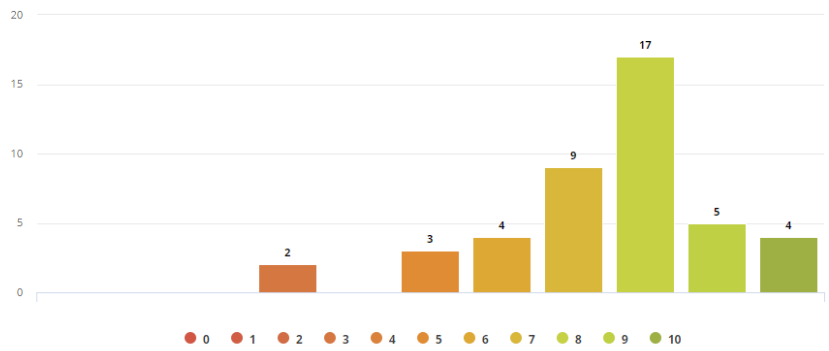
Do you think the online advertising model is broken and in need of fixing?

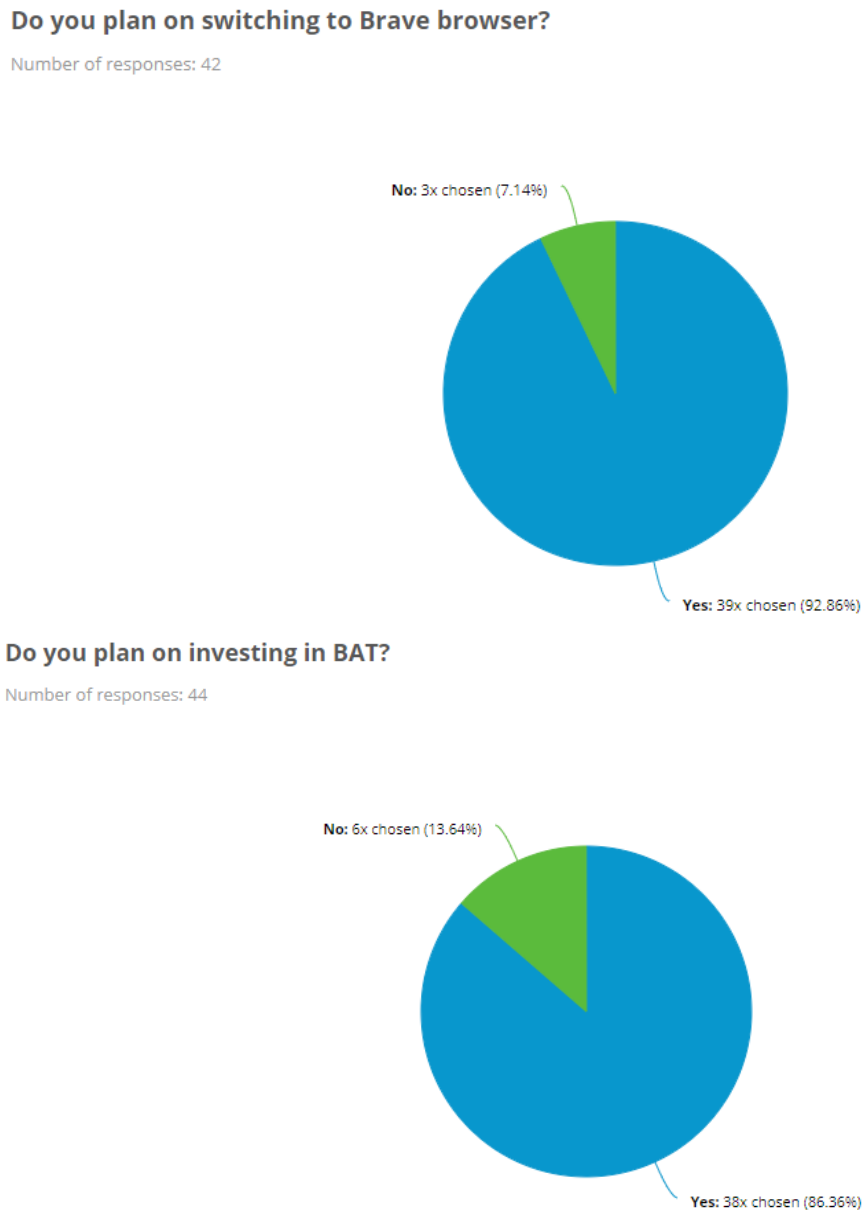
Number of responses: 43



On a scale of 1-10 how much chance do you think BAT has of fixing it?

Number of responses: 44





the potential on offer here, and just how world-changing this technology is. And definitely a good thing, I would imagine when you look back in five or ten years' time and remember where prices were today.

Survey results

Last month's issue was about the state of online advertising and how Basic Attention Token aims to fix it.

You can see the results on page seven and above.

I'm not sure who that one person is who likes the current model of online advertising, but it looks like you're on your own there.

I'm also hopeful Brave and BAT can do something to change the horrible state of online advertising as it stands today.

And they seem to mean business. Earlier this month the team behind Brave and BAT sued Google over Google's privacy violations.

From the Brave blog post on its law suit:

> *Every time a person visits a website and is shown a "behavioural" ad on a website, intimate personal data that describes each visitor, and what they are watching online, is broadcast to tens or hundreds of companies. Advertising technology companies broadcast these data widely in order to solicit potential advertisers' bids for the attention of the specific individual visiting the website.*
>
> *A data breach occurs because this broadcast, known as an "bid request" in the online industry, fails to protect these intimate data against unauthorized access. Under the GDPR this is unlawful.*

It doesn't really get much bigger than going after Google. Just imagine what will happen if Brave wins the case.

And just imagine the exposure this case could bring. Even if Brave loses, it should get a huge amount of press coverage as the case progresses. Which I know it was smart enough to realise.

Okay, that's all for this month. No survey today. I'm off to go re-watch *Pulp Fiction*.

Until next time,

Harry Hamburg
Editor, *Crypto Wire*