



Blockchain analytics and their role in keeping the regulator happy

Insights - 05/06/2023

Before Satoshi Nakamoto 'coined' the term 'Bitcoin' back in 2007, financial crime analysts spent the majority of their time analysing transactions between traditional bank accounts across the globe.

This analysis mainly involved the use of IBAN (International Bank Account Number) numbers; a number the format of which would help identify the country and financial institution that provided the account. This therefore meant financial investigators knew which bank to contact if they were able to identify that illicit funds had been transferred to a specific IBAN.

With virtual currency it is possible to analyse the record of virtual asset transactions stored on a transparent blockchain, but in the blockchain ledgers raw format this will only result in the identification of an unattributable wallet address that the illicit virtual assets have ended up in. What you won't see are any details of who the wallet is owned by or which geographical area it is being controlled from.

The transactions to or from a wallet can be viewed by entering the wallet address into blockchain sites such as Blockchain.com which is useful, but again there are no details available to identify who has control of that wallet. That is where blockchain analytics (BA) come in.

The first major producer of BA tools was Chainalysis in 2014, which created its analytics tool to trace virtual assets stolen during the Mt. Gox crypto exchange hack. Since that time BA tools have evolved considerably with there now being a number of companies entering the BA market.

What does a BA tool do and what purpose does it serve?

In a nutshell, a BA tool 'tags' wallet addresses with intelligence reports to help identify who may be in control of that wallet, and whether there is intelligence to suggest either the wallet or assets within have come from an exchange hack, ransomware attack, are connected with a sanctioned entity or jurisdiction, or similar tags that taint the wallet and increase the risk should a potential

transaction involve it. It will also indicate if the illicit funds have been forwarded to a virtual assets exchange that could convert the virtual assets to traditional currency, and it is that virtual assets exchange that should hold sufficient due diligence information to help identify an individual connected to the illicit funds.

This therefore makes BA an essential part of AML controls for any entity considering dealing with virtual assets, be it that they plan to apply for a virtual assets service providers licence, are performing source of wealth or source of funds enquiries as part of their due diligence process, or are considering accepting payment in virtual assets. These are all key considerations that need to form part of a business risk assessment.

In summary we can see how BA tools can reduce the ML risk when dealing with virtual assets. An organisation's use of BA along with tools to detect clients who try to hide their location through IP anonymisation are seen as being pro-active in their approach to AML.

The Government of Jersey recently published an update to the Terrorist Financing National Risk Assessment and there is reference to its VASP (**virtual asset service provider**) Risk Overview, published in May 2022, which states that:

"As part of their risk management framework, some authorised service providers in Jersey have introduced the use of **blockchain analytics** tools when conducting monitoring. These entities have also been proactive in implementing measures to address their AML/CFT risk exposure stemming from their use of, or involvement with, VAs. This can be seen as a positive approach by firms to mitigate their risk exposure."

As with the implementation of any new software, a thorough risk assessment will be required. As a practitioner of BA I should point out that BA tools are not cheap and there is a skill set required for an individual to be able to carry out BA work. However, having the tools and the skills within an organisation will become essential as virtual asset and blockchain adoption becomes more mainstream.

The Ogier Regulatory Consulting team are on hand to offer detailed support to clients on BA and VASP compliance requirements including corporate governance matters, policies and procedures and tailored training for beginners to those who are more experienced.

Please contact Andy Carpenter, Amanda Reilly or Tui Iti for further information or advice.

About Ogier

Ogier is a 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. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

This client briefing has been prepared for clients and professional associates of Ogier. The information and expressions of opinion which it contains are not intended to be a comprehensive study or to provide legal advice and should not be treated as a substitute for specific advice concerning individual situations.

Regulatory information can be found under [Legal Notice](#)

Key Contacts



[Andy Carpenter](#)

Senior Consultant - eDiscovery and Digital Forensics

[Jersey](#)

E: andy.carpenter@ogier.com

T: [+44 1534 514492](tel:+441534514492)



[Owen Woolgar](#)

Global Head of Regulatory Consulting

[Jersey](#)

E: owen.woolgar@ogier.com

T: [+44 1534 841430](tel:+441534841430)

Related Services

[Ogier Regulatory Consulting](#)

Related Sectors

Technology and Web3