

BRITISH BROADCASTING CORPORATION

RADIO 4

TRANSCRIPT OF “FILE ON 4” – “THE MISSING BITCOIN BILLIONS”

CURRENT AFFAIRS GROUP

TRANSMISSION: Tuesday 6<sup>th</sup> March 2018 2000 – 2040

REPEAT: Sunday 11<sup>th</sup> March 2018 1700 - 1740

REPORTER: Geoff White

PRODUCER: Nicola Dowling

EDITOR: Gail Champion

PROGRAMME NUMBER: 17VQ6241LH0

THE ATTACHED TRANSCRIPT WAS TYPED FROM A RECORDING AND NOT COPIED FROM AN ORIGINAL SCRIPT. BECAUSE OF THE RISK OF MISHEARING AND THE DIFFICULTY IN SOME CASES OF IDENTIFYING INDIVIDUAL SPEAKERS, THE BBC CANNOT VOUCH FOR ITS COMPLETE ACCURACY.

“FILE ON 4”

Transmission: Tuesday 6<sup>th</sup> March 2018

Repeat: Sunday 11<sup>th</sup> March 2018

Producer: Nicola Dowling

Reporter: Geoff White

Editor: Gail Champion

---

#### ACTUALITY ON AEROPLANE

WHITE: A flight to Japan – the first step on the trail of the biggest theft in Bitcoin history. Tokyo is arguably the birthplace of the Bitcoin boom. It was here that the dream of a radical new type of money turned into a nightmare of hacking, theft and bankruptcy. The fall-out from it exposes not just the fragility of the industry behind Bitcoin, but the inability of global financial regulators to keep up.

#### ACTUALITY – JAPANESE STREET SOUNDS

WHITE: Here in Japan, trading in digital currency is fast becoming almost a national pastime. So much so that it's estimated almost half the world's Bitcoin trading is now done using the Japanese Yen. Its popularity has led to some pretty bizarre spin-offs, as I found out when I went to a tech trade show on the outskirts of Tokyo.

#### MUSIC – VIRTUAL CURRENCY GIRLS

WHITE: Virtual currency is so big here in Japan, it even has its own girl band – they're called the Virtual Currency Girls and they're on stage now at this cavernous exhibition hall just outside central Tokyo. There are six of them in the band,



WHITE: How are you doing? Good to see you.

BURGES: All right.

WHITE: Thanks for meeting up with us.  
We met on a flying visit to Japan. But back in 2013, he was a software developer living in the UK. When we found a quiet place to talk, I asked him how he got involved in Bitcoin.

BURGES: So, it started off around early 2013, when the price of Bitcoin started going a bit crazy. It went from \$20 to \$200 within the space of a couple of weeks. I was kind of looking for things to invest in. I had been looking at shares, that kind of thing, so I thought, wow, there is definitely a lot of potential if you can invest when it's like \$80 and then suddenly the next day it's at \$160. That's when I started getting seriously interested.

WHITE: The problem for folks like Kolin is, how do you get your hands on some Bitcoin? The simple answer is to use an exchange. It matches buyers, who want to put in their dollars, pounds etc, with sellers, who want to sell Bitcoin. And when Kolin was investing, there was really only one choice.

BURGES: Mt Gox claimed to be the largest exchange in the world by volume. They were obviously very world famous because I think they were basically the first exchange and yeah, they had been probably used more than any other exchange outside of China.

WHITE: So when you were looking to get involved in Bitcoin, Mt Gox was a natural choice for you really?

BURGES: Yes, that was what most people were using.

EXTRACT FROM ADVERT

VOICE: Magic is power. It has the capacity to create and destroy, manipulate ....

WHITE: Mt Gox got its unusual name from a card game set in a world of wizards, spells and monsters, called Magic: The Gathering. Players swapped cards on a website called Magic: The Gathering Online Exchange – MTGOX - or Mt Gox. In 2010, the site started dabbling in Bitcoin trading - at that stage, a real fringe activity. But it was great timing - Bitcoin's price boomed. And so did Kolin's investment.

BURGES: Over about two or three weeks, it went from \$50,000 to towards \$1 million in value. That wasn't necessarily what I got back out of it, but it raised to that value for a period of time.

WHITE: That's incredible. I mean, as somebody who is not involved in finance, you must have been looking at that thinking, this is really something.

BURGES: Er yeah, it was quite a shock, so I was at work doing contracting and watching as my money would just shoot up by \$10,000 one minute and then five minutes later another \$10,000 or whatever, and you are just like, wow, what has gone on?

WHITE: What Kolin and other investors didn't know was that Mt Gox was struggling - with regulators, with hackers, with the sheer volume of trading. Its Chief Executive, a 25 year old Frenchman called Mark Karpeles, was desperately hiring staff. But some new recruits found their boss's behaviour quite odd - even in the sometimes off-the-wall world of technology.

#### ACTUALITY IN JAPANESE STREET

WHITE: The company moved into shiny new offices in central Tokyo and it staffed up, employing a few dozen people, all of whom worked more or less directly with its idiosyncratic boss, Mark Karpeles. I'm on my way to see one of those ex-employees now.

GLUCKSMAN: I found myself in China studying Chinese and martial arts, then when I graduated I decided to try my luck and find a job in Japan.

WHITE: Originally from Essex, Thomas Glucksman had been drawn to Asia by a love of kung fu. His company seconded him to work at Mt Gox. He well remembers his first encounter with Mark Karpeles.

GLUCKSMAN: The first time I met Mark, I did not know he was the CEO. I saw him scrambling around, kind of fixing the lock on a door, apparently an electronic lock that he could radio control, that he had programmed and built himself. And he was kind of just scrambling around with a screwdriver and getting some wires and he was, you know, wearing jeans and a t-shirt. I assumed he was just the IT guy, you know, it was kind of like the guys from the IT Crowd. Really he looked like that, he was, you know, a little bit dishevelled and I had no idea he was the CEO of the company for about two weeks.

WHITE: As the money flowing through the company hit millions of dollars a day, there were signs the start-up was growing out of control. Thomas Glucksman says he and other staff feared Karpeles wasn't giving enough attention to a business which, by this time, was handling 70% of the world's Bitcoin trade.

GLUCKSMAN: He had an interesting passion for quiche.

WHITE: As in the flan, the dish quiche?

GLUCKSMAN: Yes, quiche as in like mushroom and onion quiche or something. The reason why I thought it was quite peculiar was erm, so it actually in the building that we moved to, Mark had also purchased space at the bottom of the building that was going to be the Bitcoin Café, and, you know, initially the concept was for that to be a showpiece for Bitcoin where, you know, you would come and you'd buy your coffee with Bitcoin, but then he had, you know, actually hired a chef who was a specialist in making quiches, and he'd invested quite a large amount of money in an oven that was specifically built to cook quiche. It's a quite a big distraction from the whole story of Mt Gox.

#### ACTUALITY OUTSIDE KARAOKE BAR

WHITE: Hi, Mark?

KARPELES: Hi.

WHITE: I'm Geoff.

KARPELES: Nice to see you.

WHITE: Shall we go inside, see if we can find a booth somewhere nice and quiet?

KARPELES: Yes, of course.

WHITE: Let's go. Have you been to this one before?

KARPELES: Yeah, I know this one.

WHITE: I met the quiche-loving Mark Karpeles at a karaoke bar, his suggestion for a relatively quiet place to meet. The French accent is still there, but his passion for all things Japanese, particularly manga cartoons, has kept him in Tokyo. In person, he's quiet, polite and meticulous.

#### ACTUALITY IN KARAOKE BOOTH

WHITE: We might have to turn the music off, I think.

KARPELES: Yeah ...

WHITE: Before Mt Gox, he ran a website hosting company. Some overseas customers wanted to pay using Bitcoin, and that got him interested in the currency. He was offered the chance to take over Mt Gox in February 2011. At that stage, the small trading site seemed like a novel side project.

KARPELES: Before taking over, the idea sounded interesting because Bitcoin was still new and Mt Gox was the only trading platform at the time. I signed the contract to take over Mt Gox in 2011 and starting that point, I think, couple of days later,

KARPELES: it was announced that Forbes magazine would include an article about Bitcoin, and that brought the number of customers in Mt Gox from about three thousand to sixty thousand only by June.

WHITE: So in a few months you went from having three thousand customers to sixty thousand, you were in Forbes magazine. Was that the light bulb moment when you realised, actually this is going to take off?

KARPELES: Actually there was no real light bulb moment about this is great or anything. It was more like I am going to have to spend all the time this month on this and hopefully next month I have some time to do something else. I accept it, just repeated all the time.

WHITE: Bitcoin's value climbed. First one coin was worth \$5, then \$10, then \$25. Imagine if the worth of your bank savings went up five times in under two years. Mt Gox was the dominant exchange and users flocked to it. Mark Karpeles raced to keep up.

KARPELES: Mt Gox went from an interesting technical project to being, I would say, a daily nightmare of dealing with banks, governments, people I never knew existed. Running Mt Gox was basically a constant race. Well actually, I don't think any other business ever had to deal with this kind of explosive growth.

WHITE: He insists he didn't waste time – not on quiche, nor any other distractions. He's even published his work diary to prove it. But the company still suffered setbacks. Early on, Mark Karpeles had discovered that tens of thousands of Bitcoins had been stolen by hackers, and he'd been struggling with the fallout ever since. But things were about to get much, much worse. By the beginning of 2014, it was obvious to customers like Kolin Burges that all was not well. He'd deposited around 300 Bitcoins into Mt Gox, aiming to change it into hard currency - at that time, worth about £180,000. But when he tried to withdraw a few days later (on his birthday, coincidentally), things went wrong.

BURGES: I decided that I would start withdrawing from Mt Gox and then realised within a couple of hours that the withdrawal hadn't actually been processed, even though Mt Gox said that it had, so that's when the worry starts.

WHITE: But this was Mt Gox - this was a big exchange. Was that part of it, that you thought, hang on, these are big guys - this shouldn't be happening to them?

BURGES: You know, that's what you tell yourself at the beginning and then I think the next morning I looked and it still hadn't been withdrawn. Then I checked online and other people had been having similar problems. At that point, your level of concern starts to raise a bit higher.

MUSIC

WHITE: Unbeknown to Kolin and its other customers, inside Mt Gox, Mark Karpeles had just made a horrifying discovery. Hackers had effectively figured out a way to empty out Mt Gox customers' accounts and hide the truth from Mark and the company for years.

KARPELES: I came to find about it around the end of February 2014.

WHITE: But how long had it been going on at that stage?

KARPELES: Well, at that stage it had been going actually for maybe one or two years.

WHITE: So what was it like when you realised potentially a lot of money had gone?

KARPELES: I would say it's probably very close to like when you're falling from a building, obviously the floor getting closer – quite like I was about to die.

WHITE: For Mt Gox it was indeed a fatal blow. In all, around 650,000 Bitcoins had been stolen. At the time, that was worth £300 million. Today, it's close to £5 billion. When Kolin Burges found out, he was furious, got on a plane and demonstrated outside Mt Gox's office. He took me to the spot where he protested for two weeks.

#### ACTUALITY OUTSIDE OFFICE

WHITE: How cold was Tokyo at that time?

BURGES: So it had just finished a huge kind of snowstorm and there was like an igloo at the end of the street.

WHITE: Did you ever see Mark Karpeles walking in and out? Did you get a chance to actually speak to him face to face?

BURGES: On the first day, yes, so that was one of the highlights of the protest, was at the very, very beginning. I met Mark as he approached the office and we had a bit of a discussion, which was videoed and then stuck on the internet, and that was really what brought the protest into public consciousness, was that confrontation.

WHITE: What was that like, actually seeing him face to face and meeting?

BURGES: The whole situation, with me coming here and standing outside here with a sign was just a very strange thing that, I mean, one of the strangest feelings at the protest was the very first day when I came here, standing on my own, pulled a sign out, feeling incredibly stupid. But as Mark Karpeles came along and we started our conversation, it became more of a ....

WHITE: It became real?

BURGES: Yeah.

WHITE: It got very real indeed for Mark Karpeles. He was arrested and spent almost a year in a Japanese prison. He's now out on bail. He's been charged with embezzlement, which relates to payments from Mt Gox to him and other companies worth £1.7 million. He says these were legitimate loans signed off by an accountant. He's also been charged with manipulation of data. That relates to trades he's alleged to have conducted to cover losses from an earlier, unrelated hacking incident. He denies all the charges - none of which actually relate to the massive hack he discovered. The 650,000 missing coins were still a mystery - just the thing for some hi-tech armchair detectives.

#### ACTUALITY OF SKYPE TONES

NILSSON: Hello?

WHITE: Hi, is that Kim?

NILSSON: Hi, yes, this is Kim.

WHITE: Hi Kim, it's Geoff White from BBC Radio 4. How are you?

NILSSON: How are you doing? I'm fine thank you.

WHITE: Kim Nilsson is based in Tokyo too. A software developer like Kolin, he had several thousand pounds in Mt Gox. He remembers the reaction as the site collapsed.

NILSSON: I think a fair amount of people were panicking a bit. I think most people, they held on to their hopes for as long as possible that it was going to turn around, because it's human instinct, I suppose. You don't want to admit that there is a catastrophe in the making, and some people had probably put in way too much money than they could afford to lose. If the money is indeed all gone, then all right, that is a big disaster, and you are going to have to deal with it somehow. But at the very least you want to know what happened. I think it was the driving question for a lot of people.

WHITE: A question Kim set out to answer.

NILSSON: There was me and a couple of other people and I think we all shared the opinion that there is no realistic way that law enforcement is going to come to a satisfying conclusion investigating this case, mostly because it was such cutting edge technology that there was no way there were going to be forensics experts ready for this kind of crime. So we felt that we can't just sit around and wait for answers; we have to try to dig and find them on our own.

WHITE: That sounds like quite a daunting task.

NILSSON: It certainly was; it was initially a wild stab in the dark. Bitcoin was sort of a unique scenario where this is at least theoretically possible.

WHITE: Possible because of how Bitcoin works. To send and receive Bitcoins, you need a digital wallet, a sort of online account that stores your funds. Each wallet's got a unique number, like a bank account. But unlike banks, every transfer from one Bitcoin wallet to another is published on the internet. This public ledger is called the blockchain. It's part of what gives people faith in Bitcoin, and it gave Kim Nilsson and his team a chance to trace the missing Mt Gox coins. After years of number crunching, the digital trail led them to another virtual currency exchange: a competitor of Mt Gox called BTC-e. At least half the stolen coins ended up there, he says.

NILSSON: BTC-e was another big Bitcoin exchange that gained a fair amount of notoriety over time as, for lack of a better word, the shadiest exchange. A lot of criminal proceeds from cyber heists would end up at BTC-e, because presumably they asked the fewest questions. So a lot of the time, as a blockchain analyst, if I am following a Bitcoin theft somewhere, probably four times out of five those coins are going to end up at BTC-e for being sold there.

WHITE: Kim Nilsson wasn't the only one honing in on BTC-e – the bankruptcy trustees of Mt Gox were also on the hunt. So was the FBI. They already knew about BTC-e. They believed it was a major hub for laundering the profits from global



WHITE cont: it was an online exchange, BTC-e claimed it was operated by a British company called Always Efficient Ltd; one of their addresses was in East London.

#### ACTUALITY IN EAST LONDON

WHITE: I'm standing on a busy main road here in East London, and I'm outside the offices of Always Efficient - that's the British company that the old BTC-e website listed. So I'm going to ring the bell and see if there's any sign of them here.

#### ACTUALITY OF BELL RINGING

WHITE: Oh hello, I'm trying to find a company called Always Efficient, they're meant to be at this address. You haven't heard of them? Okay, thanks anyway.

So, there was no sign of Always Efficient at their offices. I'm going to delve deeper into their company registration documents and see if there's anything I can find. It says here up until last year, the company members listed on Always Efficient's documents were the names of two women in the tax haven of the Seychelles. Then in July, their names were replaced with two companies based in the Marshall Islands, that's another tax haven just west of Hawaii. There's no phone number or email address online for either of them. Under new regulations introduced in June 2016, businesses are supposed to publish a list of 'people with significant control' over a company. It says here, up until last year, Always Efficient listed a man in Russia called Alexander Buyanov. Let's see what we can find out about him. Russian investigative journalist, Andrei Zakharov, researched the story of BTC-e and tracked Buyanov down. He seems pretty far removed from the world of hi-tech currency trading.

ZAKHAROV: It was registered to Moscow DJ, Alexander Buyanov.

WHITE: It was registered to a Moscow DJ?

ZAKHAROV: Yes, he's a DJ.

WHITE: In a nightclub?

ZAKHAROV: Yes. It was not a very good club.

WHITE: And how do you know that?

ZAKHAROV: Well, I just found his account in social web and then I found information where he works and I came to his place and spoke with him, and he officially says that he knew nothing about BTC-e and he said that there are a lot of ways where people could get his documents. And Buyanov, yes, he's considered to be a drop, you know, a drop-man who doesn't know ...

WHITE: What does a drop-man mean?

ZAKHAROV: A drop-man is like he has nothing in common with the company.

WHITE: We asked Mr Buyanov why his name used to be on the Always Efficient company documents, and what his involvement was with BTC-e. He didn't respond. Empty company offices, tax havens, people supposedly in control who aren't: it looks very much like Always Efficient Ltd is a shell company. File on 4 has previously covered the failings of the UK company registration system, particularly issues with the 'person of significant control' requirement. The anti-corruption campaign group, Transparency International, has also been researching this area. When we told them the address we had for Always Efficient, they told us that address had been used by several other companies they've found to be involved in significant corruption. Director of Policy, Duncan Hames, told us such tactics can be used to conceal crime.

HAMES: So people laundering money will set up a network of companies to create layers between the original crime and their attempts to then integrate the process of their crime into the economy, and so in setting up companies to create these layers, these companies are not evidently conducting any kind of actual business, but rather they simply enable a series of transactions to take place, to create this distance and to obscure the trail of the proceeds of crime.

WHITE: We've found an instance with the company we've been looking into, Always Efficient Ltd, where the person with significant control turned out apparently to be a nightclub DJ in Moscow, who had a very limited grasp of whether he was involved with the company at all, let alone what it did. That seems to make a mockery of the concept of a person with significant control, doesn't it?

HAMES: Indeed it does, and I think it's very doubtful that that was indeed the person with significant control.

WHITE: So can you just give the name of a person, put them on the Companies House website and almost make them up? Does anybody check this?

HAMES: So to do that is obviously an offence, but it needs someone to check that and to take enforcement action in relation to that offence for there to be any credible deterrent against people filing patently false information.

WHITE: Companies House told us they have a dedicated team dealing with Persons of Significant Control, and take action when irregularities are identified. We also asked the National Crime Agency if they're investigating BTC-e or Always Efficient. They wouldn't say, but they did tell us they've set up a taskforce with Government and banks, which has arrested dozens of people and dealt with hundreds of reports of suspicious activity. If BTC-e really was a hub for cybercrime, and if Always Efficient was running it, they seemed to have little problem registering in the UK. But who was really behind this shadowy operation? If the stolen Mt Gox money pitched up at BTC-e, who's thought to be on the receiving end? Back in Japan, Kim Nilsson and his team had begun to connect many of the stolen coins to a name: a Russian called Alexander Vinnik.

NILSSON: He did receive the money on a quite regular basis, coming more or less straight out of the Mt Gox wallet so even if he wasn't involved with the thefts himself personally, he obviously had some kind of an arrangement that yes, send me all your Bitcoins and I will sell them off, or something like that. If you're privacy minded, it's not hard to hide your identity online. In Vinnick's case, he was not particularly careful; he used his real name in connection with his online handle, ironically complaining about exchanges not accepting his Bitcoin, in response to which he was sending them legal threats

NILSSON cont: under his own real name, and that's how, that's how Vinnik appeared in my investigation notes - basically because he had been, he had been complaining loudly online about it.

WHITE: It turned out the FBI was coming to the same conclusion. Like Kim Nilsson, they'd traced the email addresses and usernames through which the stolen Mt Gox money had passed, and arrived at BTC-e, and Alexander Vinnik. Andrei Zakharov spent months probing Vinnik's past. He says he started out in a town of 300,000 in Central Russia.

ZAKHAROV: He was born in Kurgan. He started economics, I think, in Kurgan State Agricultural University, but at the beginning of the century he moved to Moscow with his mother and so he didn't have any special technical education, and everybody said that he was not a hacker, he was a financial specialist and specialist in transactions. So he moved with his mother and started to search where he could work and so very fast he found out that new sphere where he could work, because at that time all these web money systems appeared. He worked in the centre of Moscow so everybody could come and see him.

WHITE: So if you worked in Moscow and you'd been paid one of the types of online currencies, Vinnik would be the guy you'd go and see to get your virtual currency transferred into real money?

ZAKHAROV: Yes, yes.

WHITE: Vinnik ended up working for BTC-e, where US law enforcement claim he ran the accounts into which those stolen Mt Gox Bitcoins were paid. Undercover US agents started testing out BTC-e, according to Department of Justice documents. They claim BTC-e support staff offered to launder drug money, and that the site was used by corrupt public officials and hacking gangs. They also say they were able to register anonymously using just an email address. The FBI claims the site was directed and supervised by Alexander Vinnik. They drew up criminal charges against him last January. Vinnik went on holiday to Greece last July, oblivious to the legal action hanging over him.

WHITE cont: With the FBI's suspect now outside his native Russia, the police pounced, shutting down BTC-e and seizing Vinnik.

ZAKHAROV: They were on the beach and his wife was swimming, and when she turned back, she saw a lot of people with sunglasses near her husband and that's how he was arrested.

WHITE: So he was arrested on a beach, sunbathing basically?

ZAKHAROV: Yes, on a beach, yes.

## MUSIC

WHITE: The US now wants to extradite Alexander Vinnik on 21 charges of money laundering and other financial crimes. But the Americans aren't the only ones trying to get him. Russia has also filed an extradition application, though on much lesser and completely unconnected charges. If convicted in Russia, he might be sentenced to several years in prison. In the US, it's likely to be more than fifty. The Greek Government must now make up its mind between the two. Vinnik is in a legal tug of war. Via his lawyers, we asked Alexander Vinnik whether he was involved in theft and money laundering, and what his connection is with BTC-e and Always Efficient. In a statement he told us:

READER IN STUDIO: The allegations of the US Department of Justice are just that: allegations. BTC-e is just a web platform for buying and selling Bitcoin, not an exchange. As such, it cannot be held responsible for the source of the money used to buy Bitcoin, no more than a bureau du change can be held responsible for exchanging a stolen \$100 note into pounds sterling. Mr Vinnik denies having any connection to Always Efficient.

WHITE: But BTC-e's UK registration isn't the only British link in this story. When customers of BTC-e wanted to move money from their bank accounts into and out of the site, they had a choice of payment processing companies - one of which was a UK firm called Mayzus Financial Services. It's registered with the Financial Conduct Authority as an authorised payment institution. Millions of pounds was moved in and out of BTC-e by Mayzus. Given what we now know about BTC-e's company setup, its alleged role

WHITE cont: in global cybercrime and no-questions-asked policy, should Mayzus have got involved with this cryptocurrency exchange? I asked their Head of Compliance, Igor Sergeev.

SERGEEV: There is no exchange which can be bulletproof against the possibility that some of the Bitcoins traded on it or some of the traders on the Bitcoin exchange are not doing something illicit. We have done our due diligence, because for us, every BTC-e Bitcoin trade is a high risk trade. You can Google this now, there is a recent complaint from people whose fund has been blocked by my team.

WHITE: Broadly speaking, your argument is that when people withdrew money from BTC-e, using Mayzus Financial Services, you were able to check who those people were and where they were transferring the money out into the accounts they were transferring it out into?

SERGEEV: Yeah absolutely.

WHITE: It does beg the question though, you have outlined the risks of Bitcoin exchanges. Mayzus Financial Services is a large company with presumably a lot of other customers, is FCA regulated - Financial Conduct Authority regulated in the UK, is held to a high standard. Why was it worth taking the risk of getting involved with an exchange which, according to the Americans, was a hub of cybercrime for some parts? Why take the risk?

SERGEEV: Once you know the risks which any client will bring to you, what you do is that you trying as hard as possible to mitigate those risks and set up procedures which would protect you - that's what you do.

WHITE: Mayzus Financial Services said it only handled a small proportion of BTC-e's transactions and that it's fully complying with law enforcement requests. The Financial Conduct Authority told us companies like Mayzus Financial Services have to submit details of their anti-money laundering systems and their risk management and internal controls. This all started with the theft from Mt Gox. So what does its former boss, Mark Karpeles, say now?

WHITE cont: Many thousands of people put their money into Mt Gox, trusted the company and you were the head of that company. They feel you are responsible for them losing money.

KARPELES: I am very sorry that when I was in charge, things happened the way they did, so I am trying to do my best to get this to be sorted as fast as possible, and at the same time making sure that all the money that was in Mt Gox gets distributed to creditors one way or another.

WHITE: But those creditors, including Kolin Burges, might still turn a profit, thanks to one final, bizarre twist in the story. After the theft from Mt Gox, Mark Karpeles found 200,000 Bitcoins that hadn't been stolen.

BURGES: We are basically trying to get our share of the 200,000 Bitcoins back. Effectively that's about a quarter of what was lost, so we should in theory get a quarter of the number of bitcoins, very approximately.

WHITE: Given how much Bitcoin's gone up in value, even a quarter would be worth way more than his original investment. But there's a snag.

BURGES: Due to technicalities of Japanese law, our Bitcoins were valued at a specific price at the start of the bankruptcy, a specific price in Japanese Yen, and the bankruptcy law doesn't allow for us to get back more than the value of those Yen.

WHITE: So Kolin and others don't know whether they will get back the 2014 price for each Bitcoin - about £300 - or the £7,000 each of those Bitcoins is worth today. Unsurprisingly, many of them are pushing for a legal solution that would see their share of investment refunded in the current Bitcoin price. The collapse of Mt Gox and the revelations around BTC-e have sounded huge alarm bells for regulators across the world. They're now starting to grapple with how to control decentralised, digital currencies. In the UK, the FCA doesn't directly regulate cryptocurrency at the moment. That could change. Finance ministers from twenty countries, including the UK, are discussing cryptocurrency regulation later this month. In Britain, the Treasury Committee's investigating the issue; so is the Bank of England.

## ACTUALITY IN JAPAN

WHITE: But how effective would regulation be? Here in Japan, they already police the cryptocurrency trade and there have still been problems. Last month, a major exchange here announced it had been hacked and lost almost half a billion dollars. Guess whose money was tied up in it?

## MUSIC - VIRTUAL CURRENCY GIRLS

WHITE: That's right - the poster girls for virtual currency safety are now victims of crime themselves. The agency that hires them had some of their money in that latest company to get hacked. The Virtual Currency Girls are still waiting for the cash.

TRANSLATOR: The account was frozen for some time; now it's been defrosted, but there are still people who haven't been refunded, but we still haven't been paid our salary in crypt.

WHITE: Cryptocurrency may have turned out to be a nightmare for some, but for most of the people I interviewed for this programme, they still believe in it. Kolin Burges is still investing, Thomas Glucksman still works in the area, and the Virtual Currency Girls – they are still singing cryptocurrency's praises.