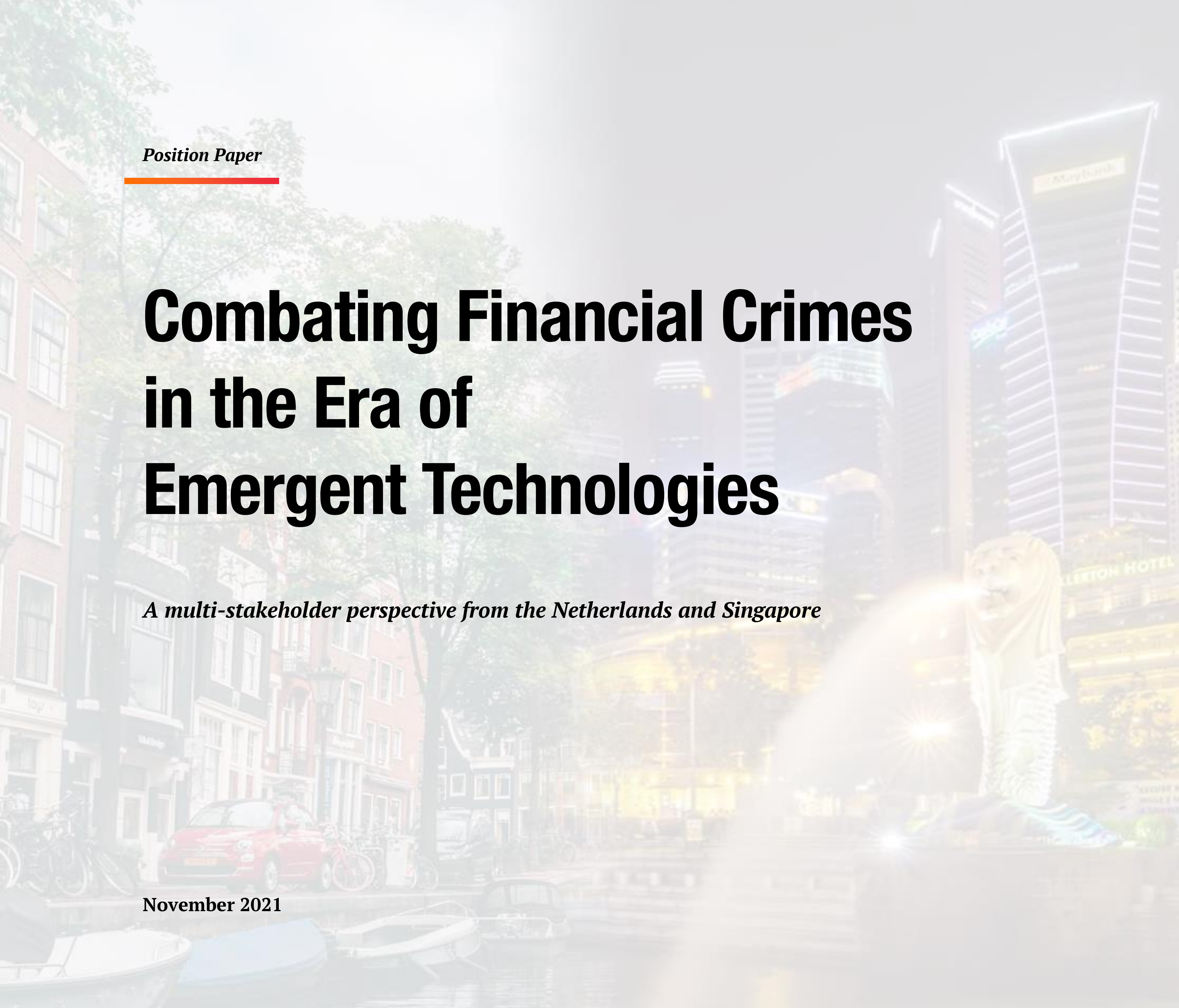

*Position Paper*

# Combating Financial Crimes in the Era of Emergent Technologies

*A multi-stakeholder perspective from the Netherlands and Singapore*

November 2021

Netherlands

Singapore

SPIEGELGRACHT JUWELIERS
12
games
tinkerbell
toys
Tribal Design
JP-153-T

# Executive Summary

On 3 March 2021, the first Roundtable between the Netherlands and Singapore on Combating Financial Crimes in the Era of Emergent Technologies (“Roundtable”) took place. Emergent technologies such as blockchain, cryptocurrencies, artificial intelligence, and privacy-preserving technologies have created many opportunities for innovation and economic growth, as well as a new borderless threat landscape. Since these cyber-enabled financial crimes involve a significant number of threat actors, combating them poses a challenge that requires the collaboration of multiple stakeholders and the utilization of innovative solutions.

The Netherlands and Singapore are both small countries with strong financial centres that are highly digitalized and connected, as well as heavily focused on innovation. This Roundtable is envisioned to build strong foundations of trust and confidence upon which to share our mutual challenges and good practices. During this inaugural meeting, perspectives from all angles of the triple helix were shared, leading to the identification of important topics and development of a prioritized agenda as follows:

1. Virtual Asset Intelligence
2. Information Sharing with Privacy and Security by Design
3. Stronger Know Your Customer (KYC) Facilities
4. Collaborative Mechanisms and Good Practices
5. Regulatory Challenges and Opportunities
6. Complexity of Technology and Data Volumes

During the course of follow-up sessions, it is envisaged that these topics will be deliberated by stakeholders from both countries, deepening our understanding and expertise in combating borderless cyber-facilitated financial crimes.

ABN·AMRO

CFLW
Cyber Strategies

ecXX.com

HSD
The Hague Security Delta

HTX

MERKLE SCIENCE

Ministry of Justice and Security

POLITIE

OPENBAAR MINISTERIE

NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

Embassy of the Kingdom
of the Netherlands

TNO innovation
for life

TAU

Dutch
Blockchain
Coalition
connect and create

# Table of Contents

# Introduction

New and disruptive technologies such as blockchain, cryptocurrencies, artificial intelligence, and privacy-preserving technologies have created many opportunities for innovation and economic growth. However, the convergence of finance and cyberspace has also disrupted the financial crime threat landscape. Today's paradigm for understanding new preventive, investigative, and corrective measures is to collaborate more closely within, between, and across silos to identify the common challenges faced and share good practices in tackling them. In a globalized economy, threats have become borderless and require international cooperation to address. As small countries with open economies, the Netherlands and Singapore share the same vulnerabilities toward cyber-enabled financial crimes in their quest to achieve global pre-eminence as Smart Nations and leading technological innovation hubs.

In the world of digital transformation that involves digital assets, cryptocurrencies, and cross-border peer-to-peer transactions (otherwise known as decentralized finance (DeFi)), how might funds be laundered across borders? Upcoming global regulations aim to instil a higher standard of market integrity, but regulatory requirements may not be evenly implemented in all countries by financial industry participants, impacting the sharing of information across organisational and national boundaries.

The law enforcement agencies and judiciary prosecuting high-tech financial crimes are now faced with tough new questions such as which jurisdiction's laws might be applicable, what kind of evidence would be considered as court-admissible, and how they should work with participants across the chain of digital evidence to ensure artefacts are properly preserved. Even as emergent technologies facilitate new criminal methods, these technologies and artificial intelligence also provide opportunities to combat financial crimes more effectively. New questions arise over how to sustain an information position during a time of increasing globalization and transaction fragmentation, and how to utilise new technologies and solutions to better secure our financial systems.

Many more questions are now being raised as to how best to combat new crimes arising from the convergence of finance and cyberspace. This position paper presents the outcomes of our first Roundtable discussion on these matters organised on 3 March 2021 between the Netherlands and Singapore.

## Partnership between the Netherlands and Singapore

The Roundtable and its follow-up activities are organised by the Partners for International Business (PIB) – the Netherlands–Singapore on Blockchain[1]. PIB is a public-private partner initiative from the Netherlands.

Singapore is transforming into one of the most digitalized and technology-focused nations in South East Asia, as well as in the world. Its focus on becoming a Smart Nation, with a digital economy, government, and society, has also led to Singapore paying more attention to the digitalisation of daily lifestyle activities and business uses, including that of digital assets and the blockchain.

The Netherlands has been an excellent market for technological experiments, with forward-thinking corporates and government participating in numerous projects. In addition, it has proven to be a frontrunner in the field of blockchain and digital assets, resulting in a vibrant ecosystem, proficiency in cyber-criminal investigations, and the accumulation of expertise through developing use cases and proofs of concepts.

The Dutch blockchain ecosystem is highly interconnected, and this means that Singaporean partners not only have access to the organizations in the PIB, but are also just a handshake away from many other potential partners. The goal of the PIB is to co-create innovative solutions to solve complex global challenges such as those addressed in this position paper on cyber-enabled financial crimes. This Roundtable, together with its follow-up activities, is one such solution.

[1] https://www.dutchblockchainsolutions.com

## Roundtable

The Roundtable facilitated an open and informal dialogue on problems involving cryptocurrency (digital assets) and blockchain applications, which pose multi-stakeholder challenges. Participants contributed their various perspectives on challenges faced and practices that worked well, enabling us to set and prioritize an agenda according to relevance, importance, and practical considerations.

Compared to other leading blockchain communities, the Netherlands is performing especially well in regards to implementing the “triple helix model” for cooperation, where government, industry, and research institutes join forces to develop solutions. In the same vein, this Roundtable solicits from the perspectives of all members of the triple helix.

Arising from the Roundtable discussion, this position paper identifies specific agenda items for further discussion, sharing of perspectives, and deepening of understanding through regular meetings. The Roundtable follows Chatham House rules whereby none of the statements or recommendations may be attributed to specific persons or organisations.

# Problem Statement

To set the tone for the Roundtable discussion, the following problem statement was articulated:

In 2010, 10,000 bitcoins were worth only the price of 2 pizzas. During that period, bitcoin was associated with the “dark side” of the internet comprising marketplaces such as Silk Road and AlphaBay, and used in illicit transactions and criminal proceeds. During that time, the prevailing wisdom was that “bitcoin is bad but blockchain is good”.

As a measure of mainstream adoption of cryptocurrency, 1 bitcoin is now worth about USD50,000 in March 2021, which values the 2 pizzas at about USD500 million in 2010! Visa, Paypal, Fidelity, and other regulated financial institutions are now intermediating bitcoin and other cryptocurrencies such as ethereum (ETH), with the participation of retail and institutional investors. Cryptocurrency is increasingly viewed as an alternative asset class for investors, with Morgan Stanley, for example, offering its wealthy clients access to bitcoin funds.

The story of bitcoin and the larger cryptocurrency space has developed quickly since 2009. The potential that people saw in bitcoin during its earlier days has since become a reality. For example, cross border bitcoin remittances used to require a $30-50 fee and 3-5 days, but has since become free and can now be initiated within 10 minutes and completed within an hour.

Innovations in cryptocurrency or virtual asset space now include non-fungible digital tokens (NFTs) offering digital uniqueness, confidentiality-enhanced digital coins and wallets, stablecoins, digital bonds and financial instruments, digital representation of currencies, fractionalised ownership, and DeFi. The crypto ecosystem is deepening and maturing, regulations are being enacted for fit-and-proper governance, and mainstream adoption is increasing.

However, perverse uses of bitcoin and the crypto ecosystem are still prevalent. Bitcoin remains a major payment instrument in the dark web that is used to facilitate cybercrimes like ransomware and scams, and enable transactions of illicit materials like drugs. Fast Layer 2 payment, anonymous-enhanced wallets and coins, and DeFI can also serve as criminal tools offering pseudo-anonymity.

The second, and main focus of the Roundtable, was on guarding against the misuse and abuse of crypto. Given the human, technological, and financial aspects of fighting financial crime, successful criminal detection and investigations would involve transnational collaboration across both developed and under-resourced jurisdictions, as well as multi-disciplinary expertise and tools.

In combating crypto-facilitated crimes, how should effective governance and cooperation be implemented? As an example, crypto-related anti money laundering (AML) detection can be roughly divided into three technical layers from the top downwards:

1. The application layer (based on red flag indicators),
2. The blockchain layer (based on blockchain graph analysis)
3. The network or dark web layer (involving filters and monitoring tools for TOR, I2P, VPN, IP address, etc).

At each layer, different tools, tactics, and processes are employed. There are real world identifiers at the application layer, and meta data and technical identifiers at the blockchain and network or dark web layers.

Aggregating cross-layer identifiers for analysis can help to assemble a fuller picture more quickly. Therefore, information sharing between participants, within each layer and between each layer, is key. But there are also important personal and data privacy laws as well as secrecy laws to consider. As we can see in the above example, there are multiple factors to take into consideration in the development of effective crypto-related AML tools, processes, and practices.

In the multi-stakeholder setting of the Roundtable with representatives from the Netherlands and Singapore, cross-industry experts shared their experiences and views on how to better combat crypto-related cyber financial crimes, and the practical governance and cooperation steps to take going forward.

# Initiatives from the Netherlands and Singapore

The following are highlights of the perspectives shared by participants during the Roundtable discussion.

## Transaction Monitoring Nederland

TMNL stands for Transaction Monitoring Netherlands[2], a joint initiative by five Dutch banks: ABN AMRO, ING, Rabobank, Triodos Bank, and de Volksbank. TMNL provides a platform for these banks to collectively monitor their payment transactions for signals that could indicate money laundering or flow of criminal funds. Collective transaction monitoring improves the odds of detecting criminal money flows and networks. The banks would still be required to monitor their own transactions independently, in accordance with their obligations under Dutch anti-money laundering legislation (the Anti-Money Laundering and Anti-Terrorist Financing Act, or ‘Wwft’).

## FinTech Regulatory Sandbox Singapore

The FinTech Regulatory Sandbox[3] enables financial institutions and FinTech players to experiment with innovative financial products or services in a live environment but within a well-defined space and duration.

Depending on the experiment, the Money Authority of Singapore (MAS) provides the appropriate regulatory support by relaxing specific legal and regulatory requirements prescribed by MAS that the entity otherwise would be subject to, for the duration of the sandbox.

[2] https://tmnl.nl/summary-eng/
[3] https://www.mas.gov.sg/development/fintech/regulatory-sandbox

The sandbox includes appropriate safeguards to maintain the overall safety and soundness of the financial system, facilitating the gathering of insights and practical experience in mitigating “real world” risks. Upon successful experimentation and on exiting the sandbox, the sandbox entity must fully comply with the relevant legal and regulatory requirements.

## Takedown of Bestmixer.io

On 22 May 2019, the Fiscal Information and Investigation Service (FIOD[4]) and the Public Prosecution Service took one of the largest online mixers for cryptocurrencies, Bestmixer.io, offline [5]. This operation dealt a severe blow to efforts to conceal criminal money flows through the use of coin mixers. Six operational servers were dismantled and seized in the Netherlands and Luxembourg.

The investigation was conducted in close cooperation with the Dutch Digital Intrusion Team (DIGIT), Europol, and the authorities in Luxembourg, France, and Latvia. In June 2018, the Financial Advanced Cyber Team (FACT) of the FIOD commenced the investigation under the supervision of the National Public Prosecutor’s Office for Serious Fraud and Environmental Crime and Asset Confiscation, acting upon a report from cyber security company McAfee.

The investigation gathered information pertaining to transactions between customers and Bestmixer.io. The customers were from all over the world, especially the US, Germany, and the Netherlands. The FIOD analysed the information together with Europol, thereafter sharing their findings with other countries as appropriate.

[4] Dutch: Fiscale inlichtingen- en opsporingsdienst (FIOD)

[5] https://www.fiod.nl/the-fiod-and-the-public-prosecution-service-take-money-laundering-machine-for-cryptocurrencies-offline/

## Virtual Assets Red Flag Indicators

Virtual assets use innovative technology to swiftly transfer value around the world and have many potential benefits, including making payments faster and cheaper. But the anonymity associated with them also attracts criminals, who have used virtual assets to launder proceeds from a range of offences such as the drugs trade, illegal arms smuggling, fraud, tax evasion, cyber-attacks, sanctions evasion, child exploitation, and human trafficking.

In response, the FATF Report on Virtual Assets - Red Flag Indicators[6] of Money Laundering and Terrorist Financing will help national authorities detect whether virtual assets are being used for criminal activity. Based on more than 100 case studies collected by members of the FATF Global Network, it highlights the most important red flag indicators that could suggest criminal behaviour. Key indicators in this report focus on:

- Technological features that increase anonymity - such as the use of peer-to-peer exchanges websites, mixing or tumbling services or anonymity-enhanced cryptocurrencies
- Geographical risks - criminals can exploit countries with weak, or absent, national measures for virtual assets
- Transaction patterns - that are irregular, unusual or uncommon which can suggest criminal activity
- Transaction size – if the amount and frequency has no logical business explanation
- Sender or recipient profiles - unusual behaviour can suggest criminal activity
- Source of funds or wealth - which can relate to criminal activity

[6] http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html

## Cyber-enabled Financial Crimes Trend Report

Arising from an INTERPOL Virtual Discussion Room on 2 July 2020 and officially launched during the INTERPOL Working Group on Dark Web and Virtual Assets on 14 December 2020, the Cyber-enabled Financial Crimes Trend Report provides research on security measures taken against financial crimes facilitated by virtual assets and darknet service providers[7].

This report analyses the cyber-enabled component of financial crimes, with a specific focus on darknet and cryptocurrencies. In particular, innovative payment solutions and anonymity enhanced cryptocurrencies (AEC) are being exploited by new white-collar criminals to build a service-based black market within a virtual underground economy (the Dark Web). Intrinsic properties of cryptocurrencies, namely their pseudo-anonymity and non-traceability, do not comply with baseline anti-money laundering and anti-illegal flow controls such as transparency of value transfer. This paper identified key trends driven by the cyber-enabled components and has mapped these trends onto current leading security measures, providing input for risk-based approaches to combating innovative financial crimes.

## A Privacy-friendly Way to Harness Data

Data sharing and analysis are essential when it comes to achieving economic growth and solving societal challenges. However, data sharing remains constrained by commercial and/or legal barriers, including the fundamental right to privacy. Innovative technologies such as Federated Learning and Multi-Party Computation offer a way to address this issue by securely learning from sensitive data derived from multiple sources, without having to share this data. TNO's white paper[8] provides more details about this initiative.

[7] https://cflw.com/2020/12/21/combatting-cyber-enabled-financial-crimes-in-the-era-of-virtual-asset-and-darknet-service-providers/

[8] https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/data-sharing/secure-multi-party-computation/harness-data-privacy-friendly-way

# Identified Agenda Items

Based on voting among the participants, we have prioritized the agenda items for combating cyber-enabled financial crimes as follows:

1. Virtual Asset Intelligence
2. Information Sharing with Privacy and Security by Design
3. Stronger KYC Facilities
4. Collaborative Mechanisms and Good Practices
5. Regulatory Challenges and Opportunities
6. Complexity of Technology and Data Volumes

Notably, the first four agenda items were closely scored.

The following sections summarize the different perspectives shared during the Roundtable on the six agenda items.

## Virtual Asset Intelligence

- The Netherlands authorities have developed about 100 red flag indicators in respect to Anti-Money Laundering using virtual assets. These red flag indicators have been shared with all the banks, payment processors, and related service providers.
- One of the key benefits of this public-private collaboration is for both sides to share the same feedback loop based on intelligence from Financial Intelligence Units (FIUs), and be better equipped to battle financial crime. This was also the basis for forming TMNL. The Netherlands' red flag report was a key source of inputs for FATF's 2020 Red Flag report.

- Cryptocurrencies are trending at the moment, and fall within the scope of experimentation and learning at TMNL.
- Another Netherlands-Singapore initiative with further potential for testing and collaboration is that of Merkle Science's blockchain graph analytics and TMNL, involving the refinement and filtering out of false negatives. The experience and lessons learnt can be shared with stakeholders from both countries.
- Dark Web Intelligence comprising cryptocurrency addresses and IP addresses, and deeper studies into the relationship between cyber-attacks and financial crime such as ransomware attacks, should be another key area for exploration, with the potential to lead to better-informed virtual asset intelligence positions for both private- and public-sector parties.
- Challenges faced within the data and intelligence context are the high data volumes and need for competent methods to gather intelligence and share the insights with analysts and operators. There is a need to transcend black- and white-lists and develop explainable artificial intelligence capabilities which support investigators effectively and efficiently.

## Information Sharing with Privacy and Security by Design

- The innovation and design of future tools to detect financial crime may require combining data from different regulated entities such as financial institutions. Such data is likely to be protected under regulations and laws. On a national level, sharing between entities, and across industries is challenging enough. Sharing at the transnational level is even more challenging.
- New Privacy Enhancing Technologies like secure multi-party computation (MPC) offer opportunities to learn insights and detect financial crime based on sensitive data from multiple banks without actually having to share such data, thus ensuring privacy and security by design. MPC could potentially be a high tech-based solution balancing both regulatory needs for data secrecy and confidentiality with detection and investigative needs for composite data.

- Multi-party computation for AML (MPC4AML) is a project in the Netherlands, with two major Dutch banks and TNO applying MPC to look beyond the perspective of a single organisation and help build models for advanced analytics. This collaboration is envisioned to be expanded on an international level, and is one of the opportunities to strengthen Singapore-Netherlands collaboration in the sharing of data to fight cybercrimes.

## Stronger KYC Facilities

- While transaction monitoring is important, there is also a strong need to focus on Know Your Customer (KYC). The benefits of strong KYC rules and implementation flow downstream and accrue to transaction monitoring. Developing a compliance function that incorporates holistic views, integrating KYC-client due diligence with transaction monitoring, is an essential component of any up-to-date crypto-KYC program.
- Working with national identity facilitators such as DigID (Netherlands) and SingPass (Singapore) to incorporate real-world identifiers can also help to ensure regulatory compliance.
- We should aim to develop a topology with red flag indicators and integrated KYC-transaction monitoring to provide data relevant to suspicious transaction reports, as well as advanced tech-based analytics to process high volumes of STRs.

## Collaborative Mechanisms and Good Practices

- Collaboration is challenging and involves lots of effort, adding on to the workload of day-to-day responsibilities. However, collaboration is essential to combating cyber-enabled financial crimes. How do we convince multiple entities to come together, build trust, and work hand-in-hand despite their usage of different tools and methodologies?
- Transaction Monitoring Netherlands (TMNL) was established in 2020, through which five banks (ABN AMRO Bank, Rabobank, ING, Triodos, and Volksbank) shared datasets to derive insights that

could not be obtained by the banks individually. This initiative will shortly be releasing its first few alerts.

- The ability of Trusted Third Parties such as TMNL to foster cross-border collaboration appears constrained by data-sharing restrictions. New Privacy Enhancing Technologies such as Secure Multi-Party Computation could provide a solution to this challenge.
- After taking down bitcoin mixer “Bestmixer.io”, Dutch law enforcement agency FIOD seized all relevant back-end information such as wallets, IP addresses, and transactions, and shared it via Europol with other interested countries. This gave birth to new country partnerships, illustrating that countries clearly saw the value and importance of international collaboration.

## Regulatory Challenges and Opportunities

- Singapore’s regulatory sandbox has been an important opportunity to regulate the FinTech and cryptocurrency space in a learning environment, with MAS consulting the industry extensively before finalizing the framework. In 2020, the first company, ECXX, was approved to operate from the sandbox, their strategy having been to work on different portfolios in parallel, such as crypto exchange, digital payment tokens, BTC, and ETH.
- A factor complicating governance is the transnational nature of the flows, which often take place between developed and developing countries’ jurisdictions.
- Singapore’s Payment Services Act is a core regulation to address cryptocurrencies and virtual assets, while the Netherlands also began regulating the cryptospace since 2020. The Roundtable recognises that the virtual asset space should not be allowed to operate without proper checks and balances.
- The Roundtable will monitor and participate in the FATF’s March 2021 consultation pertaining to Travel Rule guidance, which is expected to be released later in 2021. Information sharing standards such as IVMS101 are needed. Adoption is expected to progress step by step, but is key to improving the ecosystem’s information position.

## Complexity of Technology and Data Volumes

- Disruptive technology creates new technological complexities that require deeper understanding. This is usually accompanied by extreme volumes of data that cannot be processed manually, and require smart analytics and artificial intelligence for sense-making.
- Specific examples of data overload can include suspicious activity or suspicious transaction reports (SAR/STRs) filed by FIs and VASPs on cryptocurrency/virtual assets. Given the high levels of interest anticipated in this space, SAR/STRs volume is likely to overwhelm FIUs' available bandwidth and expertise. Hence, there is a need to equip FIUs with improved analytics to assess, summarize, and flag out the most important elements to the attention of operators and analysts.
- Potential solutions include tapping the blockchain to bring together tools and parties efficiently to deal with complex crime –for example, in sharing evidence securely and with integrity. FIUs should also consider exploring how new technologies such as AI-based algorithms can be used to their strategic advantage.

BITCOIN DIGITAL DECENTRALIZED CRYPTO PEER
999 FINE COPPER

# Conclusion and Recommendation

Based on an voting approach among the participants the agenda items focused on the combat against cyber-enabled financial crimes are prioritized as follows:

1. Virtual Asset Intelligence
2. Information Sharing with Privacy and Security by Design
3. Stronger KYC Facilities
4. Collaborative Mechanisms and Good Practices
5. Regulatory Challenges and Opportunities
6. Complexity of Technology and Data Volumes

It should be noted that the top four agenda items showed minor differences after voting.

Given the enthusiasm, high level of information density, and ample common ground, it is recommended to proceed with this dialogue on a regular basis and schedule follow-up sharing sessions to discuss the identified agenda items in greater detail. It would be up to the participants as to whether further activities could be established beyond this dialogue to deepen the partnership between the Netherlands and Singapore.

# Annex 1. Agenda and Participants

*Setting the Scene*
Mr Boon-Hiong Chan, Deutsche Bank Singapore on framing the problem space

Sharing Perspectives

*Governmental Perspectives*
Reinier Bredenoord, Public Prosecutors Office of the Netherlands on international cryptocurrency challenges
Dr Jonathan Pan, Home Team Science and Technology Agency (HTX) on opportunities presented by disruptive technologies such as blockchain

*Banking or Virtual Asset Service Provider Perspectives*
Ivich Hoffman, ABN AMRO Bank on innovation partnerships in transaction monitoring and KYC
Branson Lee, ECXX on the first digital asset exchange within the MAS Regulatory Sandbox

*Tech Industry Perspectives*
Dr Mark van Staalduinen, CFLW Cyber Strategies on insights into cryptocurrency abuse in the Dark Web
Mriganka Pattnaik, Merkle Science Co-founder and CEO on innovative tracking and tracing of cryptocurrency transactions and evolution in cryptocurrency cybercrime

*Academic Perspectives*
Dr Daniel Worm, TNO on Multi-party computing for privacy-preserving KYC information sharing
Prof. Lam Kwok Yan, NTU on the Cybersecurity Actions for Virtual Assets (CAVA) project

The Roundtable was moderated by Bert Feskens of the The Hague Security Delta.

# Colophon

## Partners for International Business

https://www.dutchblockchainsolutions.com/

## Photos

Amsterdam by Chait Goli via Pexels:
https://www.pexels.com/nl-nl/foto/foto-van-boten-geparkeerd-op-de-rivier-2031706/
Singapore by Kin Pastor via Pexels:
https://www.pexels.com/nl-nl/foto/marina-bay-sands-singapore-777059/
Private key by cottonbro via Pexels:
https://www.pexels.com/nl-nl/foto/hand-usb-technologie-vasthouden-5474298/
Bitcoin by Rūdolfs Klintsons from Pexels
https://www.pexels.com/photo/nature-people-internet-metal-7293793/

Maybank
STRAITS TRADING
HSBC
HSBC
UBS
OUE
LLERTON HOTEL
THE FULLERTON BAY HOTEL
EXCUSE ME
WHILE I TAKE
A SHOWER

**Partners for International Business**

**The Netherlands – Singapore**

**on Blockchain**

NL Netherlands

Singapore