[IMTF]

DR. SEBASTIAN HETZLER

Off to New Financial Crime Worlds:

The Crypto Challenge

With the growing popularity of cryptocurrencies as a means of money transfers and investments, the risk exposure for traditional banks to become passively involved in crypto-based fraud and money-laundering increases. Yet only few financial institutions have taken precautions against risks from cryptocurrencies – the majority is not even aware of the emerging threat.

Here is what you need to know to protect your financial institution.

Cryptocurrencies are coming of age

Since its appearance 15 years ago, Bitcoin has developed from a geek toy used for online gaming to a respected digital currency. While debates about the future role and significance of this new asset class are still ongoing, precedents are set by private, and public actors.

Current studies estimate that in the United States more than 15% of all consumers hold or use cryptocurrencies. In some countries in Asia, Africa, and Latin America this fraction is at 40% as digital currencies are seen as one of the cheapest ways to transfer money and to decouple from high inflation rates of the countries' fiat currencies. The global share is estimated to be at 6.8% in 2024.

Another proof of cryptos' increasing importance is the fast-growing crypto ecosystem: In 2022 the number of blockchain wallets was estimated to be 84 million with a rapid growth of +20% per year. Even more astonishing, the number of private and publicly available crypto currencies is estimated to be over 9,000, with more than 70% of the market capitalization represented by Bitcoin, followed by Ethereum and Tether. Nowadays, more than 500 Virtual Asset Service Providers (VASP) act as gateways between the fiat and crypto currency world.

Given how dynamically the crypto ecosystem has evolved over the last years, many traditional financial institutions (FI) have meanwhile overcome their early skepticism and are eager to save their share in this emerging financial market. JP Morgan, Barclays and Paypal – just to name a few – have introduced products and services in cryptocurrencies.

Finally, governments around the globe have spotted digital currencies as a potential future alternative to fiat currencies and are paving their ways into the realm of virtual assets. In 2020, the Bahamas debuted with the first Central Bank issued Digital Currency (CBDC). China followed suit with the introduction of the e-Yuan (e-CNY). Other countries are in the wings to issue digital correspondents to their respective currencies. A digital Euro is tentatively planned by the European Union for 2028.

Are cryptocurrencies built for fraud and money laundering?

Despite the rise of crypto and its growing significance for the global financial system, many people still believe that cryptocurrencies are mainly used for criminal activities. This perception is heavily influenced by the many scams and scandals reported by the media especially in the early days of crypto. Actually, only 0.34% of the total on-blockchain transaction volume was sent to wallets which have been identified as being illicit, says Chainalysis, a global vendor for blockchain analytics, in its 2024 Crypto Crime Report. Obviously, blockchain technology isn't that popular in bad circles as many believe. To better understand this misconception we have to look into two important "features" of crypto: its anonymity and transparency.

Let's go with anonymity first. To partake in the world of cryptocurrencies, actors only need a wallet that is used to receive, hold, and send cryptocurrencies. This wallet is a unique number, comparable to an account number. People or organizations can hide behind these wallet numbers without depositing any personal data and transact in cryptocurrencies in full anonymity, so a widely held belief. Even Bitcoin's mysterious inventor, Satoshi Nakamoto, emphasized that cryptocurrencies are totally anonymous. But this is only partly correct.

Firstly, the unique wallet number does not provide full anonymity. It's rather a pseudonym under which actors do transactions on a blockchain. Since relations between transactions and the pseudonym (i.e. the wallet number) are preserved on the blockchain, we can't speak about full anonymity.

Secondly, by doing this, the pseudonym leaves some kind of digital trail on the blockchain. At least for the publicly available cryptos, all transactions are logged on distributed blockchains. All transactions ever happened are always accessible to everyone. This transparency of blockchains is the main difference to fiat currencies. A coin or note in one's hand does not "carry" and reveal its whole transaction history. It's exactly this transparency that has significant impacts on illicit activities like money laundering: all illicit transactions and involved wallets are logged and can be traced on the distributed blockchains, while in fiat currency individual FIs often only see one or two layers of a large fraudulent or money-laundering scheme which goes across different countries, banks, and accounts. With blockchain analytics, investigators in compliance departments or Financial Investigation Units (FIU) are able to cluster wallets that belong to the same actor even across different blockchains, to investigate the flows of crypto through the different sending and receiving wallets, and to classify wallets and transactions according to their risk and nature.

Lastly, at some point, criminals may have to draw back on fiat currency to obtain cryptos to fund their illegal on-blockchain activities, or they have to convert cryptocurrencies to fiat currency to buy - for example - certain luxury goods that they only can pay in fiat currency. At this exchange between fiat and digital world, the link between the pseudonym in the crypto world and the real world identity may unfold.

The gatekeepers between the two worlds

According to the Financial Action Task Force (FATF), the global financial crime watch dog, Virtual Asset Service Providers (VASP) are natural or legal persons that facilitate exchanges between fiat currencies and virtual assets, and/or between different forms of virtual assets, and/or transfer and administer virtual assets by using blockchain technology.

The majority of VASP are exchanges that serve as gatekeepers to the crypto-world and back. They are converting fiat currencies like USD or EUR into crypto-currencies like Bitcoin (BTC) or others, and deposit them in a wallet.

Other VASP are Automatic Teller Machines (ATM) run with cryptocurrencies, and wallet custodians that mainly transfer or hold cryptocurrencies in wallets.

Coming back to the role of exchanges as gatekeepers: As entry and exit point to the crypto world, they decide which degree of anonymity, or better pseudonymity, they would like to grant to their customers, and the level of diligence they apply to the identification of their customers and the surveillance of their activities on the blockchains. From this perspective, they play a key role in securing the crypto sphere. But not all exchanges share the opinion of regulators on how to play this role.

The regulatory view on cryptocurrencies

While only few countries like China or Saudi Arabia banned cryptocurrencies completely, the majority of countries accepts digital assets as financial instruments, although many of them are still lacking a general regulatory framework.

However, in most jurisdictions, regulators tried to pick up with the emerging risk of the crypto ecosystems and imposed AML/CTF including travel rule regulations according to the FATF recommendations more quickly. By and large, most jurisdictions have extended the strict regulations from "traditional" financial institutions in the world of fiat currencies to the players in the crypto space.

For instance, with the 5th AMLD, the European Union has extended existing AML regulations also to virtual assets. VASP in EU-countries have to be registered and are subject to existing KYC and AML regulations in the respective country.

But these local regulations are difficult to enforce in a global, digital network. That's why the regulators look for support from the traditional banking sector. In its 2020 guidance, the US regulator Financial Crime Enforment Network (FinCEN) has extended the duties of banks to monitor, identify, and report suspicious activities connected to crypto, regardless whether a bank actively offers crypto services or not.[1]

At this point at the latest, every FI should have started to think about its crypto risk-exposure.

[1] bit.ly/FinCEN-2020-guidance June 17th 2024

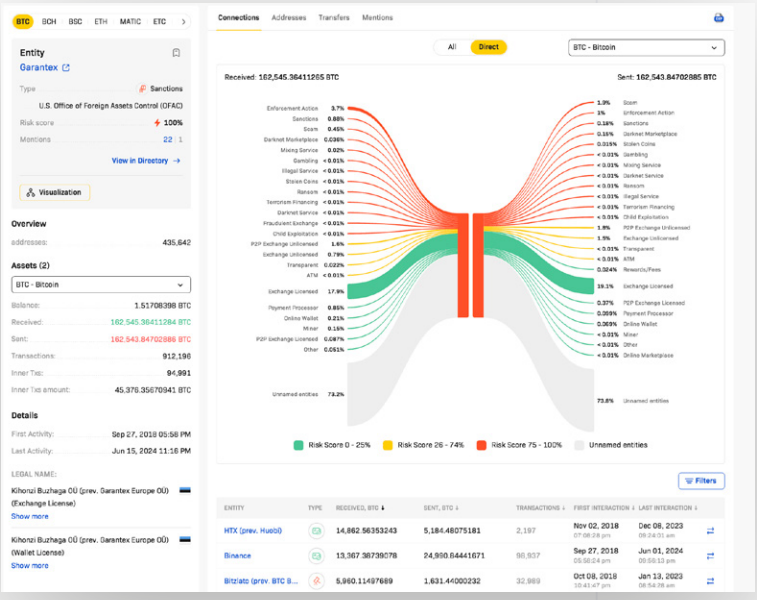
The hidden risk-exposure

In general, we can distinguish three levels of crypto engagement of a FI, each associated with a specific risk exposure.

It may sound counter-intuitive but the level with the highest crypto risk is the one without any crypto engagement of a FI. The reason for this is, that the majority believes exactly because they don't offer any crypto-related service, they are not exposed to any crypto-related risk. For many this sound reasonable. But turning a blind eye towards crypto risks is in fact a dangerous strategy. It is true that those FIs are not exposed directly to crypto risks, but passively through their customers. Unless there are good reasons not to assume differently, FIs should start with the assumption that the overall share of consumers in a country engaging in cryptocurrencies also represents the share of their customer base holding or trading crypto. So, in western countries, 15% of an FI's customers potentially expose a crypto risk.

The risk for a traditional bank becoming part of crypto-based scams or money-laundering activities becomes obvious once we are looking at a typical path from fiat to virtual currency and back: A fraudster would send fiat currency from his bank account to a VASP, convert it into a cryptocurrency and store it in a crypto-wallet. At this point, the FI losses any visibility and control over the funds. Once the fraudster has crypto-currency "in his hands", he would conduct illegal activities and then try to obfuscate the origins of the funds. He would do this by converting them into other cryptocurrencies or private coins, sending it through numerous illicit wallets or by using so called Mixers and Tumblers, crypto-services that are explicitly built to launder money. Finally, the laundered cryptos would go back to a bank account through a VASP that turns crypto into fiat currency. Unnoticed by his bank.

The second level sets in if a FI decides for strategic reasons to take on VASP as commercial clients. Again, the FI has no visibility in the VASP's clients' crypto transactions, but the FI has control over the level of diligence applied to and by the VASP to ensure that it is not involved in illicit activities.



Blockchain analytics tools like Bitfury's Crystal provide a very detailed picture of sources and sinks of crypto and associated risk. The picture shows Bitcoins flowing through a meanwhile sanctioned wallet

At the third level, FIs extend their service portfolios to include crypto-related services. As already pointed out, many traditional banks have embarked on this trend already, offering crypto services like holding and trading digital assets to their clients. Here the crypto risk is lowest since the FI has almost full visibility and control of a customer's transactions. Modern technologies like blockchain analytics tools help to analyze and visualize the flow of cryptos, their sources and sinks, and the risk associated with them. FIs would notice once its customer would start to interact with bad wallets.

Recommendations to protect against crypto risks

Financial institutions have to take action to effectively protect against crypto risks on several levels.

[A] UPDATE AML RISK FRAMEWORK

Effective protection starts with risk awareness and risk assessment about the direct and indirect risks from cryptocurrencies. FIs must assess which channels, customer group and products are prone to crypto risk and how to mitigate them. At this stage they have to decide on the risk appetite regarding cryptocurrencies. Whether to follow a strict "no crypto" approach and blocking all transactions to crypto exchanges, or a limitation of transaction amounts or types of VASP their customers are allowed to transact with, are important questions that must be answered at the onset.

[B] KNOW YOUR CUSTOMER PROCESSES

FIs should extend their customer onboarding processes to cover the identified crypto risks and ask their potential clients whether and how they engage in virtual assets. Also, the intentions of the crypto engagement should be clarified as part of the extended KYC-processes.

[C] RISK SCORING

Customer risk models should be enhanced to cover identified crypto risks and factors. FIs have to decide if and to which extend they deem customers' crypto transactions as acceptable from a risk perspective and under which conditions and limitations. The risk score and classification should represent the actual behavior of a client with regards to crypto transactions and the risk these expose to the FI. Enhanced due diligence should be applied to medium risk customers and high-risk customers. Depending on a FI's crypto policy, customer relationships should be suspended if the risk exposure is not acceptable.

[D] ONGOING CRYPTO MONITORING

The ongoing monitoring of customer transactions from and to VASP is at the core of an effective Crypto-AML program. FIs should enhance their transaction monitoring systems in order to identify customers that are engaging in cryptocurrencies and to assess the risk that is associated with this.

Commercial vendors like Mastercard provide lists containing bank accounts and Bank Identification Codes (BIC) used by major crypto exchanges. With this data asset FIs can now identify the transactions going or coming from a crypto exchange. Even more, risk-classifications of the known crypto exchanges are available. Exchanges that follow strict KYC and AML regulations are considered low risk, while high-risk VASP neither ask for identification of the clients in the onboarding process nor monitor customer transactions on the blockchains.

[E] BLOCKCHAIN MONITORING

If a bank actively engages in crypto services like custody services, they need to have stricter safeguards in place in to order to protect this business. Dedicated blockchain AML system that analyze and visualize transactions on various blockchains can help to get better transparency on a customer's behavior and a proper risk-assessment.

Embracing cryptocurrencies

Independent of the discussion which role digital assets will play in the future, they should be accepted as an integral part of the modern global financial system. Rather than turning a blind eye to the blockchain technology, FIs should take proper actions to protect their business against financial crime risks.

Crypto offers many new opportunities to building new or changing existing financial businesses. Traditional FIs with a long-standing experience in compliance and IT-security are very well equipped to extend their portfolios into the new world and to exploit opportunities that go along with digital assets.

“To be clear, exchanges are not the only ones with crypto risk exposure. These risks are not unique to money services businesses or virtual currency exchangers; banks must be thinking about their crypto exposure as well. These are areas your examiners, and FinCEN, will ask you about when assessing the effectiveness of your AML program.”

[KENNETH BLANCO, DIRECTOR FINCEN]

[ABOUT THE AUTHOR]

Dr. Sebastian Hetzler joined IMTF as a Co-CEO in December 2022 with the acquisition of the Siron business from FICO. At FICO, he has been a VP Product Management for FICO’s Compliance Solutions. Before the acquisition of TONBELLER AG in 2015 Sebastian has been the managing director of this company. With more than 15 years’ experience in the Anti-Financial Crime sector, he is one of the leading domain experts in this space. Previously, Sebastian worked in top-management consulting companies focused on strategy and organization for many years. Sebastian holds a doctorate in System Theory and Cybernetics from the University of St. Gallen, Switzerland.

IMTF group (HQ)
Route du Bleuet 1
1762 Givisiez / Switzerland
Phone +41 26 460 66 66

IMTF Siron GmbH
Stubenwald-Allee 19
64625 Bensheim / Germany
Phone +49 6251 826 27 90

IMTF Dubai
Reef Tower, Unit R30-20 / 30-21
Jumeirah Lake Towers
Dubai 5003308 / UAE
Phone +971 4 448 7570

IMTF Luxembourg
12, rue du Château d'eau
3364 Leudelange / Luxembourg

IMTF Banking Software Pte. Ltd.
Level 6 Republic Plaza
19 Raffles Place
Singapore 048619
Phone +65 6735 61 50

Informatique MTF Services GmbH
Mariahilfer Strasse 123/3
1060 Vienna /Austria

IMTF Software Pte. Ltd.
No. 6, Ground Floor, IndiQube Plaza
Wind Tunnel Road, Kaveri Nagar,
Murgesh Pallya,
Bengaluru - 560017
Karnataka / India

info@imtf.com
www.imtf.com

[OUR MISSION]

Helping fight financial crime and make the world a safer place.