Sidedoor: S11E05 – Bitcoin Bank Heist

Lizzie Peabody: This is Sidedoor, a podcast from the Smithsonian with support from PRX. I'm Lizzie Peabody.

Lizzie: One weekend not so long ago, Zia Faruqui came rolling into the Smithsonian's National Museum of American History with his family.

Zia Faruqui: *My son was wearing Heelys, so the shoes that have wheels in them? Which I explicitly forbid him from doing, but he loves to do when he goes to the museum there because the floors are very smooth and it's a big open space.*

Lizzie: *Oh yeah, it's like a big roller rink.*

Zia Faruqui: *Correct.*

Lizzie: Zia figured we might as well take a spin around one of my favorite galleries.

Zia Faruqui: *And I was like, "Oh, we should check out the Numismatics." There's a cool bank vault thing door, they love that.*

Lizzie: Numismatics is the study of money. And the Gallery of Numismatics, which you do enter through a very cool vault-like door, is filled with money in all its various forms throughout history. From ancient Babylonian tablets to gold coins to a giant stone from the Island of Yap. And that analog stuff is cool, but Zia bee-lined it for the tech section.

Zia Faruqui: *Because I was like, "Oh, they gotta have a thing for Bitcoin or cryptocurrency." And I was looking around the room for it, and then I saw the magazine cover that was like, "Bitcoin: What Is It?" or something like that.*

Lizzie: A print magazine from nearly a decade ago? Zia was not impressed. He was like, "What is this, a dentist's office?"

Zia Faruqui: *And so I took a picture of it to send snarky comments to my friends.*

Lizzie: But he didn't only message his friends.

Ellen Feingold: *And then I received this email.*

Lizzie: As curator of the National Numismatic Collection, Ellen Feingold is used to hearing from the public.

Ellen Feingold: *Usually we receive emails from people who have their grandfather's coin collection, or were out metal detectoring and came across something.*

Lizzie: But this email stood out.

Ellen Feingold: *I, in my 11 years that I've been curator of this collection, have never received an email from a judge saying, "I think I can help you." [laughs] "I think you can do this better."*

Lizzie: Oh, yeah. Zia Faruqui is a judge. A federal judge. And not just any federal judge.

Lizzie: *You've been called the "Crypto Judge."*

Zia Faruqui: *That's true.*

Lizzie: Before becoming a judge, Zia Faruqui was a federal prosecutor. And he's seen a lot of cases involving cryptocrime. So when Ellen got his email she was thrilled, because she's the first to admit crypto is not really her jam.

Ellen Feingold: *Because I am someone who is much more comfortable in 19th century files and ancient coins than trying to understand this new digital currency and also the challenge of how to document it.*

Lizzie: And it is a challenge to figure out how to represent a digital currency in a physical museum. And Ellen was very interested to hear what ideas the Crypto Judge might have about this.

Ellen Feingold: *So I picked up the phone and I called him, and I said, "I don't really know what to do here, but can you tell me more?"*

Lizzie: Judge Faruqi understood the assignment. I mean, he *is* the Crypto Judge. And he had something specific in mind. Something big. He told Ellen ...

Zia Faruqui: *You want something that's more concrete and something that really could connect with people. And, like, what could be bigger than—I mean, not like the getaway car, but the getaway device for a $4-billion heist? This case like none other? The largest bank heist in the history of the world.*

Lizzie: So this time on Sidedoor, one of the wildest, most game-changing crypto heists of all time. How federal agents tracked the hackers who disappeared into the ether—net—with billions in bitcoin. That's coming up after the break.

***

Lizzie: In the summer of 2016, hackers broke into Bitfinex, an online cryptocurrency exchange based in Hong Kong.

*[**NEWS CLIP:** Hong Kong-based Bitfinex has revealed it was victim to a hacking attack.]*

*[**NEWS CLIP:** Now more than $70 million worth of Bitcoin, the online digital currency, has been stolen.]*

*[**NEWS CLIP:** Bitfinex has now halted trading in all digital currencies while it investigates the security breach.]*

Lizzie: It was one of the biggest heists in history. And there were no fingerprints to dust for, just the record of a digital transaction moving over $70-million worth of bitcoin to the hacker's online wallet: Wallet 1CGA4S.

Ari Redbord: *The world knew the address that was associated with the Bitfinex hack because everyone watched those funds move off of Bitfinex into that. So everyone's watching this.*

Lizzie: This is Ari Redbord. He's the global head of policy for TRM Labs, a blockchain intelligence company that traces the flow of cryptocurrencies. And I want to pause here because you might be thinking, if the entire world was watching this heist happen, then couldn't you see who stole the bitcoin? Well, yes. And no. We're gonna break it down.

Lizzie: But first, let me just come clean and say when it comes to cryptocurrency, my attitude has generally been that sounds confusing. Maybe if I don't think about it, it will go away. But it hasn't gone away. So let's get a few things straight. Bitcoin is one kind of cryptocurrency. It only exists in digital space. You can't hold a bitcoin in your hand like you can hold a $100 bill.

Lizzie: And you might be thinking, "Well, I Venmoed my brother $40 for concert tickets to Blind Pilot last week. Isn't that digital?" Well, yes. But here's the key difference between buying something with bitcoin versus, say, Venmo or Mastercard online. There's no middle man.

Lizzie: With traditional currency, an intermediary like a bank or Venmo will keep track of every transaction I make so I can't spend the same $40 twice. Once I send the money to my brother, Venmo records the transaction on its internal ledger, and my $40 now belongs to my brother. But cryptocurrencies are peer-to-peer currencies. So instead of a middleman keeping a private ledger of all transactions, everything is recorded out in the open. And this public ledger is called the blockchain.

Lizzie: *When I hear blockchain, I think of blocks on a chain.*

Ari Redbord: *And as you should. And when each of those transactions is logged and verified, that's essentially when another block on that chain is added.*

Lizzie: And this is why cryptocurrency works. The public nature of the transactions creates accountability. So let's say my brother wanted to be shady and said he never got the money I sent. And even if he erased any trace of the transaction on his computer, it would still exist on the blockchain for anyone else to see and verify.

Ari Redbord: *Every transaction is logged and immutable. It's forever.*

Lizzie: Now you can buy cryptocurrency online with regular money through something called a cryptocurrency exchange. So if I wanted to buy $100 of bitcoin, I'd go to a cryptocurrency exchange and give them $100 from my real-life wallet in exchange for $100 worth of bitcoin in my crypto wallet. And here's one of the biggest supposed perks of cryptocurrency: those crypto wallets are anonymous. So I can buy and sell and do whatever I want with my money without anyone knowing it's me. Judge Faruqui says your wallet address is just a string of letters and numbers unique to you, like an email address. And like an email address, there's no telling for sure who's behind it.

Zia Faruqui: *Who is behind cryptojudge123@gmail.com or whatever it is? Is that me, or is it someone just pretending to be me? I mean, let's be clear, that's definitely not me.*

Lizzie: *I don't know, that sounds like a good email address.*

Zia Faruqui: *Yeah, exactly. Yeah.*

Lizzie: And just like every email address requires a password to log into it, every crypto wallet has a private key to unlock it. That's just a long string of numbers and letters unique to that wallet. So every crypto wallet has a public address. And all the transactions made between wallets are public. But the identity behind the wallet? That is the secret part. And that's why it was possible for hackers to rob Bitfinex in public.

Lizzie: Imagine an invisible robber broke into a bank and stole millions of dollars, then set those millions of dollars on the front stoop of that bank—big ol' bags of cash for everyone to see, locked in a glass case. You could see the money inside. But nobody could get in except the robbers. That's what happened with Bitfinex.

Ari Redbord: *Everyone's watching that bag of cash in that glass box with the lock on it sitting outside the bank.*

Lizzie: Wallet 1CGA4S.

Ari Redbord: *And they watched it for five years.*

Lizzie: For five years, most of the stolen money just sat there on the stoop. Why? Well, for the hackers, spending it was risky.

Zia Faruqui: *There are tons of Twitter accounts and things like that of people who are just watching the blockchain, waiting for transactions to move from these infamous heists, right? So this was the most infamous.*

Lizzie: Judge Faruqui says because the blockchain is public, the more infamous the heist, the more people are popping their popcorn, pulling up their desk chairs to this true-crime story unfolding on their computers in real time. But for the hackers, that meant they had a huge audience. It would be like ...

Zia Faruqui: *You just robbed a bank of a billion dollars and you have it in your basement. But if you could never spend it? I mean, that sounds like the premise to a horror movie to me! It's like, it's just sitting there and you know that even if you spend a penny of it, if you go down to the local bodega and you spend it, everyone in the world is gonna know that that penny has been spent. Now they won't know it's by you, but everyone's gonna know that you did it, and now you're one step closer to potentially getting caught.*

Lizzie: Remember, your wallet address is anonymous until someone links it to your real-world identity. That's called attribution. So every time the hackers moved money, they were leaving a clue. A new footprint to follow. And here's the big problem for them: there's only so much you can do with crypto online.

Ari Redbord: *Because at the end of the day, you still need to convert cryptocurrency to some sort of fiat currency in order to use it, you know, everything from diapers to missiles, right? It's hard to buy things with crypto today.*

Lizzie: Ari says crypto still exists in a kind of digital bubble. Like casino chips. They work like money when I'm in the casino, but I can't pay my rent with chips from Caesar's Palace. I need to cash out if I want to use that money in the real world. And this is essentially what you do when you convert cryptocurrency to or from cash. What Ari calls "on ramps" and "off ramps" to the digital bubble.

Ari Redbord: *And those are mostly the exchanges like a Coinbase, like a Binance. And what you're doing is you are, for the most part, using fiat currency to buy crypto.*

Lizzie: These exchanges are also where your online identity gets linked with your real life identity.

Ari Redbord: *So when you open an account on Coinbase, it is as rigorous a process as opening a bank account. So your exchange knows you. They can tie that alphanumeric cryptocurrency address to the person.*

Zia Faruqui: *That off-ramp is when that perceived anonymity gets totally burst.*

Lizzie: So in the case of the Bitfinex hack, if the hackers had sent their crypto directly from their wallet to an exchange to cash out their millions, all the exchange would have to do would be to look up who had registered that wallet? Whose driver's license is associated with it? "Ah, Mr. and Mrs. Hacker!" and they'd be busted.

Lizzie: So the hackers needed to disguise their ill-gotten gains before they could cash out—clean it, if you will. And that means money laundering—moving it a thousand times, splitting it up into little pieces and then reconsolidating it, trying to obfuscate and hide their tracks. Which is hard to do when all your tracks are public.

Zia Faruqui: *So it's probably better just to leave that money in your basement, in which case what have you netted yourself other than a lot of, at least for me, anxiety?*

Lizzie: In the meantime, their problem was compounding. Because the value of Bitcoin steadily went up. As years passed, $72 million became ...

Ari Redbord: *$4.5 billion.*

Lizzie: *Oh my gosh. Their problem was too much money!*

Ari Redbord: *Their problem was too much money.*

Lizzie: By 2020, the hackers had billions in the basement but couldn't buy a banana at the bodega. They were trapped in the crypto bubble!

Ari Redbord: *Picture, like,* Tron *or something, right? Where you're, like, living on a blockchain somewhere in the world, right? Living in cyberspace.*

Lizzie: *Uh-huh.*

Ari Redbord: *They couldn't do anything with these funds because CryptoSleuths, Chris Janczewski, was watching and tracking and tracing those funds.*

Chris Janczewski: *My name is Chris Janczewski. I'm the head of global investigations at TRM Labs.*

Lizzie: But before that he was a special agent in the criminal investigations division of the IRS. That's right, they're not just accountants! Guys like Chris are basically police officers with exceptional accounting expertise. They need the brains to follow the money, but they also need to be the brawn when that money leads to someone's front door.

Lizzie: Chris helped start the IRS's cybercrimes unit, which kept him busy and regularly took him all over the world—busting up terrorism-financing campaigns, arresting money launderers, taking down the biggest child exploitation website in the world. And it was the end of 2020 when he turned his attention to Bitfinex. By that time, that $70-million bitcoin heist had become a multi-billion cybercrime that was still unsolved. And Chris doesn't like to see bad guys get away.

Chris Janczewski: *So when it came back on my radar it was obviously a significant amount of money, and I felt like with the team around me, like, we kind of were in a stride and thought, "You know, if not us, if not now, why not try and give this a crack and see if we can figure it out?"*

Lizzie: So Chris sits down at his laptop to get to work. Like, what are the knowns at that point?

Chris Janczewski: *So at the time the knowns were very little.*

Lizzie: But he knew what to do.

Chris Janczewski: *We focus on following the money. It's like a mantra that's beaten into you from day one at the academy.*

Lizzie: And the nice thing about the public ledger ...

Chris Janczewski: *It makes it much easier to follow the money. Now it might not understand why or who's behind it, that's the investigation part of it, but the money is there to be followed.*

Lizzie: *It's almost like, like you have really clear boot prints in the sand. You just don't know whose boots they are. But you can follow them really, really clearly. I guess they're boot prints in cement, actually.*

Chris Janczewski: *That's right, yeah.*

Lizzie: Chris was retracing the hackers' steps.

Chris Janczewski: *So going back and looking at everything that happened from day one.*

Lizzie: For the first few months after the Bitfinex hack, absolutely nothing happened. The stolen money sat on the stoop of the bank untouched. And this was a significant clue, because the usual suspects in these types of cybercrimes move money quickly.

Ari Redbord: *So when North Korea hacks a crypto exchange, they move those funds as fast as they*

can to an off ramp. They're trying to get it off the blockchain as fast as they can.

Lizzie: *Protecting their identity is not as much of a priority because they're kind of out of reach.*

Ari Redbord: *They don't care.*

Chris Janczewski: *They're not concerned about getting caught.*

Lizzie: But these hackers appeared to be concerned.

Ari Redbord: *They were really careful. And that's just very different than the typical cybercriminal that we deal with in the world.*

Lizzie: So for months, no money moved at all. But then in January 2017, the hackers started laundering, moving small amounts of money at a time. And Chris was tracing every step.

Lizzie: Combing through past digital transactions and every new one, looking for patterns and associations. He describes the investigation process as "part art, part science."

Chris Janczewski: *And so the science is that the transactions definitely took place: Address A sent one bitcoin to address B at this date and time. Nobody refutes that. Everyone can see that it's there. The art of it is understanding why.*

Lizzie: Why does the money always move at a certain time of night?

Chris Janczewski: *Does that suggest that maybe they're in this part of the world?*

Lizzie: Why do they always send an amount equal to the US dollar value?

Chris Janczewski: *And so, like, as the investigation proceeds, you get more and more context. So your kind of 'artist's eye' that's looking at things changes or matures over time.*

Lizzie: Retracing steps, Chris quickly found that of the cybercrimes he'd investigated ...

Chris Janczewski: *The Bitfinex money-laundering process was by far the most complex one that I had seen.*

Ari Redbord: *These guys were using every possible trick in the book.*

Lizzie: Most of the stolen Bitfinex money was still sitting on the stoop. But small bits of it had been siphoned off and routed through complex sets of transactions to try to clean it, so when it got to an off ramp it would look legitimate. This meant sending funds to a bunch of different places.

Ari Redbord: *We saw them move through Darknet markets.*

Lizzie: Think eBay-style markets for bad guy stuff.

Ari Redbord: *Narcotics, but also murder for hire and other types of things. They bought gold, gift cards. We saw funds move through mixing services.*

Lizzie: Kind of like a blender for crypto.

Ari Redbord: *You put some of your crypto into the mixer, it mixes with other people's, and sends out obfuscated to the other side.*

Lizzie: By using tracing software to follow the money down every possible route, Chris could start to find patterns. Like stepping back from a pointillist painting—each dot, each transaction, is just a blob of color, but taken together, a picture begins to emerge.

Ari Redbord: *Basically a pattern of dispersion and consolidation.*

Lizzie: Some of the stolen crypto led to exchange accounts, those off-ramps to the real world.

Chris Janczewski: *There were multiple accounts that were created in what appeared to be false identities.*

Lizzie: But bit by bit by tracing every thread ...

Chris Janczewski: *There was this spider web of transactions that then began to condense, that landed on exchange accounts that were in the name of Mr. Lichtenstein and Ms. Morgan.*

Ari Redbord: *That was a major turning point in being able to connect the dots in this investigation.*

Lizzie: They had names. Accounts linked to real people with real addresses living in the real world. Okay, that last part might be a stretch. They were living in their own world.

Ari Redbord: *Oh, man. Like, this case is going to be a really big deal in large part because of how*

interesting these defendants are.

Lizzie: When we come back, we meet the hackers with the keys to the glass case of money on the front stoop of the bank.

Ari Redbord: *I was very very surprised.*

Lizzie: After the break.

***

Lizzie: Chris Janczewski braced himself outside the door of a posh Manhattan apartment on Wall Street. Surrounded by a team of FBI and other federal agents, he took a deep breath. If his suspicions were correct, the hackers whose footsteps he'd tracked virtually for the last year were now only feet away. And there was no telling how they'd react to a knock on the door.

Chris Janczewski: *When you're standing outside of someone's door about to make entry, you don't know what's gonna happen.*

Lizzie: Almost six years after the Bitfinex hack, Chris and his team had "followed the money" through the blockchain and up the service elevator of this apartment building to this very spot. It was January, 2022. It was cold. Early morning.

Lizzie: *Why did you go so early?*

Chris Janczewski: *That's most likely when they're gonna be there. That's most likely where you can kind of potentially catch them off guard.*

Lizzie: The 'them" was a married couple in their early '30s. Ilya Lichtenstein, a Russian-born entrepreneur, tech bro and self-described magician. And his wife.

*[**ARCHIVE CLIP, Heather Morgan:** This song is for the entrepreneurs and hackers, all the misfits and smart slackers. Razzlekhan.]*

Lizzie: Razzlekhan. Also known as Heather Morgan. And I am just gonna just let her introduce herself.

*[**ARCHIVE CLIP, Heather Morgan:** I'm many things: a rapper, an economist, a journalist, a writer, a CEO and a dirty, dirty, dirty dirty [bleep].]*

Chris Janczewski: *Miss Morgan, she had a very—we'll call it heavy social media footprint.*

Ari Redbord: *You know, all kinds of people commit all kinds of crimes.*

Lizzie: *It takes all types.*

Ari Redbord: *It takes all types. And these types? These types were really interesting types.*

Lizzie: Morgan and Lichtenstein's names surfaced only a few months into the investigation. And once Chris had linked those names to accounts with stolen crypto, a whole new world of investigation opened up to him. A strange one.

*[**ARCHIVE CLIP, Heather Morgan:** Razzle dazzle. Genghis Khan but with more pizzazz. That's my name—Razzlekhan.]*

Chris Janczewski: *And so in many ways, if you think of a crime scene, and you put the yellow tape up around somebody's house, for me, that was virtual. So it might be like the blockchain of these transactions is kind of my crime scene, or all the evidence you might find on Facebook or Twitter from people's social media posts.*

Lizzie: Chris scoured social media the same way you'd search a crime scene for evidence. Posts showed first-class travel around the world. Liechtenstein tasting the gourmet food fed their exotic cat, Clarissa, who got pushed around the block in a baby stroller.

*[**ARCHIVE CLIP, Heather Morgan:** Razzlekhan here! And I wanna talk about ...]*

Lizzie: Morgan offering instructional videos on everything from how to become a self-made CEO and tech investor to how to not bedazzle but "berazzle" your old clothes as the self-described "Turkish Martha Stewart."

*[**ARCHIVE CLIP, Heather Morgan:** Turkish Martha Stewart ...]*

Ari Redbord: *And I encourage people to like, look, listen. I mean, it's absolutely fascinating.*

*[**ARCHIVE CLIP, Heather Morgan:** Do you ever have someone in your life who just suck? Well, this song's about them.]*

Ari Redbord: *She's really close to the camera, doing all kinds of crazy hand gestures. It's a little obscene.*

Lizzie: Here Razzlekhan is wearing blue glitter in front of a hanging animal skin of some kind, while wielding a vacuum cleaner.

*[**ARCHIVE CLIP, Heather Morgan:** Dudes show up to my [inaudible]. Show your uninvited top my ...]*

Ari Redbord: *I think that she is not good by any stretch of the imagination.*

Chris Janczewski: *Yeah, I mostly watched the videos on mute.*

Lizzie: But in another sense, these videos were great!

Ari Redbord: *I mean, she provides a lot of great evidence.*

Chris Janczewski: *What might be a quirky rap video to one person, to me that's a video shot inside of somebody's house, that they're giving you an eye into their private area and you can see, oh, there's a laptop sitting over there. Oh, it's an Apple laptop? We have device logs connected to this virtual currency exchange that says it was an Apple laptop.*

Lizzie: Meanwhile Chris's laptop was amassing more and more evidence.

Chris Janczewski: *The laptop was very much kind of the funnel, the consolidation point for where all of the pieces of information come together.*

Lizzie: But there was one very big piece of evidence missing: the private keys to the accounts containing the stolen Bitcoin.

Chris Janczewski: *There's a saying within cryptocurrency that if it's not your keys, it's not your crypto. To control or spend cryptocurrency you have to have the private keys behind it.*

Lizzie: Remember, the private key to your wallet is kind of like the password to your email.

Chris Janczewski: *It's basically a way of authenticating that you are the owner of this account.*

Lizzie: If they could find the private keys, that would be like the smoking gun proving that Morgan and Lichtenstein had control over the stolen money. But not only that, with the keys Chris could take the Bitcoin back.

Chris Janczewski: *And so it's really critical in cryptocurrency investigations to find those private keys. And once you're able to get possession of those, you too can control that crypto and send it off to a destination of your choice.*

Lizzie: And that's what Chris and the team were hoping to find on that cold January morning in 2022 as they prepared to enter Morgan and Lichtenstein's Manhattan apartment. About 10 agents from three-letter outfits, IRS, FBI, HSI—[whispers] that's Homeland Security—knock on the door. Announce themselves. Behind the door were Lichtenstein and Razzlekhan.

Lizzie: *Did they seem surprised?*

Chris Janczewski: *I don't know, it's hard to judge. You don't know, like, what is surprised and what is, like, still sleeping.*

Lizzie: The suspects weren't under arrest, so they were free to leave while police searched the apartment. Clarissa the cat was free to go as well.

Chris Janczewski: *We were all for it. The cat was not part of our search warrant to be seized.*

Lizzie: But the cat was hiding under the bed, and only responded to Morgan.

Chris Janczewski: *And so we agreed to let her get it out from underneath the bed.*

Lizzie: But what Chris didn't know was Morgan's cell phone was next to the bed.

Chris Janczewski: *And when she knelt down at the side of the bed ...*

Lizzie: Supposedly to fetch Clarissa ...

Chris Janczewski: *She grabbed her cell phone.*

Lizzie: She went for it! Grabbed her phone and started frantically hitting the button on the side.

Chris Janczewski: *It appeared that Ms. Morgan was making attempts to more firmly lock her phone. And I grabbed her hand and pulled the phone out of her hand.*

Lizzie: *And so what happened after that?*

Chris Janczewski: *They got their cat and they left.*

Lizzie: And the search for the private keys began. Remember, it's just a string of letters and numbers.

Chris Janczewski: *And that can be stored electronically, so it could be on a computer. It could be on a thumb drive. It could also be written down on a piece of paper. And you could think, like, how small could you write on a piece of paper? Could you, you know, take off the cover of a light switch and put a little piece of paper inside of there?*

Lizzie: They had to check every crevice, combing through the apartment room by room.

Chris Janczewski: *So if you're at a bookshelf, you pull down each book, meticulously look through it. Pull the next book down, then look at the shelf and then move on to the next area.*

Lizzie: As the day wore on, they found a few things that some people might call suspicious.

Chris Janczewski: *Under the bed, there was a bag of old cell phones. And on the bag was labeled 'Burner.'*

Lizzie: *That's a pretty bold way to label a bag. [laughs]*

Chris Janczewski: *Yeah. It seemed a little on the nose. There was also, like, a book that was hollowed out much like in a spy movie where you could seal something in. It was empty. But again, atypical.*

Lizzie: It's almost like they were trying to play criminals on TV. The team seized some electronic devices to go through later, but at the end of the day the private keys were nowhere to be found. Chris was deflated.

Chris Janczewski: *Yeah that's fair. Disappointed.*

Lizzie: He flew back to Michigan. Started going back over the evidence. Where hadn't they looked? Did they need another search warrant? And then a couple days later, Heather Morgan made a grave error. She sent a tweet, just a harmless little tweet.

Chris Janczewski: *And it was very kind of 'What good can you do in the world?' or some type of, like, platitude. And for whatever reason, it just, like, kind of stuck with me.*

Lizzie: Remember kids, you never regret the tweet you didn't send. This one stuck in Chris's craw.

Chris Janczewski: *I don't know, I view myself as, like, a bit of a competitive person. It's never personal but, like, I do want to be right and I want to be able to prove that I'm right.*

Lizzie: That tweet was all he needed. Chris suited back up for battle. Opened his laptop ...

Chris Janczewski: *Drank a lot of coffee, put my noise-canceling headphones on and went back through, like, every piece of evidence that we had: every email, every file, every transaction for the past couple years. And this is many different files.*

Lizzie: And as he was going through these old files, something caught his eye, something that had been there all along but he hadn't noticed before.

Chris Janczewski: *Some files that we had from the online cloud storage kind of like stuck out.*

Lizzie: And you know how Chris says investigations are part art, part science? Well, this was a Michelangelo moment. Because when I asked him what stuck out, all he could tell me was ...

Chris Janczewski: *You know, if you could imagine a cabinet that has, like, a bunch of stuff in it, that's never moved, and there's dust on it, but then there's these, like, shiny, nice things in this cabinet? Like, it may not mean anything, but your question is, like, why? And it's like these files kind of had that appearance. It just, like, stuck out.*

Lizzie: The files were password protected, but with the help of his co-case agent at the FBI, Chris got in. And inside was a list of alphanumeric characters.

Chris Janczewski: *Two thousand of them, which is unique because there were about two thousand unauthorized transactions from Bitfinex, each one going to a different, unique Bitcoin address.*

Lizzie: He could hardly believe it.

Chris Janczewski: *No. No. That's not right. Right? No. And you kind of have this debate in your head.*

Lizzie: Could it really be?

Chris Janczewski: *You think this is it? Maybe. Yeah, this is! This is totally the private keys to billions of dollars sitting here on my laptop.*

Lizzie: And remember, your keys, your crypto.

Zia Faruqui: *We say, you know, possession is nine-tenths of the law. I don't actually know as a judge or lawyer if that's true, but we say possession is nine-tenths of the law.*

Lizzie: *[laughs]*

Zia Faruqui: *I always said cryptocurrency possession is ten-tenths of the law.*

Lizzie: Crypto Judge Faruqi again.

Lizzie: *Right. If you have the key, it's yours.*

Zia Faruqui: *Correct.*

Lizzie: Chris was sitting on $4 billion that were by this definition, ten-tenths his. And I don't care who you are, there has got be some temptation to hop on the next plane to a non-extradition country and live like a queen with all of your friends in a castle you built for them where you can host your own private Taylor Swift concerts, and have these huge dance parties in your living room, could be entirely made of cushions. You have indoor slides and a built-in ice cream bar in your kitchen and a private jungle ropes course, and never have to set the alarm in the morning again. That'd be nice. But Chris and Ari are impervious to temptation like that.

Ari Redbord: *If I knew that no one would ever find me and I could live on a desert island, like, yeah, I'd totally take the money.*

Lizzie: *[laughs]*

Ari Redbord: *[laughs] But, like, the reality is you're gonna be hunted literally like a criminal your entire life.*

Lizzie: Okay, so maybe not so much impervious as practical. These guys know they'd be caught. In fact, one of the first arrests Chris made in the cybercrimes unit was of a federal agent who had stolen almost a million dollars of bitcoin in an investigation.

Chris Janczewski: *And, like, here I am in possession of billions of dollars.*

Lizzie: Chris did not run for the border. Instead, he canceled his evening plans, called up his team and began what he describes as the most exciting, terrifying, boring seizure ever. Exciting, because this was about to be the largest seizure in the history of the United States government and also, the world. Terrifying, because he had to send the crypto to the right place. Remember, crypto is a peer-to-peer currency. There's no middle man. No help desk in the sky to contact if you send money to the wrong person. With bitcoin ...

Chris Janczewski: *Once you hit send, it's gone.*

Lizzie: With one typo, Chris could go from hero to national dingus.

Chris Janczewski: *Nobody wants to be the guy that lost billions of dollars on behalf of the United States government.*

Lizzie: And it was boring because ...

Chris Janczewski: *Screenshots, taking notes ...*

Lizzie: ... bureaucracy, man! He couldn't send all the money at once, so he had to split it up in small pieces. And from his laptop at his home office in Michigan, he worked, methodically moving money.

Chris Janczewski: *Long into the night, into the next day.*

Lizzie: And remember: on the blockchain, people around the world can see what's happening as it's happening.

Chris Janczewski: *So as we're moving the money we'd actually see tweets go up in real time of people saying, like, "The stolen Bitfinex money is on the move." And then other people would comment, like, "Is the hacker trying to launder it? Where is it going now?"*

Lizzie: *Was there any concern that the hackers themselves would see the money moving and then try to move what they could elsewhere?*

Chris Janczewski: *Yeah, absolutely.*

Lizzie: But Chris was banking on the suspects being on New York time, so they should have been sleeping.

Chris Janczewski: *But we have no idea. Maybe they have alerts that anytime something happens, you know, their phone goes off. And if they moved faster, they don't have to document and take screen shots. And they can be much quicker. It was certainly a risk.*

Lizzie: But after a long, tense night, as the sun started to come up in Michigan and the birds started chirping, the final Bitfinex funds came home to roost.

*[**NEWS CLIP:** This morning, the Justice Department announcing the largest single seizure of funds in the department's history.]*

Lizzie: Ilya Lichtenstein and Heather Morgan were arrested later that week.

*[**NEWS CLIP:** The department has charged Ilya Lichtenstein and Heather Morgan for their alleged roles in a conspiracy to launder stolen cryptocurrency.]*

*[**NEWS CLIP:** Who are these people?]*

*[**NEWS CLIP:** 34-year-old Ilya Lichtenstein and 31-year-old Heather Morgan are tech entrepreneurs.]*

*[**NEWS CLIP:** Heather Morgan is a part time rapper and reportedly a former contributor at Forbes.]*

*[**NEWS CLIP:** Lichtenstein who describes himself online as an occasional magician is the founder of a digital wallet company designed to stop fraud and terrorism.]*

Lizzie: The berazzled Razzlekhan had been derazzled. Heather and Ilya pled guilty and both were convicted.

*[**ARCHIVE CLIP:** Today, the Department of Justice has dealt a major blow to cybercriminals looking to exploit cryptocurrency.]*

Lizzie: This case was like the Bonnie and Clyde of crypto. It was so big, so high profile, it pierced the myth of cryptocurrency's untraceability.

Zia Faruqui: *The point is not just was this the first investigation ever to trace money, you know, on the dark web or through cryptocurrency or through using these tools. No. I mean, many of our other investigations did that. But when you successfully use these tools to solve the biggest bank heist of all time that had confounded people for years, and was the biggest source of attention within the, you know, cybercommunity, not just the virtual currency community, that's what makes this case extraordinary.*

Lizzie: And that's what made Judge Faruqui write to curator Ellen Feingold and tell her the story you just heard.

Ellen Feingold: *This particular case was a landmark moment because it really crystallized that the federal government could not only track illegal behavior, but they could arrest the people that they believed were responsible for it, they could use the evidence online that they had gathered, they could prosecute, and they could convict.*

Zia Faruqui: *The fact that this laptop is going into the Smithsonian is so insane!*

Lizzie: So move over, Bitcoin Magazine! Chris Janczewski's laptop will now be part of the updated Value of Money exhibition at the Smithsonian's National Museum of American History.

Zia Faruqui: *Which, like, still just blows my mind. I'm very humbled and honored.*

Lizzie: Ellen says this laptop, a portal to the crime scene, is the perfect on ramp to help museum visitors understand the rapidly-evolving world of cryptocurrency.

Ellen Feingold: *This was the perfect starting point for most people. Not asking them to understand what cryptographic code is, but helping them understand that what they're seeing in the news reflects this major shift in what crypto is or is not, or how we understand what crypto is and is not, and how that might shape that's role in our economies in the future.*

Lizzie: *This kinda looks like my Macbook Pro. It's got, like, a little bit of gunk on the speakers, where maybe some crumbs fell, and it's got some fingerprints on the trackpad, and the screen is a little scuzzy.*

Lizzie: Come see for yourself. It's a humble machine that tells a much bigger story.

***

Lizzie: You've been listening to Sidedoor, a podcast from the Smithsonian with support from PRX. To learn more about the Bitfinex heist, there's tons coming out these days. We'll link to a bunch of it in our newsletter. You can subscribe at SI.EDU/Sidedoor. Come see Chris's computer for yourself at the newly reopened Value of Money exhibition at the Smothsonian's National Museum of American History. And if you haven't gotten enough of Ari Redbord, he hosts a podcast all about crypto stuff called TRM Talks. Check it out! We'll link it in our newsletter, too.

Lizzie: For help with this episode we want to thank Chris Janczewski, Ari Redbord, Zia Faruqui and Ellen Feingold. Thanks also to Valeska Hilbig and Emma Rhodes. This investigation involved a robust and highly skilled team of people working together, including: Jessica Peck, Alden Pelker, Chris Brown, Brian Rickers, Angela De Falco, Jessi Brooks, Chris Wong, Mark Van Wieren, Sherri Arp, Carlos Orozco, Jason Palumbo, Aaron Bice, Eulia Garrolini and David Burpoe.

Lizzie: Our podcast is produced by James Morrison, and me, Lizzie Peabody. Our associate producer is Nathalie Boyd. Executive producer is Ann Conanan. Our editorial team is Jess Sadeq and Sharon Bryant. Mimi Plato writes our newsletter. Episode artwork is by Dave Leonard. Transcripts are by Russell Gragg. Extra support comes from PRX. Our show is mixed by Tarek Fouda. Our theme song and episode music are by Breakmaster Cylinder.

Lizzie: If you have a pitch for us, send us an email at Sidedoor (@) si.edu. If you want to sponsor our show, please email sponsorship(@)prx.org. I'm your host, Lizzie Peabody. Thanks for listening.

Ari Redbord: *I can't believe I'm talking about me judging hip hop on a podcast right now.*

Lizzie: *[laughs] Don't worry.*

Ari Redbord: *But this is gonna be a pretty cool moment if this makes it. [laughs] Really hoping this makes it.*

-30-