

Cryptoasset Regulation in Germany

How to implement the requirements with Scorechain

December 2021



Table of content

Introduction	2
German crypto regulations and the solution from Scorechain	4
Overview	4
German Banking Act	5
German Money Laundering Act and Interpretation and Application Guidance	6
Money Laundering Act and Risk Management	6
Obligated Entities and Risk Assessment	6
Obligated Entities and Due Diligence	7
FATF Guidance	8
Legislative plans of the EU Commission	9
Concretization of the approach through Scorechain	10
Adhering to German regulatory requirements with the Scorechain S.A. solution	11
Risk Ratings	12
Monitoring and Reporting	13
Exploration Tool	16
Conclusion and Outlook	19
Conclusion	19
Outlook on Kryptowertetransferverordnung and Travel Rule	19
About	20
About Scorechain	20
About PwC	20
List of abbreviations	21

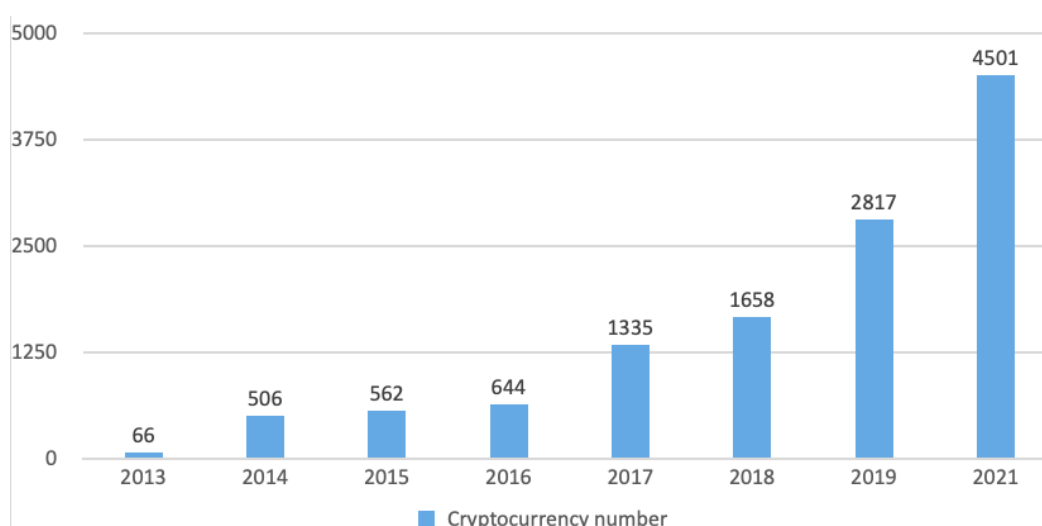
Introduction

Digital currencies and distributed ledger technology created a whole new innovative framework to the financial services industry and reshuffled the way people invest, transact, and understand financial technology.

On the other hand, this technology brought many risks associated with money laundering (ML), terrorism financing (TF) as well as fraud and other criminal offenses.

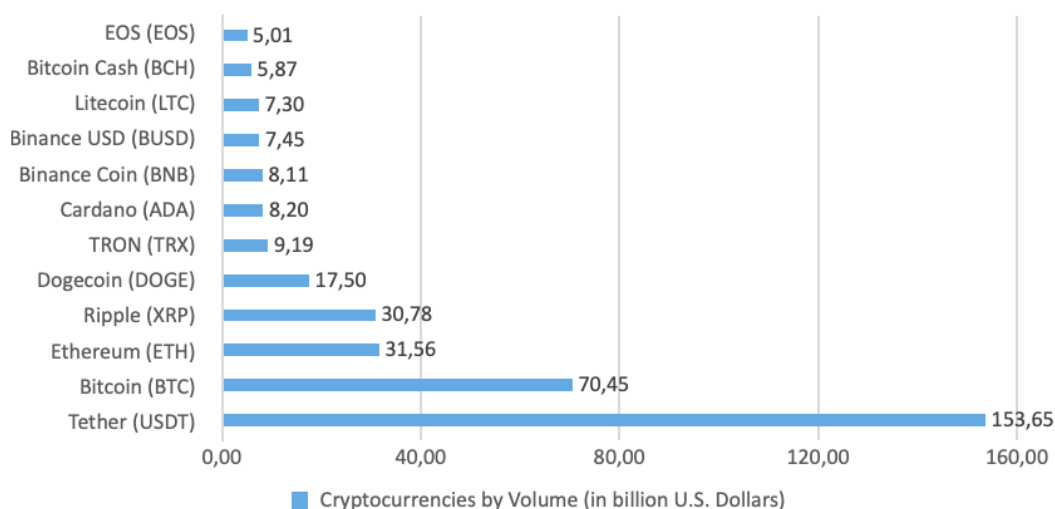
There is little agreement in the literature as to whether cryptocurrencies are a type of independent currency or rather virtual assets. It is still disputed whether cryptocurrencies are comparable to money in the economic sense of a currency or whether they serve as an object of speculation. Despite all the discussions, the term cryptocurrency has now become generally established in the German regulatory framework's usage. Since the price development of the existing cryptocurrencies is linked to the classic fiat money, there is a notable interface to the original financial system. Meanwhile, several thousand different cryptocurrencies are traded on the market and almost all of them show high volatility in terms of prices and/or their inherent characteristics. Since the outbreak of the COVID-19 pandemic in the spring of 2020, investments in crypto assets have been on the rise. However, already prior to this more, and more countries worldwide are setting up the legal basis for crypto transactions leading to headlines in the news and a continuously growing number of market participants. Furthermore, in addition to the significant growth of market participants, the following graphs illustrate the substantial increase of cryptocurrencies in the world as well as their significant volume.

Number of cryptocurrencies worldwide from 2013 to 2021



Bar Chart 1: Source: CoinMarketCap, Published by GP Bullhound; The Motley Fool; Investing.com, Source link: [coinmarketcap.com](https://www.coinmarketcap.com), February 2021, quoted from [de.statista.com](https://www.statista.com/statistics/863917/number-crypto-coins-tokens/), 2021 (<https://www.statista.com/statistics/863917/number-crypto-coins-tokens/>)

Biggest cryptocurrencies in the world based on 24h volume on April 14, 2021 (in billion U.S. dollars)



Bar Chart 2: Source: CoinMarketCap, Published by: CoinMarketCap, Source link: coinmarketcap.com, June 2021, quoted from [de.statista.com](https://www.statista.com/statistics/655511/leading-virtual-currencies-globally-by-purchase-volume/), 2021 (<https://www.statista.com/statistics/655511/leading-virtual-currencies-globally-by-purchase-volume/>)

As a result of the growing crypto market, governments and intergovernmental bodies such as the Financial Action Task Force (FATF) already started to respond to all these challenges. The Federal Ministry of Finance of Germany dedicated a separate chapter to the topic of cryptocurrencies in the first edition of the National Risk Analysis (2018). It stated there that the risk of money laundering activities has increased, but that "no large-scale money laundering activities are yet discernible". Furthermore, the German Financial Intelligence Unit (FIU) published an overview of crypto reporting in its 2019 annual report. The FIU is observing an increasing number of money laundering suspicious activity reports.

The new technology blockchain and cryptocurrency makes new infrastructures and systems necessary. New requirements are emerging and must be implemented. This includes, for example, new "watch lists" about known conspicuous addresses (darknet, black market). The rapid further development of products (e.g., new currencies) requires timely adjustments to preventive measures to adequately cover risks.

Scorechain S.A. and PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft (PwC) as a strategic cooperation bring together the technical and subject matter expertise to tackle the challenges in the area of cryptocurrencies and regulatory requirements. Scorechain S.A. provides a solution for monitoring suspicious behavior by applying sophisticated methodologies and a database that enables precise activity tracking. PwC brings long-lasting and in-depth expertise in the area of Anti Financial Crime and holistic consulting services.

German crypto regulations and the solution from Scorechain

Overview

The Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht - BaFin) is Germany's authority responsible for the supervision of the financial sector. BaFin is among others responsible for monitoring of credit and financial institutes, insurance companies and the trading of securities, and is therefore the principal authority for supervising and ensuring the proper functioning, stability, and integrity of the German financial system. As a result of its prudential approach, BaFin was one of the first authorities in the European Union that amended its legislation in order to include the requirements of the Fourth and Fifth EU Anti Money Laundering Directive and since January 2020, BaFin requires from obliged institutes that provide crypto custody business to apply for authorization by gaining an official license.

The legal framework for the supervision of credit institutes and financial services institutes in Germany is the German Banking Act (KWG). In addition to the KWG, the German Money Laundering Act (GwG) is of particular relevance to the financial supervisory authority since, among others, financial institutes pursuant to Section 1 (1) of the KWG and financial services institutes pursuant to Section 1 (1a) of the KWG are obliged parties under the GwG. This means that they must take appropriate measures to prevent money laundering and terrorist financing through their institution in order to maintain the soundness, integrity and stability and trust in the financial system.

In addition to the supervision of institutes, BaFin also publishes information on current topics and advice on the interpretation of legal requirements. This is done, for example, in circulars, the annual report or the BaFin journal. One of the most important pieces of information regarding compliance with the provisions of the Money Laundering Act is BaFin's Interpretation and Application Guidance in relation to the German Money Laundering Act (Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, abbreviated AuA). In June 2021, BaFin also published the Interpretation and Application Guidances special part for credit institutes according to Section 2 (1) Nr. 1 GwG. The Interpretation and Application Guidance is intended to assist obligated institutes subject to BaFin supervision in adequately and fully implementing the requirements of the Money Laundering Act.

The following section highlights the legal regulations in more detail. At the same time, it will be described how Scorechain's solution fits and fulfils the legal requirements from a technical perspective.

Scorechain, the Luxembourgish company, has been established in 2015 with a worldwide presence. The company provides cryptocurrency monitoring for the purpose of Anti-Money Laundering (AML) and acts as a trusted provider for crypto markets with a transaction tracking system and scoring formula that helps compliance teams to assess the associated risks better and more efficiently. This is possible by providing general blockchain information on transactions, addresses, blocks, the de-anonymization and categorization of crypto addresses, data related to tokens and transaction moves, real-time assessment on the risk scoring of incoming and outgoing transactions, addresses, entities as well as information on possible risk red flags that are configured as part of the compliance policy of each user.

In terms of risk scoring, the goal is to rate crypto activities depending on the origin and destination of funds. All addresses, entities and transactions have two types of scoring

(incoming and outgoing scoring) between one, which represents extremely risky activities, and 100 that represents extremely low risk. In terms of red flag risk indicators, the goal is to display useful information on suspicious activities for entities, addresses and transactions. There are three categories of risk indicators that users can configure based on their needs. The entity risk associated with the type of entity. The behavioral risk associated with these transaction behaviors that could pose a risk. Lastly, the country risk is the last category of risk indicators and shows the risk associated with the jurisdiction of a registered exchange. All the above functionalities go along with features such as the Entity Directory, the Case Manager for managing suspicious cases and options for generating reports on addresses and transactions.

German Banking Act

Since the implementation of the requirements from the Fifth Money Laundering Directive (directive 2018/843) into national law, terms such as crypto custody and crypto assets have been mentioned in German law for the first time.

Pursuant to Section 1 (1a) sentence 2 No. 6 of the KWG, crypto custody business, i.e., the custody, management and safeguarding of crypto assets or private cryptographic keys used to hold, store or transfer crypto assets for others, is considered a financial service.

And according to Section 1 (11) No. 10 of the KWG, crypto securities are considered financial instruments within the scope of Sections 1 to 3 and 17 and within the meaning of Section 2 (1) and (6) of the KWG.

It should be noted that institutions that conduct banking business or provide financial services require authorization in writing from the supervisory authority, BaFin, in accordance with Section 32 (1) KWG.

German Money Laundering Act and Interpretation and Application Guidance

As mentioned above, financial institutes pursuant to Section 1 (1) of the KWG and financial services institutes pursuant to Section 1 (1a) of the KWG are obliged parties under the Money Laundering Act pursuant to Section 2 (1) No. 2 GwG.

Money Laundering Act and Risk Management

As a result, institutes conducting cryptocurrency custody business or dealing in crypto assets under the Act must prevent money laundering and terrorist financing from taking place through their operations.

The Money Laundering Act stipulates, among other things, that obliged parties must implement a fully functioning risk management system, comply with due diligence obligations towards their customers, and report suspicious circumstances to the German Financial Intelligence Unit.

Risk management is regulated in the second clause of the Act. It follows from the section that obliged parties under Section 4 GwG must operate a risk management system and that this must consist, of a risk assessment (Section 5), internal safeguards, for example through controls (Section 6) and a money laundering officer (Section 7). Furthermore, record-keeping and storage obligations must be complied with (Section 8). There are also group-wide obligations for parent companies that must be complied with in this context.

How Scorechain implements the requirement:

The Case Manager feature of Scorechain's solution is able to provide a reliable solution to the specific section of the act, where risk analysis documentation (such as KYT (Know your transaction), KYA (Know your Address) reports, URLs, notes and comments) can be saved and also be reviewed as frequently as considered necessary by the compliance team. Furthermore, all the above information can be extracted easily and sent to the authorities.

Obliged Entities and Risk Assessment

Obliged entities shall identify and assess their institution-specific risks towards money laundering and terrorist financing. Therefore, according to Section 5 (2) of the GwG obliged entities need to document, regularly review and update the risk assessment and if needed, make this updated assessment available to the authorities. According to the Interpretation and Application Guidance, the regular review should happen at least annually or ad hoc and the changes must be made apparent and must be documented.

According to Section 8 (1) No. 1b GwG the obliged entities are required to record and retain the data collected and information obtained about business relationships and transactions, in particular transaction documents, within the scope of the fulfillment of due diligence obligations, that can be used for transaction investigation purposes.

According to the Interpretation and Application Guidance, the records can be stored digitally on a “storage medium”, but the stored data have to be consistent with the details and information collected, available for the duration of the retention period and can be made readable within a reasonable period of time at any time.

How Scorechain implements the requirement:

Scorechain's platform provides Know Your Address (KYA) and Know Your Transaction (KYT) reports with all the necessary information and can be stored digitally for unlimited time. This information can be retrieved almost immediately.

Obligated Entities and Due Diligence

The third clause of the GwG contains the provisions on the due diligence obligations that the obliged party must retain in relation to the customer. Section 10 of the GwG states that the obliged party must exercise general due diligence. These include, among others, the identification of the contracting party as well as information on the nature of the business relationship. Due diligence must be fulfilled

- according to Section 10 (3) No. 1 of the GwG when establishing a business relationship,
- according to Section 10 (3) No. 2 of the GwG when doing transactions outside the scope of an existing business relationship,
- according to Section 10 (3) No. 3 of the GwG when transactions are in connection with money laundering or terrorist financing and
- according to Section 10 (3) No. 4 of the GwG when there are doubts arising in the course of an existing business relationship in respect of the accuracy of the information collected regarding the identity of the contracting party.

In addition to the general due diligence, there are also simplified due diligence requirements (§ 14) and increased due diligence requirements (§ 15).

How Scorechain implements the requirement:

Although there are IT tools that are specialized in user identification services, Scorechain's solution offers features that support institutions to better assess the level of due diligence (DD) that is adopted by other transacting entities. The Entity Directory amongst others provides detailed information on the level of due diligence that is followed by virtual services providers (such as simplified DD, enhanced DD or just basic Know Your Customer Policies).

As already mentioned, Scorechain provides detailed information on transactions, information on the type of the transacting entity and can even “identify” entities that offer gambling services.

Obligated Entities and Suspicious Activity Reports

Finally, Section 6 of the Act sets out the obligations in connection with reports of factual circumstances. Pursuant to Section 43 GwG, obliged entities must report suspicious activities to the FIU. And according to Section 45 GwG, the report should be filed electronically via the German FIU's web-based system GoAML. GoAML is an IT application provided by the FIU to secure the electronic suspicious activity reporting process via the Internet. According to the Interpretation and Application Guidance, the types of transactions which must be reported if suspicious include non-cash transactions, including electronically executed transactions, cash transactions or other transfers of assets, such as trade-ins of valuables, transfers by way of security or gifts. Furthermore, according to the Interpretation and Application Guidance in chapter 10, the entity and the employees need not to be certain that a corresponding asset has resulted from a predicate offence under Section 261 of the StGB (Strafgesetzbuch - German Penal Code) or is associated with terrorist financing. Since facts, indicating the existence of the circumstances specified in Section 43 (1) GwG are sufficient to trigger the reporting obligation.

How Scorechain implements the requirement:

Scorechain provides all relevant reporting electronically that can be stored safely on the centralized case management feature.

As mentioned already in the current report, the Case Manager feature can provide a platform where such reports can be kept and include all the necessary information such as specific addresses, KYA and KYT reports of suspicious entities and transactions and users can even "attach" URLs and provide comments. In combination with the Risk Indicators feature, such reports are useful for generating reliable results that are also part of a well-structured suspicious activity report filing.

FATF Guidance

The FATF is a self-proclaimed global money laundering and terrorist financing watchdog and comprises, in addition to other observers, associate members and observer organizations, 37 member jurisdictions and two regional organizations. The FATF sets international standards that aim to prevent money laundering and terrorist financing and other related threats to the integrity of the international financial system. The FATF recommendations guidance is one of the most prominent, providing a global standard against money laundering and terrorist financing.

As virtual assets have become more of a relevant concern for the financial sector, the FATF has taken a closer look at their risks and their appropriate regulation. In order to prevent the misuse of virtual assets for money laundering and terrorist financing, the FATF has released a guidance for a risk-based approach for virtual asset service providers (Guidance for a risk-based approach – virtual assets and virtual asset service providers, June 2019) and a report including red flag indicators regarding virtual assets (FATF report virtual assets red flag indicators of money laundering and terrorist financing, September 2020).

The Guidance on the Application of the risk-based approach to VAs (virtual assets) and VASPs (virtual asset service providers) is intended to assist affected national agencies, as well as private entities seeking to engage in VA activities, in gaining an understanding of VA activities and VASPs. The Guidance on red flag indicators contains a collection of indicators of suspicious VA activity or possible attempts to evade prosecution. The Guidance includes indicators on transaction behavior, anonymity, asset origin, geographic risk, recipients and senders. This Guidance is currently being updated (status: June 2021). Prior to that, in October 2018, the FATF had updated its standards regarding the application of FATF standards to VA activities and VASPs. This was done for the purpose of helping jurisdictions mitigate the money laundering and terrorist financing risks associated with VA activities. The Interpretive Note on Recommendation 15 was released in June 2019.

How Scorechain implements the requirement:

The clarification on the implementation of the Guidance and the Red flag indicators by Scorechain is given in chapter “Concretization of the approach through Scorechain”.

Legislative plans of the EU Commission

On 20 July 2021, the European Commission presented an ambitious package of legislative proposals to strengthen the EU's anti-money laundering and countering terrorism financing (AML/CFT) rules. According to the European Commission, the aim of the package is to improve the detection of suspicious transactions and activities, and close existing loopholes used by criminals to launder illicit proceeds or finance terrorist activities through the financial system.

According to the European Commission, the package includes a new EU authority which will be the central authority coordinating national authorities to ensure the private sector correctly and consistently applies EU rules.

Furthermore, the package includes a new regulation on AML/CTF (“single EU rulebook”) which directly sets applicable AML/CFT rules and requirements imposed on obliged entities. The single EU rulebook includes a few additions to the list of obliged entities in the EU. Among those additions are all types and categories of Crypto-Asset Service Providers, which will align the EU legislation with the relevant FATF standards.

The package also includes the sixth directive on AML/CTF as well as a revised regulation on transfer of funds of 2015. The regulation extends its scope to transfers of crypto assets. Therefore crypto-asset service providers will have to include full information about the sender and beneficiary of such transfers with respect to all transfers of virtual assets.

Concretization of the approach through Scorechain

The following table gives a deeper insight on how Scorechain responds with its solution to the requirements set out by global and local regulatory requirements on financial crime prevention in the context of crypto assets. It therefore lists the individual categories of the GwG which includes global and local requirements on risk management obligations and compares them to the implemented measures through the solution.

Category	Implementation of Scorechain Solution	Index origin
Risk Management	Documentation of risk analysis by accessing all relevant KYA and KYT reports.	<ul style="list-style-type: none"> • Section 5 (2) GwG, • Section 25h KWG • FATF Recommendation 11, 18
	Use of Case Manager feature for reporting and notes	
	Alert, tag and group features	
Customer Due Diligence	Information from the company directory: <ul style="list-style-type: none"> • Entity type • Risk ratings (Scx Scoring) • Risk Indicators 	<ul style="list-style-type: none"> • Section 10 (1) GwG and Section 10 (2), 14 (1) and 15 (2) • FATF Recommendations 1, 9 - 21
Transaction Monitoring	High volume transaction	<ul style="list-style-type: none"> • Section 10 (1) GwG • Section 25h (2) KWG • FATF Red flag indicators • FATF Recommendations 16, 19
	Regular transactions with specific pattern	
	Transactions with high-risk jurisdiction	
	Transactions with other VASPs	
	Transactions involved with cases of terrorism	
	Transactions involved with abuse or dark web	
	Transactions involved directly with phishing	
	Flagged VA addresses associated with suspicious activity	
	Transactions to VASP with no VA regulation or low AML/ CFT requirements	
	Transactions to unregistered VASPs	
	Transactions to VASPs with low levels of AML and KYC	
	Transactions involved directly with hacks and/ or scams	
	Use of Case Manager feature for storing all relevant information of ongoing cases	
Suspicious Activity Reporting / Transaction Reporting	Know your Address reporting	<ul style="list-style-type: none"> • Section 43 GwG • FATF Recommendation 20
	Know your transaction reporting	

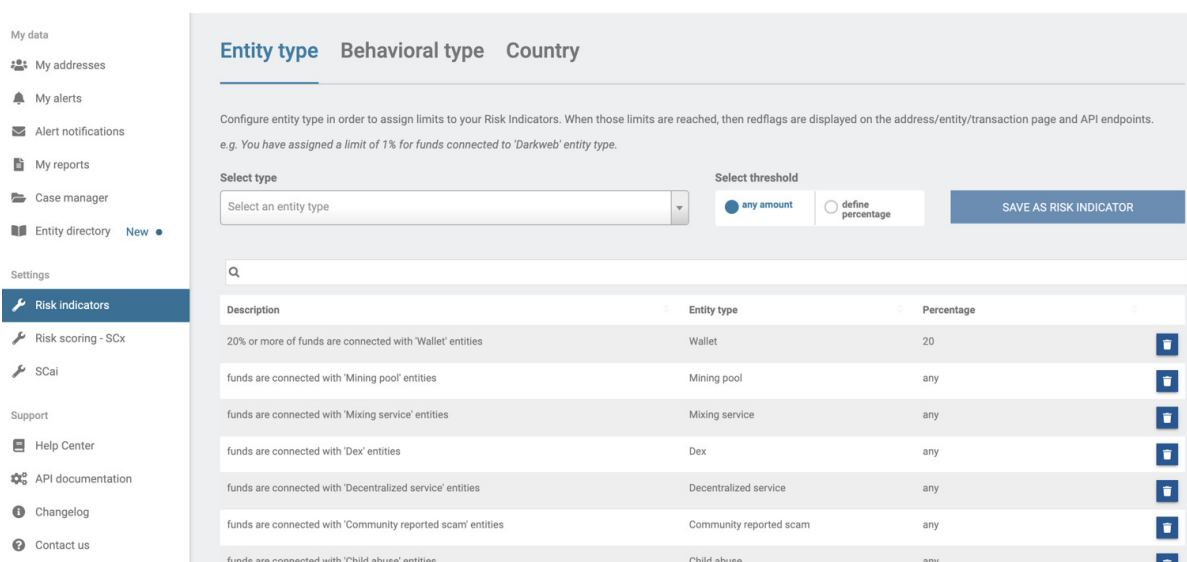
At this point it is prudent to mention that Scorechain is confident to fulfill all existing regulatory requirements towards transaction monitoring of all cryptocurrencies that are already covered by companies.

Risk Ratings

As for risk scoring, the goal is to rate crypto activities (addresses, entities, transactions) depending on the origin and destination of funds. All addresses, entities and transactions have two types of scoring (SCx). One for incoming and one for outgoing funds and it is between one and 100, represented in a pie chart in red, orange, or green color. The closer the score gets to 100, the more trustworthy a transaction/ entity or address is. The closer to 1 the score is, the higher the risk that it imposes. The SCx is computed by tracking the cryptocurrencies received or sent. More specifically, the SCx is based on the in-depth analysis and uses a harmonic mean formula. For each type of entity (exchanges, Darknet websites, mining, etc.), Scorechain sets a default trust index. Default scoring is based on different criteria (example of criteria for exchanges platforms are the KYC level, if there were previous hacking or security breach incidents, if private coins were accepted, if they follow enhanced due diligence policies etc.).

As for risk indicators, the goal is to display actionable risk insight to easily flag suspicious activity for entities, addresses and transactions. Scorechain users are responsible for key risk indicator configuration among more than 350 risk scenarios. Risk indicators can be configured in three scenarios (as also shown in the picture below):

1. Entity risk: this category focuses on the associated risk related to the type of the entity e.g. gambling, decentralized exchanges, etc.
2. Behavioral risk: the specific category refers to the associated risks related to the type of transaction behavior e.g., payment channel, mixing pattern, etc.
3. Country risk: this category refers to the associated AML and CTF risk related to specific jurisdictions.



Entity type Behavioral type Country

Configure entity type in order to assign limits to your Risk Indicators. When those limits are reached, then redflags are displayed on the address/entity/transaction page and API endpoints.
e.g. You have assigned a limit of 1% for funds connected to 'Darkweb' entity type.

Select type:

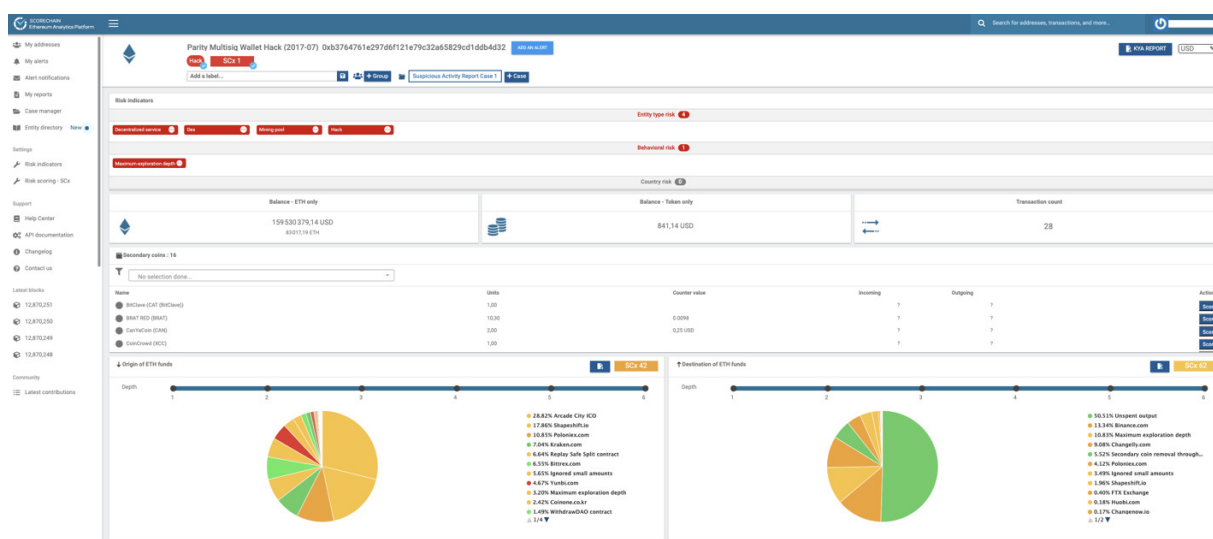
Select threshold: ☒ any amount ☐ define percentage

Description	Entity type	Percentage
20% or more of funds are connected with 'Wallet' entities	Wallet	20
funds are connected with 'Mining pool' entities	Mining pool	any
funds are connected with 'Mixing service' entities	Mixing service	any
funds are connected with 'Dex' entities	Dex	any
funds are connected with 'Decentralized service' entities	Decentralized service	any
funds are connected with 'Community reported scam' entities	Community reported scam	any
funds are connected with 'Child abuse' entities	Child abuse	any

Adhering to German regulatory requirements with the Scorechain S.A. solution

This chapter of the guide will include examples on how Scorechain's solution supports compliance teams on implementing the German Money Laundering Act and mitigate potential risks.

In July 2017, it has widely been reported in the press that a few multi-sig wallet accounts with large balances of ethereum (ETH) have been compromised. The funds of the hack ended up in a specific address (0xB3764761E297D6f121e79C32A65829Cd1dDb4D32). In the picture below, it is shown that the address is flagged on Scorechain's platform. The importance of the specific data is vital for compliance teams that need to make sure, no funds from undesired parties are accepted and that way, all relevant risk management procedures stipulated by the German Money Laundering Act are being taken into consideration.

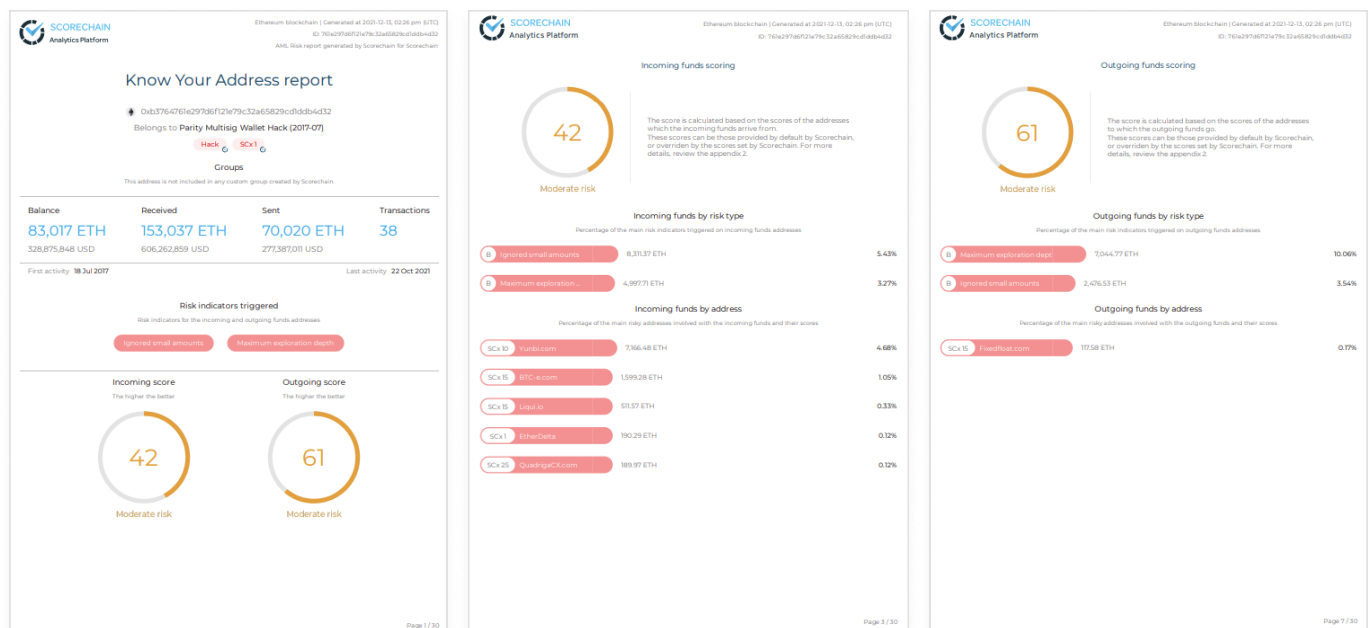


Picture 1: The specific address is shown above and was flagged with a critical Scorechain Index (SCx1) and the warning signal "Hack". At the section "Risk Indicators", further risks can be found (entity type risk, behavioral risk, country risk). SCx is based on the In-depth analysis. The monitoring tool also shows the origin of the funds as well as the destination within a pie chart.

Monitoring and Reporting

In addition to what has been mentioned above, users can activate alerts and monitor any movement of funds related to the specific case and provide a real-time alert system. The importance of the real-time alert system lays on the fact that compliance teams can be notified immediately if additional transactions and/or addresses are involved and thus decide if funds should be frozen. As already mentioned, Scorechain also provides reliable reports that can be used for further investigating transactions and if needed include them in suspicious activity reports to the FIU.

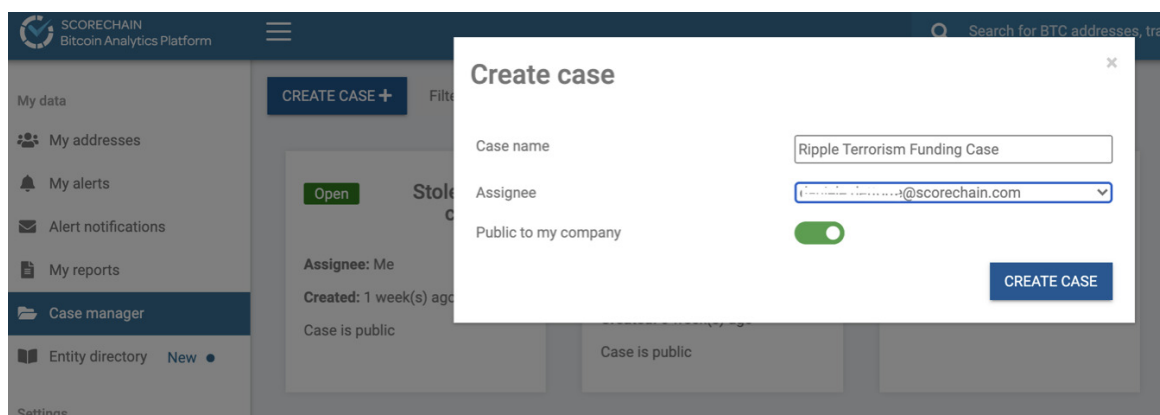
In our case, users can easily access the KYA report of the address through a structured download function. The KYA report provides details on the incoming funds, outgoing funds and the report shows the overall risk level and even includes the risk indicators that are associated with the specific case. It is important to mention the role of risk indicators in the specific example. The risk indicators help users to flag the case as high risk. Consequently, risk indicators along with the overall scoring really help compliance teams to draw an as complete as possible picture of the risk levels of transaction or address.



Picture 2: Here is an example of KYA, including information such as financial data, origin and destination of funds, risk AML scoring for incoming and outgoing funds, and risk indicators.

Let us now take into consideration that the compliance team that spotted the specific issue, collected enough information and wants to file a suspicious activity report as obliged by the German authorities. Scorechain's crypto compliance solution helps users to strengthen their crypto anti-money laundering policies with the feature 'Case Manager' and 'Entity Directory'.

This can be done quite efficiently and easily by using the case manager feature and by adding detailed description of the case, attaching the KYA and KYT reports that have been generated previously and of course add any other useful information to the authorities that need to be officially investigated. As shown below, the suspicious activity report on our example is completed and ready to be filed to the authorities.



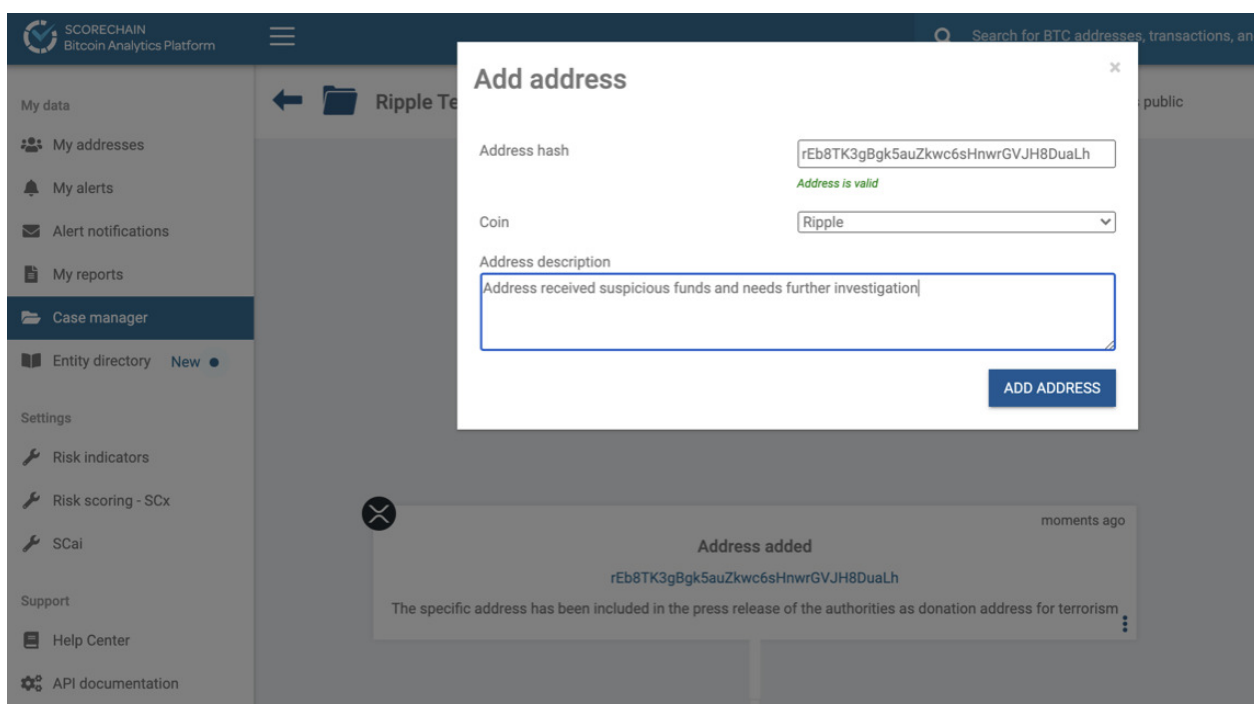
Create case

Case name:

Assignee:

Public to my company: ☒

CREATE CASE



Add address

Address hash:
Address is valid

Coin:

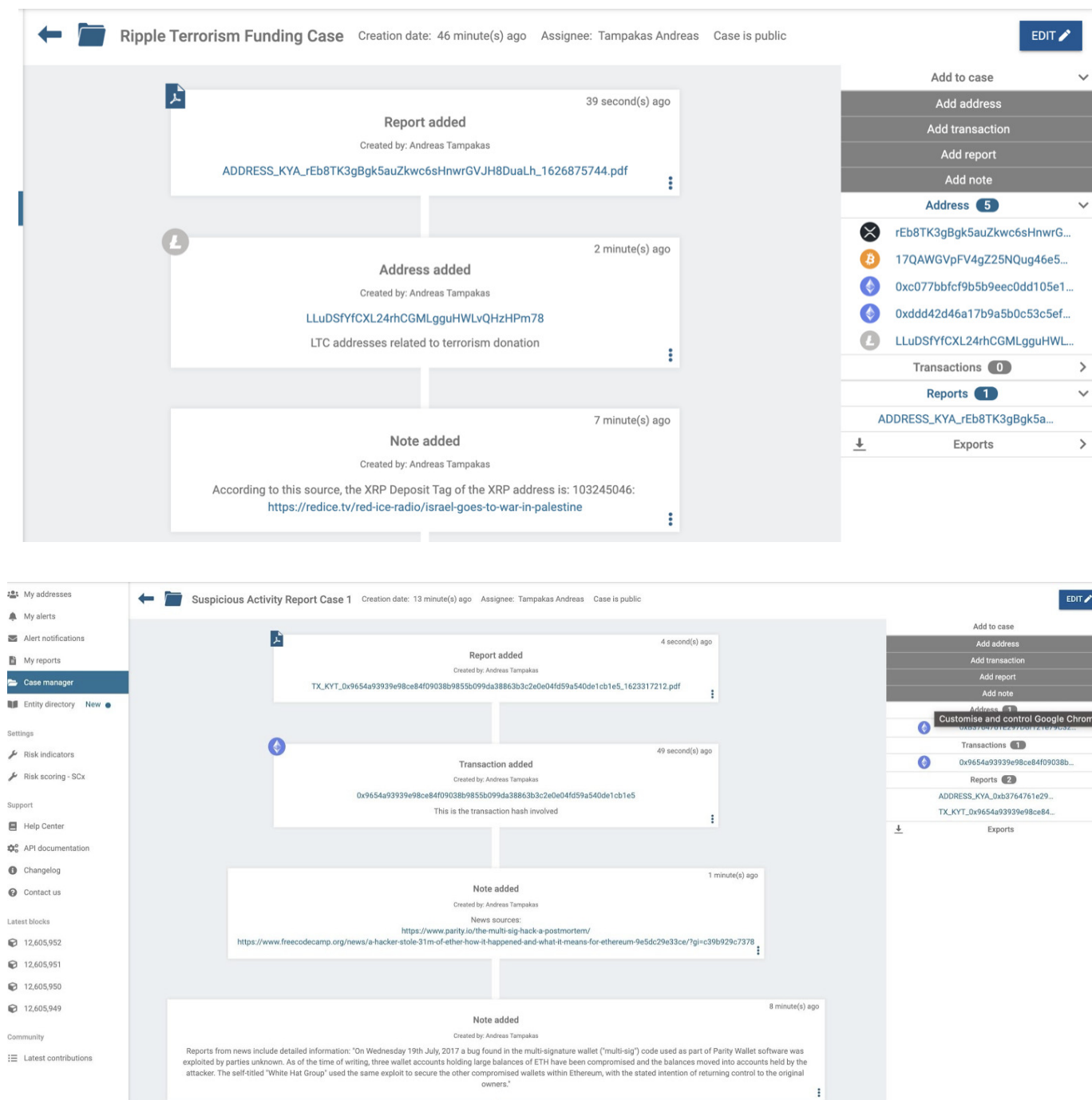
Address description:

ADD ADDRESS

Address added moments ago

rEb8TK3gBgk5auZkwc6sHnwrGVJH8DuaLh

The specific address has been included in the press release of the authorities as donation address for terrorism



The screenshot displays the Scorechain Case Manager interface. The top section shows the 'Ripple Terrorism Funding Case' with details: Creation date: 46 minute(s) ago, Assignee: Tampakas Andreas, Case is public. The case content includes a 'Report added' (ADDRESS_KYA_rEb8TK3gBgk5auZkwc6sHnwrGVJH8DuaLh_1626875744.pdf), an 'Address added' (LLuDSfYfCXL24rhCGMLgguHWLqHzHPm78), and a 'Note added' (According to this source, the XRP Deposit Tag of the XRP address is: 103245046: https://redice.tv/red-ice-radio/israel-goes-to-war-in-palestine). The right sidebar shows options to 'Add to case', 'Add address', 'Add transaction', 'Add report', 'Add note', and a list of addresses including rEb8TK3gBgk5auZkwc6sHnwrG... and 17QAWGVpFV4gZ25NQug46e5....

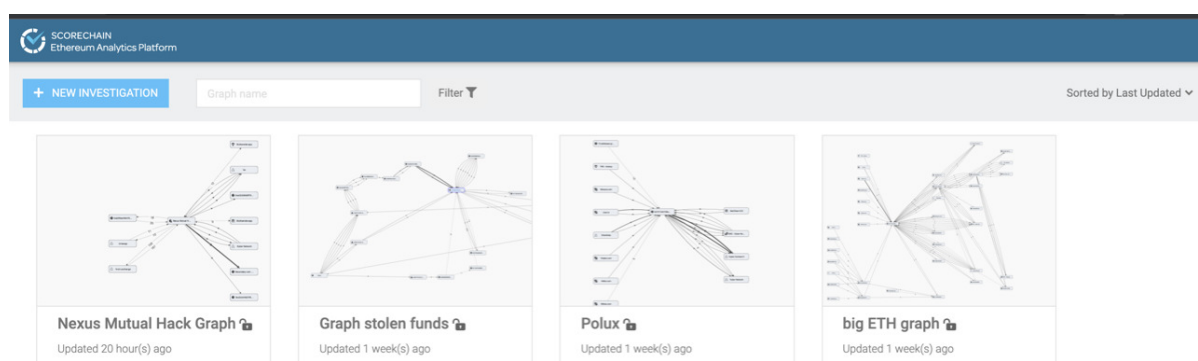
The bottom section shows the 'Suspicious Activity Report Case 1' with details: Creation date: 13 minute(s) ago, Assignee: Tampakas Andreas, Case is public. The case content includes a 'Report added' (TX_KYT_0x9654a93939e98ce84f09038b9855b099da38863b3c2e0e04fd59a540de1cb1e5_1623317212.pdf), a 'Transaction added' (0x9654a93939e98ce84f09038b9855b099da38863b3c2e0e04fd59a540de1cb1e5), and two 'Note added' entries. The right sidebar shows options to 'Add to case', 'Add address', 'Add transaction', 'Add report', 'Add note', and a list of addresses including 0x9654a93939e98ce84f09038b... and ADDRESS_KYA_0xb3764761e29....

Picture 3: This feature provides a useful collaborative tool to handle cases from beginning to end under the coordination of a responsible person while involving several team members. To look for a specific case, one can use different filters: Assignment, status, confidential mode, or just enter the case name in the search bar. The case can be exported as a PDF which gives the investigation audit trail. For each update or any change in the case, the assignee will receive the notification by email.

These examples have been used to give an indication on Scorechain's holistic approach on tackling the associated financial crime risks (including frauds, terrorism financing activities and money laundering). The specific examples also give an idea on how compliance teams can use the software to better implement the German regulatory requirements in an efficient and effective way that helps coping with compliance challenges that go along with this new and highly innovative technology.

Exploration Tool

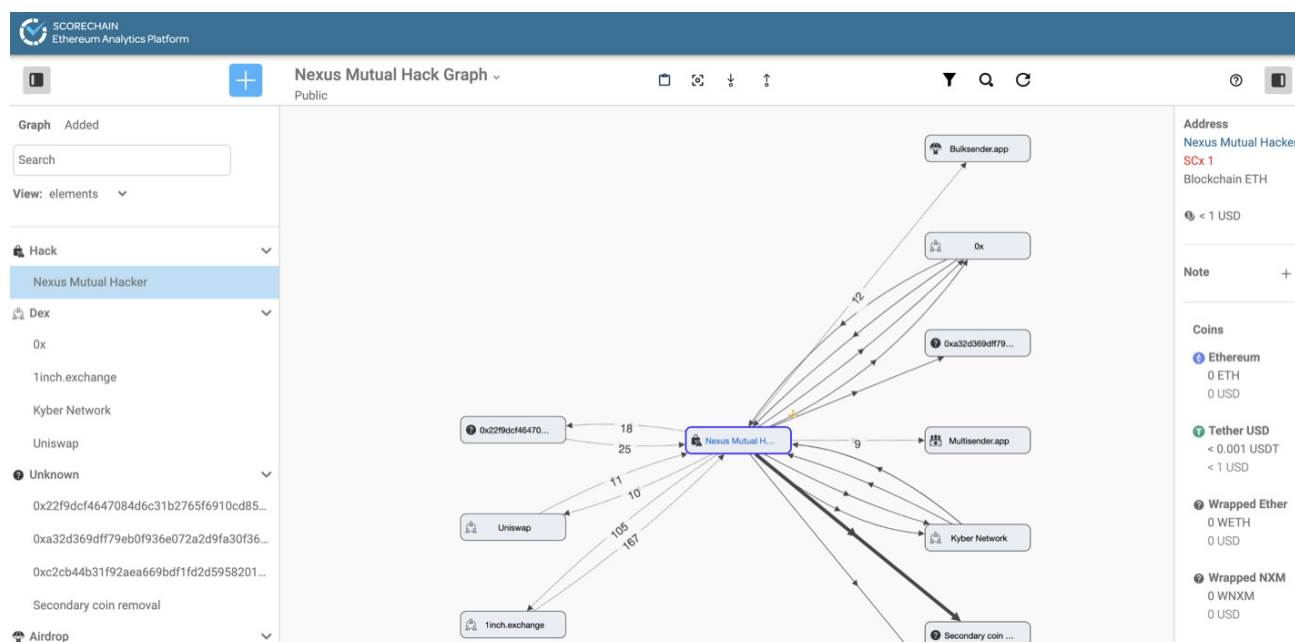
Part of an efficient monitoring procedure is also the proactive investigation since it is fundamental for compliance teams or regulators to be able to trace illegal or suspicious funds and spot where these funds are going in order to take the necessary actions. As a result of that, Scorechain's Exploration Tool is able to conduct investigations on specific crypto addresses or groups of addresses and see clearly how these wallets interact with each other and how they are linked to certain kinds of illicit or suspicious activities. Also, the tool shows their interactions with other types of platforms (exchanges, mining pool, services) and follow the way of the funds. The tool supports all the currencies that are already available in Scorechain's platforms, which means that users can use this tool to investigate Bitcoin, Ethereum, ERC20 tokens, Litecoin, Bitcoin Cash, Dash, XRP Ledger, Tezos and Tron. Consequently, Scorechain's Exploration Tool is a powerful feature that indicates the relationship that exists among different addresses and can clearly demonstrate if funds move from one address to another and give details on the exact path or paths that have been followed. The users can also initiate an investigation by not only using addresses, but also entitles or types or even groups.



Picture 4: Here is an example of the exploration tool interface.

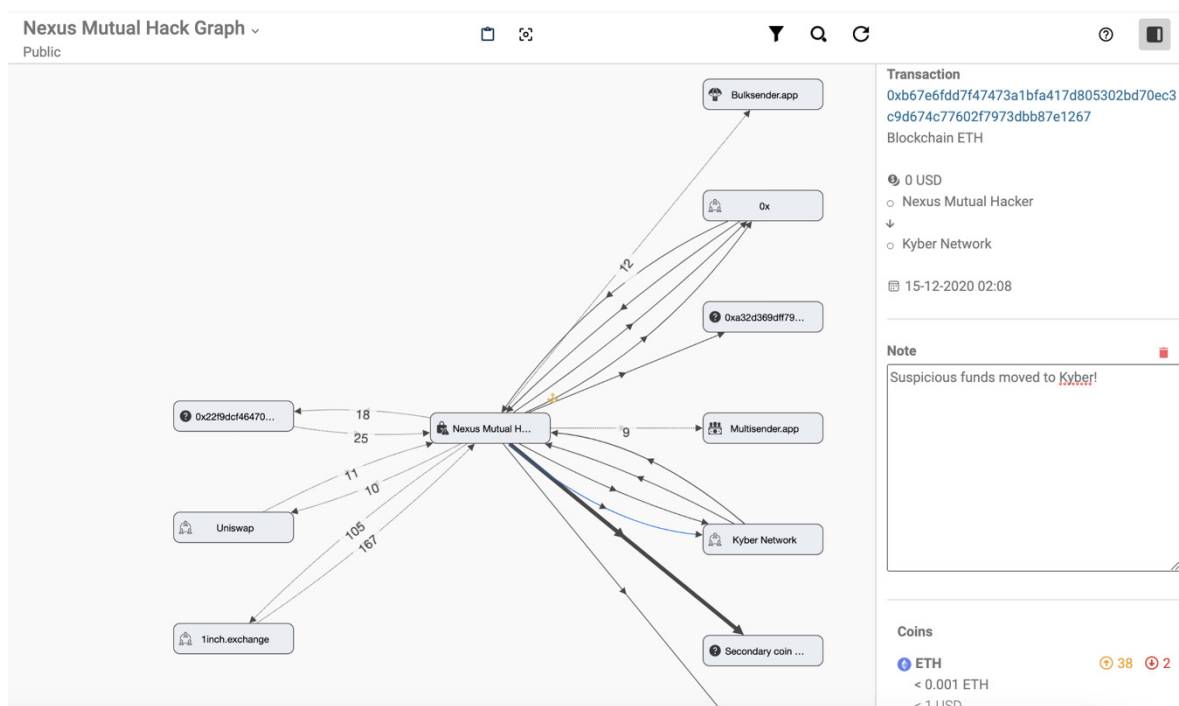
The following case will further help us understand how the exploration tool can be a vital assistant for regulators, law enforcement agencies and compliance teams and showcase what has been described above. In December 2020, there was a serious security breach that lead to a theft of 8 million USD. The hack affected the Nexus Mutual address of the CEO. The Exploration Tool of Scorechain clearly shows the move of the funds (both, the incoming and the outgoing).

It is also worth mentioning the fact that users can click on each address and get more information on the amount that has been transferred, the coin that has been used and also keep notes related to the case they are working on.



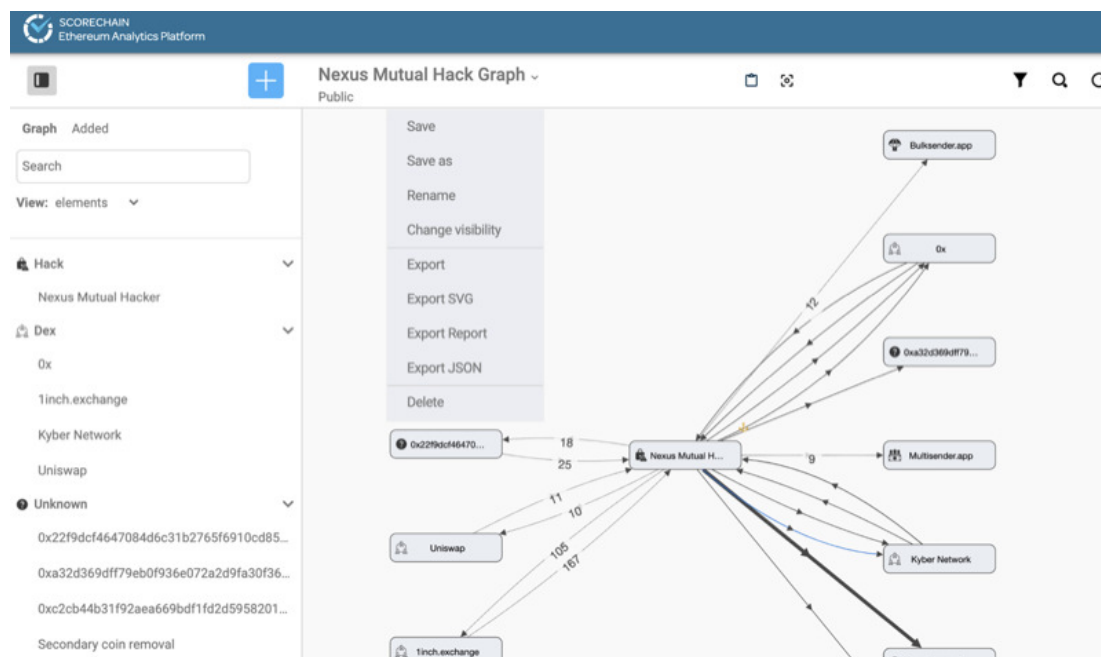
Picture 5: This is the graph of the case that has been described in the current guide. The graph clearly illustrates the moves of both the incoming and the outgoing funds.

To be more specific, the graph shows us that funds moved from the address of the hacker to decentralized exchanges such as Uniswap and 1inch as well as Kyber network and a few unknown addresses. It is also useful to mention that users can also highlight an element by clicking on it in the list or in the graph and get more information about it such as the address details, transactions details and so on.



Picture 6: Here is an example of the how users can get information on the transaction details and also how the note feature works..

Users can also choose to highlight the incoming or the outgoing transaction in the graph and that way get more details and help them understand exactly how funds moved. Last but not least, the users can also save a graph by using the drop-down menu to save a duplicate / rename / change visibility (public to private, and vice versa) and export in different formats: JPG, SVG, Report in PDF, JSON / Del. A feature particularly useful also for record keeping purposes and for filing suspicious activity reports in an accurate a complete matter.



Picture 7: As mentioned above, users can save the graph and even export a report easily and in different formats.

Conclusion and Outlook

Conclusion

It is of fundamental importance that compliance teams of financial institutes can identify abnormal and high-risk activities. Scorechain's tool is aiming to help identifying abnormal activities by providing a risk associated score on transactions and entities by offering a plethora of risk indicators that spot suspicious activities, hacks, phishing, scams, terrorism related activities. The tool also provides information such as VASP's jurisdiction that can affect the overall risk of a transaction, mixing patterns and complex transactions that may raise further questions such as peeling chains transactions. Consequently, and according to EBA's risk factor guidelines, institutes that offer crypto related services, need to implement due diligence and verify their customer's identification and although, Scorechain does not provide identity verification features, Scorechain's software can definitely help in identifying risks and thus assist compliance teams to perform enhanced due diligence or extra checks when needed.

Outlook on Kryptowertetransferverordnung and Travel Rule

Furthermore, the specific guide aims to inform financial institutions trading cryptocurrencies on the basic AML requirements that need extra attention and suggest the ways to deal with. As has already been mentioned, the German authorities have an active role in regulating the crypto sphere. Therefore, on May 26, 2021, the German Federal Ministry of Finance published the ministerial proposal of a regulation on enhanced due diligence requirements for the transfer of crypto assets (Kryptowertetransferverordnung - KryptoTransferV) based on Section 15 (10) Sentence 1 No. 1 of the GwG. The regulation mandates the transmission of information on the originator and recipient when cryptocurrencies are transferred so that transactions can also be tracked in relation to the beneficiaries to prevent misuse for money laundering or terrorist financing purposes. The proposal serves to implement the Financial Action Task Force standards (Recommendation 15 - Interpretive Note 7b, so-called "travel rule" for crypto securities). Furthermore, the proposal mandates that if the transfer is made from or to an electronic wallet that is not managed by a crypto custodian ("unhosted wallet"), the details of the beneficiary or principal of a crypto value transfer must be obtained and retained. Associations had until June 14, 2021 to provide statements on the draft. Pursuant to Section 6 of the Regulation, it shall enter into force two months after promulgation.

The specific draft is clearly stating crypto anonymity as the main source of concern for financing terrorist activities and money laundering that can potentially risk the country's financial stability. The draft is even moving one step forward by suggesting amongst others the transmission of information of the clients and recipients when transferring cryptocurrencies and of course adequate due diligence policies. Scorechain is also closely following the latest updates on FATF's plenary meetings on jurisdictions and how they should regulate and supervise the cryptocurrency ecosystem and also what approach should keep when it comes to the travel rule implementation which will inevitably affect Germany's future regulatory work.

About

About Scorechain

Scorechain is a Luxembourg-based company operating worldwide since 2015. The company spotted quite early the above-mentioned challenges and thus provided a reliable and sufficient cryptocurrency transaction monitoring software for AML/CTF regulation compliance. Scorechain Blockchain Analytics suite helps compliance teams in crypto firms, financial institutes and governmental authorities to reduce their risk exposure of illicit crypto activities when dealing with cryptocurrencies and comply with the regulations.

Scorechain is a European leader in cryptocurrency transaction monitoring and has helped more than 200 customers from more than 40 countries, ranging from cryptocurrency businesses to financial institutes with crypto trading, custody branch, digital assets customers onboarding, audit and law firms and some LEAs.

Scorechain Analytics Suite covers Bitcoin, including Lightning Network, Ethereum with all ERC20 tokens (traceability of swap tokens through DEX), XRP Ledger (IOU tokens), Tezos, Litecoin, Bitcoin Cash, and Dash. Scorechain de-anonymizes blockchain data with more than 60,000 entities identified and allows users to adopt a risk-based approach to cryptocurrency monitoring. The solution provides risk scoring for each crypto transaction/address/wallet with customizable parameters, which allows the users to identify and manage the money laundering risks by implementing their internal control policy. With the 'Risk indicators' feature, users can red flag suspicious activities at the level of entities/transaction behaviors and jurisdictions with more than 350 risk scenarios.

About PwC

PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft is the leading auditing and consulting firm in Germany. PwC sees its mission in building social trust and solving important problems. More than 276,000 employees in 157 countries contribute to this with high-quality, industry-specific services in the areas of auditing, tax and management consulting. The services of PwC also include compliance services around blockchain-based financing projects.

The compliance financial services unit serves its clients with solutions in all issues relating to securities compliance, money laundering and other criminal activities (fraud). The experts in this area support annual audits and consulting projects both nationally and internationally.

List of abbreviations

AML	Anti-Money Laundering
AuA	BaFin's Interpretation and Application Guidance in relation to the German Money Laundering Act
BaFin	Federal Financial Supervisory Authority
CFT	Countering Terrorism Financing
EBA	The European Banking Authority
ETH	Ethereum
EU Commission	Commission European Commission
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GWG	German Money Laundering Act
KryptoTransferV	Kryptowertetransferverordnung / regulation regarding the transfer of crypto assets
KWG	German Banking Act
KYA	Know your Address
KYC	Know your customer
KYT	Know your transaction
LEAs	Aufsichtsbehörden
ML	Money laundering
PwC	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft
SCx	Risk scoring
StGB	German Penal Code
TF	Terrorism financing
URLs	Uniform Resource Locator
VAs	Virtual assets
VASPs	Virtual asset service providers