Future of crypto investigations and enforcement:
the investigator's and lawyer's perspective

FORENSIC RISK ALLIANCE

Ogier

Newsworthy events and reader interest abound, whether it's the collapse of a high-profile custodian / exchange, the ongoing volatility of Bitcoin's trading price, or simply intrigue about what the future looks like in this evolving space, as crypto and virtual assets continue their relentless march to disrupt traditional fiat currencies.

Our panel – an expert investigator of cryptocurrency enabled money laundering and computer intrusion incidents, and a lawyer specialising in contentious regulatory matters - explore the latest themes in crypto investigation and enforcement, and look ahead at potential future trends in this space.

Who's who

Speaker

Meredith Fitzpatrick - Director of Cryptocurrency, Investigations and Compliance Forensic Risk Alliance (FRA)

Meredith joined FRA's Washington, DC office as Cryptocurrency Director after seven years as a Special Agent at the Federal Bureau of Investigation (FBI). She is a subject matter expert in the investigation of cryptocurrency enabled money laundering and computer intrusion incidents, including Russian state sponsored computer intrusions, non-compliant cryptocurrency exchanges, theft of Personally Identifiable Information and Intellectual Property, ransomware, dark-web marketplaces, and Business Email Compromise (BEC) schemes. Meredith has extensive experience working multinational investigations and collaborating with foreign intelligence services and law enforcement agencies to solve complex investigative issues.

At FRA, Meredith uses her investigative experience and deep ties in the crypto and blockchain intelligence industries to develop solutions that support organisations resolving issues associated with cryptocurrency and emerging financial technology. Meredith has used her blockchain expertise to investigate cryptocurrency enabled money laundering, wash-trading allegations, and high-value cryptocurrency thefts.

Speaker

Tom Hall - Managing Associate
Ogier

Tom is a Dispute Resolution lawyer based in Ogier's Jersey office in the Channel Islands. As a leading international financial centre, Jersey is one of the world's foremost jurisdictions in the measures it is taking to combat financial crime.

Tom specialises in advising on contentious regulatory and white-collar crime matters, including money laundering, proceeds of crime and sanctions advisory and defence work. He also advises leading onshore and offshore companies, financial institutions and office holders on multi-jurisdictional fraud, asset tracing and recovery actions, whether in the context of litigation or insolvency, which will often have a virtual asset dimension.

Moderator

Andy Carpenter - Senior Consultant
(Virtual Assets and Blockchain), Ogier Regulatory Consulting

Andy is a senior consultant at Ogier Regulatory Consulting. He is an experienced fraud / financial Investigator and is also a digital forensics expert specialising in crypto fraud, open-source intelligence, AML and crypto investigations / prosecutions.

Andy is an expert in the use of NUIX, Graykey / Axiom, Cellebrite, XRY, FTK and other digital forensics, blockchain analysis and e-discovery tools. He has spent the last 20 years in both public sector law enforcement and private sector consultancy firms managing complex and technical cases. After completing a number of ICA qualifications, he shifted his focus to AML/KYC and source of wealth controls, especially with regards to virtual assets.

He is passionate about anti-money laundering, blockchain, crypto, fintech, virtual assets and emerging technologies.

Investigations

Another thing to keep in mind is what kind of illicit goods and services you can purchase using cryptocurrency.

Does crypto really offer financial anonymity? How is the ecosystem being used by illicit actors, and what are the main challenges facing investigators?

Andy Carpenter moderates a discussion with Meredith Fitzpatrick and Tom Hall exploring key questions at the centre of crypto investigations.

The cryptocurrency industry is no longer operating in the "Wild West" as it was in its infancy.

AC: Despite the know your client / anti-money laundering (KYC / AML) requirements of centralised cryptocurrency exchanges and the ability to use blockchain analytics to trace the flow of funds, some policy makers still claim that cryptocurrency remains the method of choice for criminal networks and terrorists. Can you separate fact from fiction?

MF: This is a great question to start off on as it touches on the important differences between Traditional Finance (TradFi) and cryptocurrency.

The cryptocurrency industry is no longer operating in the "Wild West" as it was in its infancy. Centralised cryptocurrency exchanges (commonly referred to as a Virtual Asset Service Provider, or VASP), are the most common way people interact with the cryptocurrency ecosystem, whether it be to convert fiat currency to cryptocurrency and vice versa or to trade cryptocurrencies. The majority of VASPs have KYC / AML programs and powerful blockchain analysis tools with robust attribution data. More importantly, governments around the world have shown that they have crypto-savvy investigators and the means to affect large cryptocurrency seizures. The belief that cryptocurrency offers financial anonymity for illicit actors has largely been debunked at this point.

However, one major departure from TradFi is the concept of a non-custodial wallet, and these are commonly used by illicit actors to remain anonymous. A non-custodial wallet is a wallet software or hardware in which the user of the wallet retains total control of the private keys, seed phrases, and activity of the wallet. Importantly, non-custodial wallets like MetaMask, Electrum, and Trezor do not collect KYC information. If someone exclusively used non-custodial wallets, it would be akin to someone operating exclusively in cash and never creating an account with a centralised body like a bank.

There are also cryptocurrency mixers, which essentially provide money laundering as a service and enhance the anonymity of cryptocurrency transactions by combining transactions and funds with other pools of transactions or funds. Illicit actors can also use privacy coins, such as Monero and Zcash, which are coins with enhanced cryptography and privacy features that conceal the identity of and transaction history of their users.

Non-custodial wallets and obfuscation services like cryptocurrency mixers can make an investigator's job more difficult, but investigators have made huge strides to defeat these techniques. Using non-custodial wallets, cryptocurrency mixers, and privacy coins in conjunction also requires an immense amount of effort and technical expertise.

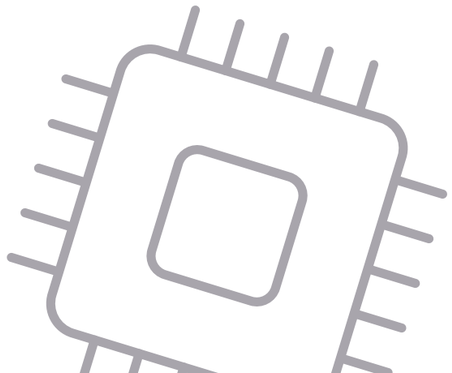
Blockchains are also immutable, permanent ledgers. It's there for all to see, forever. For the average user, cryptocurrency may offer less privacy compared with offshore accounts for companies incorporated in low transparency jurisdictions, as many blockchains leave behind a deep footprint of financial activity for those who know how to analyse it. So if attribution on a wallet is discovered in the future, investigators will be able to go back and analyse all transactions associated with that wallet in a new light. So, in my opinion, cryptocurrency presents very limited capabilities for an illicit actor to operate anonymously.

Another thing to keep in mind is what kind of illicit goods and services you can purchase using cryptocurrency. Yes, one certainly could purchase things like drugs, guns, malware, child pornography online with cryptocurrency. But could one purchase enough guns to arm an insurgency or terrorist group or enough materials for a nuclear weapon? Highly unlikely. At some point, nefarious actors need to convert the cryptocurrency to fiat currency to purchase illicit goods at scale.

TH: I agree with Meredith. While I agree that it is unlikely that crypto alone could be used to purchase weapons or nuclear materials, illicit actors are creative creatures. I would add two short points about the funding of illicit activities using crypto.

Firstly, and certainly when talking about proliferation financing, it's important to be mindful that dual-use goods are a common way to try to circumvent sanctions. By dual-use, I mean something that could have an innocuous use but also a nefarious one, such as computer chips. Anti-money laundering (AML), counter-terrorist financing (CTF) and counter-proliferation financing (CPF) considerations apply just as readily with crypto as they do with fiat currency transactions in this sense.

Secondly, to Meredith's point about converting crypto to fiat currency to purchase illicit goods. There may be an intermediary step where crypto is used to buy valuable or luxury assets such as art which is then laundered via a sale (to raise fiat currency) or traded in order to purchase illicit material.



AC: Meredith, from your experience as a Special Agent in the FBI (as part of its Virtual Currency Response Team), what challenges did you encounter in investigating crypto thefts / frauds, particularly where illicit actors (be they individuals, entities or state-sponsored organs) mask their involvement through a proxy or mule, or with use of a virtual private network (VPN), which masks their geo-location, or the use of non-custodial wallets where KYC info is not recorded?

MF: As I previously described, state sponsored and technically sophisticated illicit actors commonly use non-custodial wallets, cryptocurrency mixers, and privacy coins in conjunction to obfuscate the flow of funds. This is especially true in cases of large scale thefts and ransomware payments.

Another challenging aspect was when illicit actors would purchase cryptocurrency or "cash out" via an over the counter (OTC) exchange or peer-to-peer (P2P) cryptocurrency exchanges. P2P / OTC marketplaces match traders with one another and oftentimes have more lax compliance and reporting standards, if they even have them. The transactions occur in a closed environment between two individuals on a negotiated price outside of the market fluctuations. P2P / OTC marketplaces and brokers can create blind spots for enforcement agencies and financial institutions and are often used by nefarious actors.

The nature of crypto transactions by a given person is that they may be sporadic or frequent and higher or lower value, making it potentially less easy to discern patterns of suspicious behaviour with crypto transactions.

AC: Centralised cryptocurrency exchanges oversee millions of transactions a day. What are some flags or patterns their Financial Intelligence Units (FIUs) should watch out for to help them find the "needle in the haystack"?

MF: VASPs are swimming in data – both in transactions going into or out of the exchange and in on-platform trade data. To prevent financial crime, VASPs need to have a fit-for-purpose Financial Crime and Compliance (FCC) program that appropriately addresses the amount of funds moving on their platform and the types of financial products offered. This includes enhanced due diligence for high-risk users, robust geofencing, regular risk assessments, transaction monitoring, and trade surveillance.

However, pieces of information also need to be analysed in context. For example, someone accessing their account from a VPN doesn't automatically mean that they're trying to obfuscate their location. There are plenty of legitimate reasons to use a VPN (in fact, if you're reading this from your work computer, it's very likely that your web traffic is being routed through a VPN for security reasons). Any one data point can't be viewed in isolation – it's one component of a customer's risk profile.

TH: I agree. While in many ways, similar AML / CTF / CPF considerations will apply to crypto transactions as they do with more "traditional transactions", some considerations differ. For example, in a more "traditional transaction" using fiat currency, frequency, volume and value of transactions (or lack of them, in any case) may be sufficient to create reasonable grounds to suspect criminality. The nature of crypto transactions by a given person is that they may be sporadic or frequent and higher or lower value, making it potentially less easy to discern patterns of suspicious behaviour with crypto transactions.

AC: Given the multi-jurisdictional nature of crypto transactions, what difficulties are presented by obtaining the co-operation of international law enforcement / investigatory partners, and are there any jurisdictions that you have encountered that are particularly challenging to work with?

MF: Cryptocurrency investigations are rarely worked in a single jurisdiction – it's almost inevitable that you'll need to work with a foreign partner at some point. This isn't necessarily a downside. I have worked with many fabulous investigators around the globe who have tremendous cryptocurrency expertise and motivation to combat illicit finance. If anything, working with foreign partners and facilitating an exchange of best practices can be beneficial to an investigation.

The difficulties are the speed at which information can move across borders. Cryptocurrency can move instantly, but introducing things like Mutual Legal Assistance Treaty (MLAT) requests into investigation can greatly slow down the speed at which evidence in other jurisdictions can be acquired. This gets even more complicated when you layer in national security issues and classified information.

Enforcement

Once you have undertaken a thorough crypto investigation to trace stolen crypto or their traceable proceeds, the next step is to undertake enforcement action to recover some or all of the losses. Here our panel explore crypto enforcement.

AC: It seems like one of the difficulties when it comes to enforcement is that we are always playing catch-up with the novel methods used by the illicit actors to obfuscate their money laundering and the "good guys" have to react to these advancements. Helpfully, the courts have shown a willingness to adapt to this new financial environment, especially when it comes to recovering illicit crypto, and new legislation is imminent.

What more do you think could be done to aid in the recovery of property with ties to crypto theft/fraud?

TH: It has been a welcome development to see courts adopting an increasingly accommodating approach to tackling the novel challenges presented by crypto theft / fraud.

This perhaps starts with the recognition in some jurisdictions (with others likely to follow suit) that crypto constitutes "property". This enabled claimants to deploy well-established proprietary remedies such as proprietary injunctions, worldwide freezing orders, Norwich Pharmacal / Bankers Trust orders (to obtain disclosure from non-parties), Third Party Debt Orders and so on. Similar considerations arise in the context of the powers of office holders in insolvency situations.

We have also recently seen courts ordering "ethical hacks" as part of crypto asset tracing / recovery exercises.

It is difficult to say what more the courts could do at this stage – as new threats evolve, claimants will ask the court to grant ever more creative remedies, and the court will need to consider on a case-by-case basis how far it is prepared to bend the existing framework. So I think it will be a case of "watch this space" for now...

MF: The speed at which freezing / seizing orders can go out, especially if it involves more than one jurisdiction. Cryptocurrency moves at the click of the button, and nefarious actors are well aware that the longer cryptocurrency sits in a custodial wallet, the higher the likelihood that it's frozen. Time is truly of the essence in these scenarios

We have also recently seen courts ordering "ethical hacks" as part of crypto asset tracing / recovery exercises.

The state-sponsored proxy entity / network is unlikely to have many or any assets of its own in "friendly jurisdictions" against which enforcement could be undertaken.

AC: We have seen a rise in state-sponsored use of crypto theft, particularly from the likes of the Democratic People's Republic of North Korea.

What different investigative and enforcement challenges are presented by state-sponsored actors?

TH: Depending on the level of state involvement, including the amount of financing that is provided and the size and sophistication of the proxy entity / network, this can either make investigations and enforcement more or less tricky... but generally more tricky, I would say.

With an increase in the size of the entity / network, it can sometimes be easier to track their digital footprints, particularly if the nature of the theft / attack is a co-ordinated systematic attack on multiple targets as you have more data points to analyse. You may have a better shot at investigating the cause of the theft and its perpetrator in these circumstances than with a "lone wolf" acting through a multi-layered VPN masked network.

However, depending on the number of degrees of separation between the state and its sponsored proxy entity / network, while you might be able to identify the state-sponsored proxy entity / network, you may find there is little you can do to enforce against it.
The state-sponsored proxy entity / network is unlikely to have many or any assets of its own in "friendly jurisdictions" against which enforcement could be undertaken. Questions of state / sovereign immunity may also arise, although you rarely see countries claiming their state-sponsored entities – it somewhat defeats the point of creating a degree of separation in the first place.

In these circumstances, enforcement options may be limited to disparaging remarks in the international press, diplomatic condemnation and enhancing existing security measures to prevent further thefts. If you are the kind of state that sponsors cybercrime, these are unlikely to be effective deterrents.

MF: "More tricky" is an understatement. When it comes to state-sponsored actors like the Democratic People's Republic of North Korea, you're seeing significantly more complicated money laundering typologies, to include the number of wallets used the launder the funds, cryptocurrency mixers, and the use of OTC brokers. Think about it - when we're talking about state-sponsored cryptocurrency money laundering, we're talking about groups that have the resources, expertise and motivation to effect a complex flow of funds.

As a silver lining though, larger amounts can sometimes be easier to trace, and generally limits the avenues for "off-ramping". The larger the amount, the harder it is to find a cryptocurrency exchange or peer-to-peer trader that doesn't collect KYC and has the liquidity to convert large amounts of funds.

...continued

A number of challenges are presented by imposing consequences on illicit actors.

That is why we typically see North Korean actors using OTC brokers to move funds. For example, on April 24 2023, the Department of Justice unsealed two indictments charging a North Korean Foreign Trade Bank (FTB) representative, Sim Hyon Sop (Sim), for his role in two money laundering conspiracies designed to financially benefit North Korea, in violation of sanctions, by using cryptocurrency. The first indictment alleges that Sim and three OTC traders conspired to launder funds stolen in cryptocurrency exchange hacks and make payments in US dollars for goods through Hong Kong-based front companies on behalf of the North Korean government.

AC: If it is not possible to recover or seize crypto assets that have been stolen or swindled, what other tools are available to either compensate victims or impose consequences on illicit actors?

TH: This poses two difficult questions.

If asset tracing and recovery exercises have been unsuccessful, then victims may find they have limited options available to compensate themselves.

Unlike national governmental underwriting of deposits in respect of fiat currencies, and the general willingness of credit card providers to refund losses in the case of fraud or theft, crypto deposits and transactions do not (at least for now) benefit from analogous protections. That may change over time with a wider-spread adoption of crypto, and would be a logical step to consider to assist with easing crypto volatility.

A number of challenges are presented by imposing consequences on illicit actors.If you have been unable to successfully trace and recover assets, then it is likely that you may not have been able to identify the individual or entity behind the theft. Even if they can be identified, it may be difficult to bring them to justice, particularly if they are state-sponsored entities, or in a country that does not have analogous law enforcement and extradition protocols.

MF: This ties back to the unique challenges presented by non-custodial wallets, in the sense that they have never gone through a KYC collecting body and that the end user, not the centralised cryptocurrency exchange, controls the wallet's keys.

In these circumstances, the private keys for the wallet will need to be acquired through alternative means, which usually requires law enforcement authorities. This could happen by finding the key(s) through an authorised search of the subject's electronic devices or residence, or by the subject providing them to the government voluntarily in a custodial or non-custodial interview. For example, in the Bitfinex hack case, the USG executed search warrants on online accounts controlled by the subjects and obtained access to files that contained the private keys required to access the cryptocurrency wallet that directly received the stolen funds from Bitfinex.

If the private keys for the wallet are not found in unstructured data repositories, sanctioning the wallet is another possibility. This is also a capability restricted to government entities, but it essentially puts out a public notice that the wallet is associated with illicit activity.

Crystal ball gazing

The headlines were dominated in 2022 and 2023 by high-profile crypto exchange and lending platform collapses. The crypto space requires some good news to shore up confidence in the asset before it can see even wider-spread adoption. Part of the challenge involves ensuring that the right legal and regulatory balance is struck to ensure sufficient regulation to protect investors but not too much to stifle advancements. Here our panel explore future trends in the crypto space.

AC: While 2022-2023 were dominated with headlines of high-profile cryptocurrency exchange and lending platform collapses, 2024 seems to be the year of momentum for cryptocurrency legislation and countries courting Virtual Asset Service Providers to register in their jurisdiction.

Do you think this positive momentum is here to stay?

TH: Crypto collapses, fraud and price volatility are likely to continue to crop up periodically in headlines: there's no news like bad news, after all.

The path to the implementation of a robust but accommodating legal and regulatory framework for crypto and virtual assets is less headline-worthy, but no less newsworthy.

When I say "robust but accommodating", that is because it seems to me that a fine balance needs to be struck. On the one hand, it is important to deter theft and fraud and ensure appropriate oversight of crypto and virtual assets (notably from the point of view of AML compliance and exchanges having adequate capital sufficiency).

On the other, it is important to encourage adoption and use of crypto and virtual assets (which could be dissuaded by over-regulation), and building sufficient flexibility into the framework to allow it to evolve (potentially at pace) as crypto and virtual assets themselves, and the challenges associated with them, do as well.

MF: Tom highlights the important balance of innovation and risk mitigation. It's a give-and-take battle but they don't need to be mutually exclusive. Several jurisdictions – like the EU, UK, Dubai, South Korea, and to an extent, the US – are trying to strike this balance in their proposed or already enacted regulatory frameworks. These developing regulatory frameworks have the benefit of hindsight – the ability to incorporate lessons learned from the high-profile cryptocurrency collapses of the past few years.

75% of jurisdictions surveyed were only partially compliant or not compliant with FATF's recommendation 15.

AC: Cryptocurrency is a "currency without borders", which presents endless paths for financial innovation but also some enormous challenges when it comes to making rules of the road and the different approaches being taken globally. Adoption of the Financial Action Task Force's Travel Rule is an obvious example of that – some jurisdictions have adopted it, others haven't, and those that have often do so with differing limits.

How do you think a more globally unified approach could be taken?

TH: A more unified global approach would certainly assist, but the difficulty with doing so lies in the inherent nature of crypto – it is a decentralised virtual asset. Whereas some countries are embracing crypto with increasing willingness, and looking at how their legal and regulatory frameworks need to be updated accordingly, it is less of a priority to others. In that sense, it is perhaps little different from other cross-border / international initiatives: what is attractive to one country, may not be to all; and in the same way, what works for one country, may not work for all. Further guidance from supranational entities such as FATF may assist, but that remains dependent for effect on its implementation at national level. In this regard, it is important to note that as at April 2024, FATF reported that 75% of jurisdictions surveyed were only partially compliant or not compliant with FATF's recommendation 15. Before we can consider a more unified global approach, individual adoption rates need to significantly improve.

From my perspective, more needs to be done to bolster the effectiveness of sanctions enforcement with regard to crypto. While progress has been made, such as the US$4.4 billion settlement between the US Department of Treasury and Binance for violations of US AML and sanctions laws, more should be done. To an extent, this could be mitigated by advancements in tracing capabilities.

Similarly, sanctions laws could be bolstered to more specifically target illicit actors using crypto, followed by more proactive and robust breach and circumvention prosecutions.

MF: Piggybacking off the decentralised nature of crypto assets, the wide range of data privacy laws across jurisdictions, as well as the differing transaction thresholds, further complicate the implementation of the Travel Rule.

However, it comes back to the spirit of the law. Absent clear guidance on how to implement more complex components of the FATF's requirements or what to do when interacting with a non-FATF-compliant VASPs, organisations focus on the overarching goal of the FATF standards — preventing criminal and terrorist misuse of the sector — when designing their AML / CFT measures. Returning to the "why" of the FATF's requirements enables organisations to adopt an appropriate risk-based and fit-for-purpose approach toward preventing illicit transactions on their platforms.

AC: It seems to me that there are some jurisdictions that are more of a crypto "hotbed" than others, with the British Virgin Islands (BVI), in particular, being the present epicentre of enforcement / recovery actions.

Is there a risk that you end up with global pockets of crypto investigatory and recovery expertise, both in the law enforcement and civil spheres, and if so what knowledge sharing or other initiatives do you think could be introduced to level the playing field?

TH: It is certainly fair to say that the BVI is leading the charge in crypto enforcement and recovery actions, and my colleagues in the BVI are currently acting for the liquidators of Three Arrows Capital and the provisional liquidators of FTX. England has also seen a slew of recent crypto litigation. It is inevitably the case that these regional concentrations of investigations, enforcement and recovery actions may lead to disparities in knowledge and awareness of crypto criminal typologies and how to combat them (or mitigate their effects).

On the law enforcement / investigatory side, I think that national cyber security and financial intelligence units should continue to foster close working relationships with one another.

Quite aside from the fact that crypto theft will often have a multi-jurisdictional dimension that requires investigatory collaboration, knowledge-sharing both among themselves and with the public should help to enhance awareness and effectiveness of measures to combat / mitigate adverse effects arising from crypto.

On the civil side, knowledge sharing is again key. That could be by attending or speaking at conferences, or collaborating with practitioners in the space, as we are doing with our discussion today.

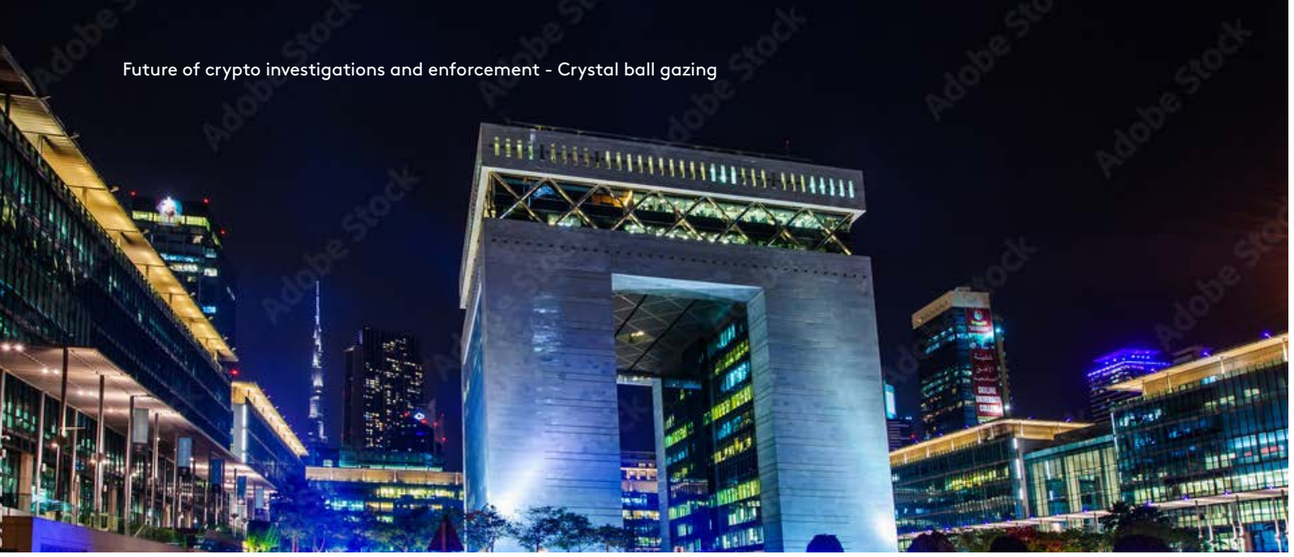
MF: I'm biased from my experience in the FBI, but US Law Enforcement, in conjunction with our international partners, has pioneered the cryptocurrency enforcement space. This is evident from the numerous high profile cryptocurrency seizures conducted by the US Department of Justice, including:

June 2021 seizure of
US$2.3 million
in cryptocurrency paid to the DarkSide ransomware variant

November 2023 seizure of
US$3.36 billion
in cryptocurrency in connection with the Silk Road case

February 2022 seizure of
US$3.6 billion
in cryptocurrency linked to the Bitfinex hack

I 100% agree that the national cyber security and financial intelligence units should continue to foster close working relationships with one another. This is a team sport – it's exceptionally rare that cryptocurrency cases only involve one jurisdiction, and the higher the baseline knowledge level, the better.



AC: Leading on from that, unfortunately more regulation doesn't always mean more effective regulation. Meredith, you have written previously about the United Arab Emirates introducing a dedicated Virtual Assets Regulatory Authority (VARA).

Do you think that this could be the blueprint for other jurisdictions, or a bit of a "white elephant" project that lacks the teeth to be effective?

MF: Time is going to tell. It's very new piece of regulation. Part of VARA's mission is to position Dubai as a global leader and international hub in the VA space.

Success at this will depend on VARA's willingness to take swift action against VASPs that do not comply with its rules and regulations.

In November 2023, VARA announced that it had issued fines to licensed VASPs for failing to comply with VARA's directives. If VARA can continue to hold VASPs accountable to its rulebooks and keep up with the pace of innovation in the crypto industry, it may be able to accomplish its mission.

Key contacts

Tom Hall
Managing Associate
Jersey

+44 1534 514443
tom.hall@ogier.com

Andy Carpenter
Senior Consultant
Jersey

+44 1534 514492
andy.carpenter@ogier.com

Meredith M. Fitzpatrick
Director of Cryptocurrency, Investigations and Compliance
www.forensicrisk.com

Direct: +1 (202) 836-1425
Mobile: +1 (202) 836-1425

About us

Forensic Risk Alliance
Forensic Risk Alliance (FRA) offers global companies and their counsel forensic accounting and technology expertise for complex investigations, disputes, compliance monitorships and risk advisory.

Unlike larger network firms, we operate uniquely in the forensic space and have no audit-related conflicts. For 25 years, clients have valued our advisors' independent mindset and credibility with authorities, courts and stakeholders.

Corporations and law firms regularly engage experts from across our global locations to resolve complex matters and mitigate risks involving fraud, bribery and corruption, money laundering, sanctions, accounting malpractice, cryptocurrency and ESG.

Supporting clients around the world with our one-firm global structure, we assemble the right team to ensure each engagement leverages the best of FRA's expertise. Whether for investigations or compliance needs, FRA's investigative mindset, risk-based approach, and integrated custom technology expertise promise efficient resolution of high stakes matters.

Ogier
Ogier is an international and offshore professional services firm with the knowledge and expertise to handle the most demanding and complex transactions and provide expert, efficient and cost-effective services to all our clients. Our commercial understanding and experience of working with leading financial institutions, professional advisers and regulatory bodies enable us to add real value to our clients' businesses. The continued global growth in the use and value of cryptoassets has seen an accompanying rise in crypto disputes. From fraud and asset tracing, restructuring, shareholder and fund disputes to regulatory and private client concerns, many areas of litigation have a nexus with cryptoassets.

Our team successfully combines market-leading legal expertise with the necessary technical knowledge of cryptoassets, including NFTs and cryptocurrencies, to effectively support our clients in this area.

With a strong track record of supporting clients across a range of disputes, our Dispute Resolution specialists work closely with other Ogier teams with a specialism in crypto to provide an end-to-end service.

Ogier Regulatory Consulting
Ogier Regulatory Consulting supports clients to navigate the complex and ever-changing regulatory landscape, while effectively mitigating regulatory risk.

Our team of trusted consultants have experience as regulators, advisors, policy makers, investigators, compliance/risk practitioners, and trainers. We bring together our expertise in regulatory requirements and expectations, practical implementation, commercial understanding and lean thinking, to provide tailored and effective solutions for your business.

If you're in, or expanding into, virtual assets, Ogier Regulatory Consulting can remove the complexity and allow you to concentrate on building a successful practice with our services including advice on:

Virtual asset forensics
Blockchain analytics
AML controls and risk assessments
Investigations