



HOUSE OF LORDS

Financial Services Regulation Committee

Corrected oral evidence: Growth and proposed regulation of stablecoins in the UK

Wednesday 11 March 2026

10.05 am

Watch the meeting

Members present: Baroness Noakes (The Chair); Baroness Bowles of Berkhamsted; Lord Davies of Brixton; Lord Eatwell; Lord Griffiths of Fforestfach; Lord Hill of Oareford; Lord Hollick; Lord Lilley; Lord Sharkey; Lord Smith of Kelvin; Lord Turnbull; Lord Vaux of Harrowden.

Evidence Session No. 10

Heard in Public

Questions 101 - 112

Witnesses

[I](#): Matthias Bauer-Langgartner, Head of Policy, Europe, Chainalysis.

Examination of witness

Matthias Bauer-Langgartner.

Q101 **The Chair:** Welcome to the second part of today's meeting, which is the 10th oral evidence session as part of the committee's inquiry into the growth and proposed regulation of stablecoins. A special thanks to you, Mr Bauer-Langgartner from Chainalysis, for attending to give evidence to the Committee. The session is open to the public. It is broadcast live and is subsequently accessible via the parliamentary website. A verbatim transcript will be taken of the evidence and will be put on the parliamentary website.

Mr Bauer-Langgartner, I believe you will make an opening statement before we get into questions.

Matthias Bauer-Langgartner: Yes, thank you, Chair. Thank you, my Lords. I am joining you remotely today because, unfortunately, I feel a bit unwell, but I am grateful for the opportunity to give evidence today.

I represent Chainalysis, the blockchain data company. For over a decade, we have been working on the intersection between technology and global finance. Our tools support law enforcement agencies, including the NCA and the Metropolitan Police, in investigations involving crypto assets. They also underpin compliance, fraud prevention and cybersecurity programmes at the world's biggest crypto exchanges and financial institutions.

We have seen stablecoins grow from a niche product to the dominant asset on public blockchains. Now they account for more than half of the volume that is transacted on blockchains, increasingly acting as a 24/7 borderless programmable payments infrastructure.

We broadly welcome the proposal of the FCA and the Bank of England on stablecoins because we think that supervising stablecoin issuers is in effect supervising financial intermediaries and, as such, the same clear prudential and conduct rules should apply, mainly around robust reserves, strong disclosures, strict AML/CFT regimes but also, importantly, the legal right of redemption at par. At the same time, some material pinch points around remuneration, holding limits, which I am sure you have just discussed, and the composition of backing assets, still risk discouraging issuers to locate in the UK and also affect its competitiveness.

It is our experience as a blockchain intelligence provider to the public and the private sector that brings me here today. I want to focus my main message on what blockchain data and also analytics can bring to supervision and compliance and why that transparency should lead us to a more data-driven, more proactive regime rather than replicating legacy systems.

For all their benefits, criminals are exploiting stablecoins. In fact, they are increasingly used in scams, in frauds, in sanctions evasions, and now account for 84% of all the illicit flows we have recorded on chain, according to our latest studies.

Unlike the opaque nature of physical cash or offshore bank accounts, though, stablecoins typically operate on public and permissionless ledgers, which are inherently transparent. Every transaction is recorded in a public ledger, and that creates this unique opportunity to derive insights into behavioural and risk patterns in near real time. The opportunity, of course, depends on high-quality data and auditable methods to deliver reliable, repeatable and also code-worthy insight that will protect firms and also consumers.

The UK should not only think about blockchain analytics, used properly, as a supervisory or compliance tool. It should think a little bit broader as part of its cybersecurity and national security programs. Realising this opportunity requires more than just a new rulebook. It requires a shift from auditing paper-based reported data to supervising a more dynamic 24/7 data flow. Here we see two concrete opportunities for the UK stablecoin regime.

The first one is around enabling firms to prevent harm rather than just reporting it. Blockchain analytics today already help firms to understand direct AML risks, but the same tools can also be used to protect consumers, for example, by flagging transactions or blocking transactions to known scam clusters before losses occur, fully in line with the FCA's customer duty guidelines. The regime should further encourage these types of proactive usage of analytical capabilities. Also, secondary market monitoring is important. Analytics today already show issuers how a token is circulating and where high-risk patterns emerge. The UK should clarify expectations for secondary market observations and when issuers may and should work with authorities to proactively freeze illicit funds before they are laundered or cashed out with appropriate safeguards for compliant users.

Then, secondly, we also have this opportunity to make supervision more efficient and more data driven. High-quality and off-chain data allows regulators to shift from periodic paper-based reporting to overseeing on a risk-based continuous track. The FCA, for example, could analyse risk trends across all regulated firms. In an instant, it could benchmark AML exposure. It could drill down into specific entities, specific firms, even specific transactions if it wanted to, or verify a firm's claim against objective on-chain data. The same applies to financial intelligence units or FIUs. The more analytics-informed these suspicious activity reports are, the more actionable they are and the better you can link them together, giving investigators a much quicker view of what is happening.

Over time, we believe that this will cut the reporting burdens for firms. It will also boost supervisory efficiency—think about regulators pulling data instantly rather than requesting it. This will strengthen the UK's competitiveness as a financial centre. For the UK to remain an

international hub, particularly as stablecoins and other crypto assets become more mainstream, the framework for stablecoins should focus and aim to be as interoperable and as cross-border as the technology that it tries to regulate, leveraging the technology to preserve financial stability but also focusing on consumer protection.

Embedding high-quality data and analytical capabilities into a supervisory and compliance framework will make the entire system much safer and much more attractive, including for responsible innovation in the longer term. It is our belief that we can use this technology's transparency to regulate the movement of the value of money rather than just institutions. Thank you very much. I look forward to your questions.

Q102 The Chair: Thank you very much indeed for that introduction. In the course of our inquiry, we have been learning about a whole new ecosystem, and so forgive some of us for any ignorance in how that works.

You have explained the capabilities that your organisation offers. Could you explain who your customers are. Do you have other competitors? Are other organisations like yours offering the same services, or are you unique in this new ecosystem? Can you give us a little bit more background about how this works?

Matthias Bauer-Langgartner: Yes, I am absolutely happy to. The most important point about Chainalysis is that we are not a crypto asset service provider. We are not issuing tokens. We are not exchanging tokens. We are working together with all stakeholders within this new ecosystem that is emerging. That includes virtual assets service providers or VASPs, crypto asset service providers or CASPs, or however you want to call them. This includes regulators, law enforcement agencies and even national security agencies.

The best way to explain what Chainalysis does is probably to think about how blockchains work. Public permissionless blockchains offer transactional transparency. That essentially means that every transaction is recorded into that publicly readable ledger. It tells you that wallet one has sent a specific amount of crypto asset or stablecoin to wallet two at a specific point in time. That is transactional transparency. You can look those transactions up in commercial products like Chainalysis, and there are also competitors out there. You can do this with freely available blockchain explorers as well. You will always find the entry of a specific transaction, outlining the recipient, the sender, the amount and the time.

It does not give you, though, an understanding of who is sitting behind those types of addresses. That is exactly where Chainalysis comes in. We look at the raw data of blockchain transactions, and then we map those transactions to real-world entities. We are literally looking for evidence that links a specific address—which you can see as akin to a bank account—to a real-world entity. We have more than 100 analysts with loads of technical capabilities who look through the entire internet, also the darknet, social media channels, WhatsApp and Telegram channels, to

find evidence that a specific wallet belongs to a specific entity. That entity could be a crypto exchange like Coinbase, Bitpanda or Kraken. It could also be a darknet market. It could be a sanctioned entity or jurisdiction. It could be an address associated with terrorist financing. All of this is then labelled in our products and visible.

That is only the first part of the service that we provide. The second part is where it gets interesting because, once you have that evidenced, deterministic attribution of a specific wallet to a specific entity, you can then look into the entire transactional history of that specific wallet address to understand whether that specific address might be controlled by an entity that also controls other addresses. You start to understand the network much better. We call that heuristics. We have more than 400 of those algorithms that allow you to cluster and collect addresses together.

A good example, to make this a little bit more tangible, is when you think about the bitcoin network and you own some bitcoins on different addresses. You have one address that holds one bitcoin, you have a second address that holds a second bitcoin, and you want to make a transaction to your counterparty worth two bitcoins. Instead of sending one bitcoin in two transactions, you can just merge those two addresses and make one transaction sending from two wallets at the same time to one recipient. This allows us to understand that the same two addresses are controlled by the same entity. We cluster all those transactions together.

This is an extremely powerful tool. It essentially gives you much more context. To give you an idea of how powerful it is, when you think about sanctioned wallet addresses, roughly 1,500 addresses at the moment have been designated currently globally. If you look into our products and you look for the specific category of sanctioned wallet addresses, you will find more than 9 million of those addresses, simply because we can link all the transactional activity back to those addresses. It is important to get that methodology right.

As to analysis, we have gone through an intensive so-called Daubert hearing in the US in a court case to validate all these methods. It is important to make sure that these methods are deterministic and based on evidenced data to give you the 100% certainty that you need for blockchain analytics.

Again, to summarise and make it a little bit more plastic, if you are looking for a specific address on chain, instead of seeing a transaction from A to B, you open that same transaction in that commercial tool and you will suddenly see that the first address, for example, belongs to Coinbase or Bitpanda, and is part of a cluster that includes more than 10 million addresses, and it is sending funds to another exchange or darknet market. This is the real value that Chainalysis brings.

Q103 Lord Lilley: Thank you very much indeed. That explained a lot of things I did not know. However, it raises the question of why criminals use this

if they are exposed to public gaze.

Matthias Bauer-Langgartner: That is a good question. Essentially, criminals use stablecoins for the same reasons that legitimate users would use them. They are a good way of moving value instantly, cross-border, and there is literally no better way to move funds at this moment. The main risk for criminals, though, is the fact that centralised stablecoin issuers use their power to freeze funds. That is a massive risk. They typically do that. I am trying to say that stablecoins are a good way of transferring value across the globe because they are global and instant. They are also easily reachable and very liquid. Instead of, for example, accepting bitcoin and others, they want to have a stable value they can count on.

Transparency is a massive gamechanger for us to fight financial crime, but of course there are also ways to obfuscate the origin of funds. Fraudsters and scammers would typically use things like mixing services that allow people, for example, to join certain transactions into one comingle fund, essentially, and pay them out again. Typically, the conception was that these would hide the trail of funds quite well. However, effectively, it is an arms race against scammers. A lot of the mixing services that exist today can automatically de-mix and so you have to do some manual work as well.

The main gist is that they are the best way to transfer value cross-border. A lot of the scam compounds, for example, sit in south-east Asia with victims being in the US, the UK and Europe.

Q104 **Lord Sharkey:** I have two short questions. First, what confidence can you have in your identification of users, and how do you assess that confidence level?

The second question is about the reversibility or not of blockchain entries. We have heard two slightly contrasting stories. One is that they are not reversible and you have to generate a fork in the chain. The other is that you can reverse it by sending the money back, which seems so simple as to be unlikely.

Matthias Bauer-Langgartner: Yes. Maybe let us start with the second question before I go into the methodology question.

Are blockchains immutable? Yes. Generally speaking, different types of blockchains work differently to try to make sure. The nodes that are part of the network conclude what the ledger should look like but, generally speaking, they are not transferable at all. Once you have a transaction added to the blockchain ledger, that is where it is and that is where it will stay.

That is also true for stablecoins. Stablecoins use that underlying decentralised infrastructure. They work on, for example, Ethereum or Solana or Polygon. There are many different technical levels, but they are all centrally orchestrated. A central party issues them. They are not a decentralised business model or business operator. They have the ability

to use their smart contracts applications—and so it is on the application level, not on a technical blockchain level—to economically reverse transactions.

For example, if funds are sent from a victim's wallet address to a scam cluster, they have the opportunity, including via on-chain analytics, to see that these funds have arrived at the scam cluster. They can then freeze those assets, which technically means that the stablecoin is not accessible any more to the original holder, the scammer. Because they still have the reserves in place, they can then reissue the token to the victim. Economically, you can reverse transactions, but it is not technical reversibility. It is economic reversibility. All these transactions, the freezing of stablecoins and the reminting of stablecoins, would be documented on the chain.

Lord Sharkey: Who decides to freeze?

Matthias Bauer-Langgarter: Exactly. This is the crucial question. At the moment, the way that the AML systems work and the entire system works is that, typically, issuers and also other financial institutions and crypto asset service providers have obligations towards the direct counterparties. They have to do transaction monitoring for all the incoming and outgoing transactions. They have to know where to send the funds and also where funds are coming from.

The beauty with blockchains is that you can also look into transactions that are further away than the direct transactions that you receive, which gives you a much clearer picture of where the funds come from. We call this looking multiple hops backwards. You can look into the last 17 transactions to make sure you understand the AML risk. If you, as a recipient, understand the AML risk to be very high, that is when you have to file a SAR and that is when you have to freeze those funds, including as a stablecoin issuer.

Lord Sharkey: I am not clear about the timeline involved in all this because the money will have moved on by the time you get to lower the temperature.

Matthias Bauer-Langgarter: Yes, exactly. That is exactly the problem. Speed is one of the main elevating risks with stablecoins because they can, in an instant, essentially, cross 15 jurisdictions in an afternoon. That is of the essence.

That is also why, for example, at Chainalysis, we are working on tools that allow crypto asset service providers and stablecoin issuers to automatically freeze transactions if they are detected as high-risk funds, for example, from sanctioned entities, child sexual abuse material or terrorist financing.

The second part that I wanted to allude to is that this is how the traditional EML system works at the moment. You look into all the transactions that you are part of and you look into your counterparty and

you assess AML risks. What we do not have at the moment—and is something that we as Chainalysis advocate for—is to think about how we can use all that intelligence that we have on stablecoins to also look into the secondary market of all the transactions that a stablecoin issuer is not part of. Typically, if you are involved in illicit activity and you build something like a circular economy by sending stablecoins from A to B—for example, from a drug net vendor to postage services or precursor materials—they typically do not hit a regulated exchange that would look into the AML risk of that specific transaction. In a way, it is well lit but there is also a blind spot within the crypto assets ecosystem as long as those funds do not hit a crypto exchange or regulated exchange that needs to look into the AML risk, including with stablecoin issuers, who typically do not have a lot of retail involvement. They mostly focus on businesses they work with to distribute.

Q105 Lord Hollick: You and other witnesses have pointed out the benefit of stablecoins to the criminal fraternity, people who are shy about having a compliant relationship with the tax authorities, people who want to invest in crypto because it is a good jumping-off platform, and also those who are seeking to move money in and out of difficult-to-trade currencies. Given all of that, what is the benefit to the real economy? How does this technology help us to put more money to work in the economy, to grow the economy, to help people to live their lives?

Matthias Bauer-Langgartner: Thank you very much for that important question. We are seeing currently that stablecoins are evolving from just providing the oil for crypto trading, typically being the second leg of a crypto transaction, into a more global cross-border payments network.

A few pointers show the direction. Stablecoins will revolutionise parts of the payments infrastructure. Witnesses before me have pointed out cross-border payments a lot and also agent payments and programmable payments. There is a case for it and some data supporting this.

The first thing that I would like to mention is that stablecoins have grown from a niche product to more than \$300 billion in market capitalisation. More than half of all the transactions that are happening on chain are already in stablecoins. We have seen that they are decoupling because the transactional volume of stablecoins is increasing partly twice as much as traditional crypto assets.

Also, when you look at the past, back in October 2025, for example, Bitcoin hit its all-time high, but now has lost half of its market cap today. Stablecoins, however, have increased their market cap since then, showing that the trading of crypto assets, which is still the main use case for stablecoins, has decoupled slightly.

We can also see this in the real-world economy, including in the UK. In fact, according to our data, the UK is leading in native on-chain merchant payments. These companies enable real-world economies, real-world commerce, to accept stablecoins directly and then process them via those

crypto and stablecoin processes. In fact, you could use any crypto assets, but around 60% to 80% of those transactions are facilitated in stablecoins.

Lord Hollick: If I may interrupt, in the UK, we have a bank system, which is free, to transfer money around and so I am not sure that is a benefit to the real economy. If I want to borrow some money to buy a house or to help my business, what can crypto do for me?

Matthias Bauer-Langgartner: If you think about purely domestic use cases, we are just starting to see them because, as you point out, the UK has efficient payment systems already.

However, secondly, when you think about cross-border payments, then stablecoins become an attractive option to send money across the globe. That is also why fraudsters are using it. In fact, 84% of all illicit activity on chain is in stablecoins since 2022 because people realise that stable value transfer on chain is the most efficient way to do this.

When we will see more uptake, including in the UK, is once we move into more agentic payments. For me, blockchains and AI rails are complementary technologies. AI is delivering the intelligence layer, thinking about what you want to do. If you want to buy a specific pair of red socks for a certain price, which is roughly where we are at the moment with agentic payments, at the beginning of development, those agentic agents could themselves hold wallet software. They could hold stablecoins themselves and could interact. Stablecoins could allow much smaller denominated payments or micro payments and higher-frequency payments in this new agentic world. We are just at the beginning of this new wave, but I am pretty sure we will see that.

I am thinking about, for example, AI models paying for content in micro pence, paying for compute while you use that, paying for newspaper articles, or whatever it might be. We are pretty much at the beginning, but stablecoins will provide a good interface into AI-enabled technologies and allow this auditable trail of financial interactions. I hope that answers your question, a little bit at least.

Q106 **Baroness Bowles of Berkhamsted:** Thank you very much. It is interesting what you have just been saying. A lot of that business is related to new types of business that will evolve rather than old business types of things that we are buying at the moment.

Overall, based on the data that you are looking at, where do the biggest risks lie in the stablecoin ecosystem? Where is it most likely to go wrong? Is it with issuers, exchangers, wallets, the cross-chain infrastructure? This is getting away from issues of fraud as such, but where are the biggest risks?

Matthias Bauer-Langgartner: This new emerging stablecoin ecosystem has multiple risks that one should care about.

The first one is this fiat peg. The proposal focuses on ensuring that there is £1 in a specific asset backing every £1 issued on chain. That is one of the most critical parts of the stablecoin regime that you should think about.

There are also other risks around cybersecurity, particularly around smart contract interactions, because bad actors might intend to get access to a smart contract and then effectively be able to either mint new tokens or new stablecoins, which are not backed by anything else, or stop the stablecoin system from working at all. That is why, as a company, we have focused a lot on cybersecurity, not only in the traditional way of auditing but in the new way, as we feel, looking at specific on-chain transactions and the transparency of on-chain transactions. Blockchains allow you to not only see the transactions on chain but also see who is trying to interact with you and the parameters of that interaction. Is the smart contract that you are interacting with malicious—yes or no?

This can also lead to some financial risks, including for the UK if the backing assets are, for example, UK gilts, and if stablecoins become systemic, which they are not at the moment. Bad actors could think about trying to get an issuer's reputation to a point where people are trying to orchestrate a stablecoin run, a bank run, which might end up in a fire sale of, for example, UK gilts and have an impact there.

The third part is around this secondary market. Stablecoins could be used—and as I said before, they are increasingly used—not only for scams and fraud but also for sanctions evasion. It also becomes a question of national security at some point. We need to make sure that the secondary market itself is also accounted for.

Baroness Bowles of Berkhamsted: How would you make a fake stablecoin? You referenced that.

Matthias Bauer-Langgarter: I am basically focusing now on the issuers. A stablecoin, technically, is an entry within a smart contract. The issuer is adding a new line saying, "We have 1 million of stablecoin X". These then can be transferred to other addresses. Now, if a bad actor gets access to that admin key, they could just include a line saying, "We have just minted 15 million new tokens", and they would then be able to transfer those around, which would have a catastrophic effect on the stablecoin issuer and the stablecoin itself. It is not a fake stablecoin. It is a fake issuance, so to speak, because then you have an imbalance between the stablecoins that are circulating and the reserve assets with all the implications that that has.

Baroness Bowles of Berkhamsted: Would you be able to tell the difference once that is in circulation? It is not like in the olden days when you could bite the coin and feel that it was not the right metal. Is there no equivalent of that?

Matthias Bauer-Langgarter: No, in this case, you cannot even bite the mobile phone. It is an entry visible to everyone and you can see who

is behind that transaction. It gives you an idea. The problem is with impersonation; if you get access to the main keys, it looks as if the stablecoin issuer itself would issue that. They would have to rectify this. That is why it is important to have strong cybersecurity rules around the issuance of stablecoins.

Then the other thing around the ecosystem that I would add is also the importance of exchanges. It is vital to have exchanges that not only do proper KYC—we are already in a world where the KYC/KYB of exchanges looks pretty much like traditional finance—but even better because they have this benefit of looking into further transactions backwards. They are vital because most of the criminals across pretty much all the categories are trying to cash out at centralised exchanges. That is why it is crucial to get regulation right there.

Q107 Lord Turnbull: We are quite a way through the consultation process in the UK. The Bank issued proposals in November. Representations have been made. This committee has held hearings. I do not know whether you heard it, but we had quite a robust defence of those proposals earlier this morning. In the next few weeks, the Bank will make up its mind.

What areas, if any, do we want to modify our proposals in? Do you have any wisdom to offer them, saying, "You may have been thinking of doing this, but you should do something else or more of that"?

Matthias Bauer-Langgartner: Generally speaking, the proposals of the Bank of England and the FCA align with global standards, which is important.

One thing that I would add is that it should be considered how the stablecoins issued in the UK are also interoperable with other regimes globally, for example, the MiCA regime in the EU, but also GENIUS in the US and vice versa, to make global stablecoins global rather than having them boxed into specific regulatory regimes. That is also highly debated in the EU at the moment.

The second thing is thinking about what benefits the use of blockchain technology can bring, not only to the issuers themselves and customers, but also to supervisors. We are still at the point where we can harness much more benefits from blockchain analytics because it gives you a much better overview of transactional behaviour. It is 24/7. It is not reported. It is factual evidence that you can see. You can use that to supercharge and boost supervisory efficiency doing that.

Most importantly—I have already said it a few times—we should start to think about how we deal with secondary market transactions because, at the moment, they are the blind spot here.

Lord Turnbull: Is there anything in those proposals that you think they should drop or severely modify?

Matthias Bauer-Langgartner: I know that there is lots of discussion around holding limits, for example, which, as far as I am aware, has not

been discussed somewhere else. Also, the EU is not considering having any holding limits, including in the upcoming MiCA review. That is clearly the case. There is also quite some discussions around backing assets.

Q108 Lord Davies of Brixton: In the briefing document we have been provided with, there is your interesting histogram of how use of bitcoin has declined precipitously and use of stablecoin has more or less taken over the criminal market, which I suppose in a strange way is testimony to their efficiency, for what it is worth. You also say that your estimate of criminal use is less than 1%.

Has that figure shifted at all over the five years that you have monitored these figures? The market is expanding. Has the 1% increased in line with the market?

Matthias Bauer-Langgartner: Yes, that is a good point. Thank you very much for raising that. Stablecoin usage by both criminals and fraudsters and for sanctions evasions mainly—sanction evasion happens to 95% in stablecoins—is testament to their efficiency. We have seen that, since 2022, stablecoins have taken over from bitcoin as the preferred asset of choice.

Bitcoin is still preferred in certain categories, including ransomware attacks, for example, simply because more sophisticated users do not want to expose themselves to the possibility of having their funds taken away. Stablecoin issuers, as I said before, can freeze funds in an instant, no matter where they are or who holds access to these types of funds, which is something that people do not want.

When it comes to the overall figure of under 1% of illicit activity globally, in the last five years this figure has not materially changed. It has fluctuated, absolutely, but has always remained below this 1% figure, which of course is also a rather conservative estimate. As I said before, we take all the rigor necessary before we label a specific address as illicit funds more broadly. We might not yet have detected some illicit usage.

Also, we know, thanks to multiple investigations, that in most crimes, crypto is used in some way, shape or form. If you do not pair some off-chain intelligence—for example, investigations into drug markets, solely from an on-chain perspective—a lot of those transactions that happen, for example, between two drug dealers would not be recognised by our systems as such if there is no way to connect them to a bigger cluster that we have already identified. It is a rather conservative estimate.

Q109 Lord Griffiths of Fforestfach: What are the main income streams of your business? Where do you make money? You have 100 or so people working for you. What are the products that you are selling and how are they doing?

Matthias Bauer-Langgartner: We have more than 800 or 900 people already.

Lord Griffiths of Fforestfach: My apologies for underestimating.

Matthias Bauer-Langgartner: Chainalysis is a force. We have loads of different products and we are selling access to our software. Increasingly, we are also selling access to the data that we create.

Think about law enforcement agencies. They are now increasingly looking into finding traces of crypto because, as I said before, pretty much every crime has a crypto angle to it. The second they find an address, they can use our tools instantly, even on a mobile phone, to check whether that address holds some funds, crypto, whatever it might be. Then they can use our tools to trace back the transactions to understand the flow of that specific bitcoin, Ethereum, stablecoin, and link it even to scam clusters.

The NCA, for example, had a case around a ransomware payment. The payment was made and it was received. It was a bitcoin transaction, if I remember correctly. Based on that specific transaction, they looked at the contextual information and were able to dismantle a multibillion-dollar Russian money laundering network—just because of that one single transaction. That is for law enforcement.

For exchanges, what we do is typically know-your-transaction systems. They also investigate, but the starting point of every investigation is knowing your transactions. Every transaction that a cryptocurrency exchange receives will be screened by our tools. It will give you information on the sender and the specific AML risk attached to it. We do not score transactions or entities, but we will give you a complete understanding of previous transactions. We will say, “These funds are directly derived from a darknet market, which looks like someone who has sold some illegal goods on a darknet market”, or we might say, “This is the fifth transaction, and five hops back is some exposure to terrorist financing”, for example. A cryptocurrency exchange can look at that specific risk exposure and think about whether it is within its risk appetite or whether it should freeze those funds because of the AML risk attached to it.

Then we also work with regulators, precisely for AML reasons but increasingly also for supervisory purposes. If an exchange, for example, comes to a regulator and says, “We have an operating business that would like to set up locally here”, a regulator could just look into all their transactional history and understand how they are behaving on chain. What are the counterparts, for example, of that specific exchange? Where do funds come from and where do their customers send funds to? That gives you a good understanding of where an entity is sitting and its AML risk exposure. You can do this over time even for supervisory purposes because you can see how the transactional patterns move and change. Is a new AML policy effective, yes or no?

Then we also work with national security agencies mainly around cybersecurity threats and national threats because, as I said before, sanctions evasion is becoming industrialised, not only in Iran, Russia and North Korea. That is where we protect our customers.

The reason why I said we increasingly sell not only services but also data is because of the massive shift in how analytics works. It is getting much more customisable to look for the type of information you need and to surface that insight in the way that you need it.

Stablecoin issuers, for example—and that is what I am talking about when I am thinking about secondary market observations—can use all of that intelligence and essentially see that transaction number 17015 has just been received by a cluster that we have identified as terrorist financing and it is sending funds on or a sanctioned entity. With that insight, stablecoin issuers can assess whether it is appropriate to freeze those funds and deter financial flows.

However, the problem that we have at the moment is that there is no clear regulation around how and when they should do that and how they work with law enforcement. As was pointed out before, stablecoins are extremely quick. Time is of the essence. Sometimes it is just too late to do that.

Q110 Lord Vaux of Harrowden: You have described this extraordinary transparency and the amount of data that you can take out of the system, but does this create an enormous privacy concern? If the use cases of stablecoin take off, as people talk about, you would be able to see every transaction that I have ever made on it. You would be able to see, for example, a company that is paying its staff, what every employee is paid, and all the rest of it. Is this an enormous privacy problem?

Matthias Bauer-Langgarter: Yes, it is a good point that you point out privacy because, when you think about what we do as a company, we are not attributing wallet addresses to individuals. We are attributing them to services—for example, exchanges, OTC desks, darknet markets, payments processors. You would be able to see only that the transaction originates from Coinbase, Bitpanda, Kraken or a specific OTC desk. We do not have any information on individuals. We are not tracking individuals' transactional history. We are just tracking institutional flows.

Individuals sit behind those institutions. That is the typical way that investigations work. If law enforcement is tracing transactions back to a regulated exchange, they would then have to pick up the phone and inquire about the identity and the KYC information of that particular individual that has access to or has sent funds to this exchange. We track only Coinbase, Bitpanda and Kraken, but not individuals behind it.

Lord Vaux of Harrowden: If I receive a payment from somebody and I know who that is because I can see their wallet identity or whatever, I can then see what else they have transferred money to or from over huge amounts of time. Anyone can do that. It does seem open to abuse. Am I misunderstanding?

Matthias Bauer-Langgarter: If you are receiving funds from a business partner and you know their wallet address, you would see the

transaction. Everyone else would also see the transaction. You can then use our tools, if you have access because access is restricted to these types of tools, to follow the funds. You could also do this manually with freely available software. Yes, you could do that.

That is also why, for example, payments processors disperse funds in a way that cannot be attributed to individuals any more. Also, when you think about exchanges, most people will stay with regulated exchanges. Self-custody is an important thing for stablecoins and crypto assets more broadly, but not a lot of people will have self-custody of funds. If you send transactions from an exchange, there is no way that you could track through an exchange. If your business partner is holding an account with a crypto exchange that is sending you funds, you have no way to understand any of the network because it all ends up with Coinbase, which is a massive cluster of transactions, and there is no way you can link that. The only way to do what you have described is if you have an individual wallet address that sends you a transaction and you know personally that that specific wallet is person X or business X.

Q111 **Lord Lilley:** I am getting confused. You were saying that most things go through exchanges and then they cannot be traced. How do you do the tracing?

Matthias Bauer-Langgartner: That is an important point. Whenever we do our tracing, we are tracing back to the last regulated endpoint. That typically is a cryptocurrency exchange because most of the transactions originate at regulated exchanges.

Let us put it the other way around. If someone is selling drugs and we have detected that flow, we then look at typically how money launderers would like to launder. One pretty basic typology is sending funds around five different addresses before they are sent to a cryptocurrency exchange to convert it into fiat money. We can trace those five hops and we can trace the transaction back to that specific cryptocurrency exchange, but that is where our tracing stops because it commingles so many funds of millions of customers that you cannot trace through that.

Crypto asset exchanges operating by having a specific wallet address where they essentially commingle all the customers' funds. It is segregated wallets for their customers. It is not individual wallets per customer. That is also why you have to trace back to an exchange and ask for further information on that specific individual. If you want to, I can also go a little bit into how custody generally works at cryptocurrency exchanges. Let me know.

Lord Lilley: Yes, please. Sorry, could you do that, either now or in writing?

Matthias Bauer-Langgartner: Cryptocurrency exchanges buy and sell crypto assets and they also custody crypto assets to a massive extent. What they typically do for security reasons is they have segregated accounts, just like in the normal fiat world, where they hold all their

assets securely—typically, in so-called cold wallets. These wallets are not connected to the internet, which makes them much safer from cyberattacks. They are harder to move, but they are securer. Typically, I would guess, around 95% to 98% of customer funds are securely in those air-gapped cold wallets offline. Only a smaller portion of crypto assets are held in wallets that are directly connected to the internet, essentially to allow transactions to be effected with customers when they have to do transactions on chain.

Most of the transactions at cryptocurrency exchanges internally are done internally. A lot of them will not be transactions on chain because people are trading, for example, against a cryptocurrency exchange. If customer A is selling and customer B is buying, the only thing that happens internally at an exchange is that they will just change how these funds are allocated rather than having to effect a crypto transaction on chain.

Lord Lilley: There will be no record of B to C or C to B?

Matthias Bauer-Langgarter: Yes, if it is internally with an exchange, it is just an internal entry but not a blockchain transaction.

Q112 **Lord Smith of Kelvin:** I have two questions. First, you have explained what you do for a living. I would be interested to know what your customer base looks like, what your competitors look like, how you get business and so on, and if it is growing.

The second one is a basic question. Are the UK regulators doing enough to monitor illegitimate and illicit use? I had written down here, “Or too much”, but I should not ask that. You will not give me an answer to that. You talked a bit about the UK fitting in with the US and EU. Tell us how that might develop.

Matthias Bauer-Langgarter: What does our customer base look like? At the moment, it is already roughly split in two halves between public sector customers and private sector customers. A few years ago, it was more tilted towards public sector customers but, as supervisory regimes across the globe are emerging for crypto assets, more private sector companies are coming into this space, including the big traditional finance players that have waited for regulatory certainty to further explore and take the first steps into crypto assets. A lot of them are currently thinking about custody solutions for their customers. Particularly in places like the European Union, we see a lot of uptake in stablecoin issuance. There are more traditional financial services players, including in conglomerates, in networks, in consortiums, building up stablecoins. The private sector is growing.

Generally speaking, the entire industry is growing. The crypto assets industry is growing and, with it, analytical capabilities are growing. That field has a lot of competition, as you know, and the interest is picking up as well. They are coming from all walks of life.

The Chair: Mr Bauer-Langgarter, that was a fascinating session. It has given us new insights into this world that some of us find a little strange.

It has been helpful to our inquiry. Thank you very much for your evidence today. Thank you.