Blockchain Intelligence Forum 2025

Co-Hosts:

NATIONAL INSTITUTE FOR RESEARCH AND DEVELOPMENT IN INFORMATICS - ICI BUCHAREST

BLOCKCHAIN INTELLIGENCE Professionals Association

Supporting Organization:

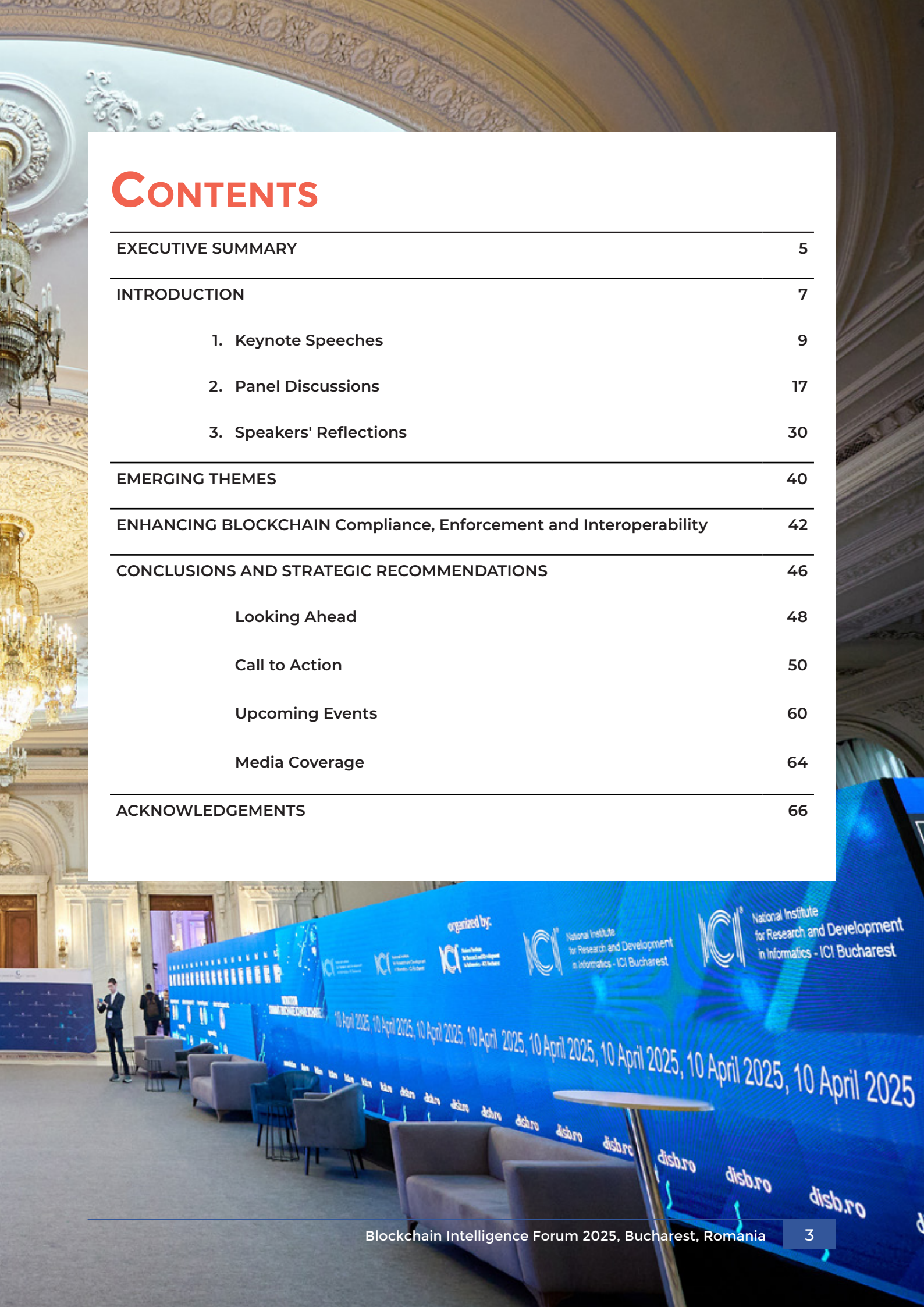
BASEL INSTITUTE ON GOVERNANCE

10 April 2025
Palace of Parliament, Bucharest, Romania

EVENT REPORT


Is initiated by:
IDEA FACTORY THINK TANK
and organized by:
under the auspices of:
in partnership with:
supported by:
ICI DIGISERVICES

Contents



EXECUTIVE SUMMARY

The inaugural Blockchain Intelligence Forum 2025, co-hosted by ICI Bucharest and the Blockchain Intelligence Professionals Association (BIPA) and held alongside the Digital Innovation Summit Bucharest, marked a significant milestone in the establishment of blockchain intelligence as a recognized professional discipline.

The first of many.

On 10 April 2025, over 500 delegates from more than 35 countries, including government officials, and leaders from central banks, financial institutions, law enforcement agencies, regulatory bodies, and blockchain analytics firms, gathered in Bucharest at the iconic Palace of the Parliament to participate in the Forum.

Keynotes, panel discussions, and case studies focused on the importance of establishing common standards for blockchain intelligence, developing professional training pathways for independent accreditation, and - building frameworks to enable the interoperability of blockchain data.

Given the transformative potential of blockchain technology to reshape finance, governance, and security globally, the lack of common blockchain intelligence capabilities, regulatory alignment, and skilled practitioners, could hamstring adoption and exacerbate systemic risks.

Keynote speeches by Dr. Victor Vevera (ICI Bucharest), Nico Di Gabriele (European Central Bank) and Vincent Danjean (INTERPOL) set the strategic tone for the Forum:

- Blockchain intelligence must evolve beyond crypto-asset tracing to proactive, predictive and standards-driven methodologies that are transparent and independently verifiable
- Cross-border cooperation and data interoperability are fundamental to the effectiveness of law enforcement operations and regulatory oversight given the transnational nature of crypto-assets.
- Sustained investment in training, investigative tools and ethical frameworks is essential to transform blockchain intelligence into a core pillar of global financial and security ecosystems.

Panel discussions examined:

- The barriers to unlocking blockchain intelligence for investigations and asset recovery,
- The urgent need for data exchange standards and technological interoperability,
- The benefit to the sound management of firms (including banks) providing crypto-asset services and in turn to financial stability,
- Ways to embed blockchain analytics into existing anti-money laundering (AML), countering the financing of terrorism (CFT) and sanctions compliance frameworks.
- Using blockchain technology in registers of beneficial owners.

Investigators and regulators stressed the pivotal role of Multifunction Crypto Intermediaries (MCIs)– firms providing at the same time more crypto-asset services such as exchange and custody–and the necessity of strengthening supervisory models and compliance expectations through blockchain intelligence integration.

A key outcome of the Forum was the launch of the Blockchain Intelligence Improvement Pledge, a voluntary initiative encouraging blockchain analytics providers and crypto-asset service firms to align their methodologies, attribution standards, and cooperation frameworks using common standards and industry best practices.

The Forum concluded with strong calls to action:

- Deepened collaboration across public, private and academic sectors;
- Acceleration of blockchain intelligence-specific training and certification pathways;
- Embedding blockchain intelligence capabilities at the heart of financial regulation, law enforcement and corporate compliance.

In particular, the Forum invited supervisory authorities and blockchain analytics providers to join new interoperability projects and standards initiatives in the coming year, reinforcing global efforts to enhance transparency, security and trust in blockchain technology.

For public authorities, the Forum highlighted actionable pathways to strengthen investigative effectiveness, reduce compliance ambiguity, and build institutional resilience against crypto-enabled crime.

By engaging with the Blockchain Intelligence Improvement Pledge and interoperability initiatives, stakeholders can benefit from cutting-edge tools, harmonized standards, and a collaborative international network–all designed to make blockchain intelligence more accessible, reliable, and impactful.

The Blockchain Intelligence Forum 2025 set a decisive direction:

Blockchain intelligence is no longer an emerging add-on to financial crime investigation and compliance–it is becoming a central pillar in ensuring global security, economic integrity, and innovation.

INTRODUCTION

The State of Blockchain Intelligence Today

Blockchain technology is not confined to crypto-asset markets and has embedded itself across financial services, logistics, healthcare, identity management, and increasingly, criminal ecosystems.

While the inherent transparency of blockchain transactions offers investigative opportunities, it also poses new, complex challenges for law enforcement, regulators, and compliance professionals. In particular, Multifunction Crypto Institutions (MCIs) which internalize transactions among their clients (off-chain recording) reduce transparency.

At the same time, criminals and other illicit actors have rapidly adapted blockchain innovations for their nefarious purposes.

Decentralized finance (DeFi), privacy coins, decentralized exchanges (DEXs) and self-custodial wallets provide means to obscure asset ownership and movement of value at a scale and speed traditional financial crime frameworks were simply not designed to handle.

Despite the associated risks, the institutional response to blockchain-enabled crime has been fragmented, and investigative capabilities vary widely between countries.

Data interoperability remains limited and existing compliance regimes often fail to adequately address the technical complexity of on-chain transactions.

There are also no universal professional standards for blockchain intelligence.

These challenges were underscored by leading authorities during the Blockchain Intelligence Forum 2025 and echoed in insights from INTERPOL, the Basel Institute on Governance, and financial regulators participating in the Forum.

As blockchain technology reshapes the future of finance and digital assets, four critical needs emerge for building effective blockchain intelligence frameworks:

Harmonised Standards

Without consistent data attribution, investigation methodologies and regulatory definitions, cross-border investigations will remain slow and fragmented.

Professional Training Pathways

Blockchain intelligence demands a new breed of professional, combining technical literacy, forensic investigation skills, financial compliance expertise, and ethical integrity.

AI and Real-Time Analytics Integration

Manual tracing of blockchain transactions is increasingly unsustainable given the sheer volume of blockchain transactions. Intelligence must move toward predictive analytics, anomaly detection, and automated risk identification, without sacrificing legal admissibility.

International Cooperation and Data Interoperability

Financial crime is global, and blockchain technology has accelerated the globalization of illicit fund flows – a key reason why blockchain intelligence networks and the technological platforms that monitor and combat such threats need to be interoperable.

The Blockchain Intelligence Forum 2025 was convened precisely to address these pressing issues.

Throughout the keynote speeches, panel discussions, case studies, and roundtables, delegates agreed that investment in blockchain intelligence capabilities is no longer optional, it is essential to safeguard financial stability, security and innovation.

This report captures the key insights, challenges, and forward-looking strategies identified during the Forum, offering a blueprint for governments, regulators, financial institutions, and technology providers to navigate the emerging blockchain intelligence landscape.

1. Keynote Speeches

The Blockchain Intelligence Forum 2025 brought together a lineup distinguished international experts, policymakers, and industry leaders, each offering unique insights into the evolving landscape of blockchain intelligence.

Keynote speeches, presentations, and case studies explored the current state of blockchain adoption, regulatory challenges, enforcement needs, and the broader vision for a harmonised and professionalised blockchain intelligence ecosystem.

The following summaries distil the core messages and contributions of the Forum's key speakers, providing a concise overview of their perspectives and strategic recommendations.

"Innovation has value when it translates in improvements for people's life… we can harness the full potential of technological innovation and make the financial system more stable which is a pre-condition for sustainable economic growth."

1.1 Digitalizing Finance to Boost Economic Growth

In his keynote address, Nico Di Gabriele, Senior Team Lead at the European Central Bank (ECB), highlighted the potential for profound impact of blockchain technology on the digital transformation of the financial sector. He emphasized that digital finance is no longer a distant prospect but an evolving reality that is reshaping how financial services are delivered, regulated, and secured. Technological advances offer an opportunity to create an integrated European capital market for digital assets, a goal the ECB has been always supportive.

He acknowledged the European Union's leading role in regulating crypto-asset activities through the Markets in Crypto-Assets Regulation (MiCA) but stressed that ongoing dialogue among regulators, financial institutions, and blockchain innovators is essential to maintain market integrity and trust, to ensure financial stability.

Di Gabriele also highlighted the need for data interoperability standards, particularly as financial assets move increasingly towards tokenization. He advocated for investment in blockchain intelligence capabilities, including tools and training that enable supervisors and compliance teams to detect, trace, and understand on-chain activity in real time.

He emphasized that in a more digitalized world the role of cybersecurity can hardly be overestimated and efforts have to be made to ensure the availability, reliability and sound management of data which have become a key driver in whichever business sector.

A major theme of Di Gabriele's speech was the critical need for establishing harmonized regulatory frameworks across the globe. Without regulatory alignment, he warned, the risks associated with decentralized finance (DeFi), tokenization, and new forms of digital assets could outpace supervisory capabilities.

In closing, he called for pragmatic public-private sector collaboration to drive responsible innovation, support economic growth, and bolster the resilience of the financial system in a digital-first world.

Nico Di Gabriele, Senior Team Lead
European Central Bank

1.2 Emerging Supervisory Frameworks for Stablecoin Issuance - Challenges and Opportunities

Skyler Pinna, Director and Technical Advisor at the New York State Department of Financial Services (NYDFS) began his keynote by discussing how stablecoins were designed to be global financial products but were first created in the absence of any clear supervisory requirements. To address this gap, various jurisdictions have begun to implement supervisory frameworks to oversee stablecoins.

Pinna further expanded on similarities and differences across these emerging frameworks. He highlighted that supervisors share common core principles, but sometimes diverge in terms of technical requirements. Stablecoin issuers often seek to have their product available globally, and so may seek to modify their issuance models and operating structures to comply with emerging requirements.

In closing, Pinna noted these differences also present a great opportunity for supervisors to collaborate and learn from one another as they continue to implement and build on their respective frameworks.

Skyler Pinna, Director and Technical Advisor
New York State Department of Financial Services

1.3 Strengthening International Police Cooperation to Combat Cyber-Enabled Financial Crime

Vincent Danjean, Head of INTERPOL's Cyberspace and New Technologies Laboratory, delivered a powerful message on the evolving challenges law enforcement faces in tracing illicit blockchain transactions. He highlighted how the pseudo-anonymous nature of blockchain networks, combined with the rapid rise of privacy coins and decentralized finance (DeFi) tools, has made traditional investigative methods increasingly difficult.

Danjean emphasized the growing role of automation and artificial intelligence (AI) in blockchain investigations, explaining how large language models and AI-aided pattern analysis now help classify blockchain activities and detect suspicious transactions. However, he warned of the significant challenges posed by the "black box effect," where investigators cannot fully explain or reproduce AI-driven findings, posing a risk to the admissibility of evidence in judicial proceedings.

A major challenge Danjean addressed was cross-border jurisdictional fragmentation. He explained that when investigative teams in different countries use different blockchain analytics providers, their data, tags and taxonomy can vary, complicating efforts to share intelligence and collaborate effectively. He described INTERPOL's work in developing the Darknet and Virtual Assets Taxonomy (launched in 2018) to promote interoperability between agencies and solution providers.

Danjean also underscored the critical need for public-private partnerships but added that true success will come from including "the people" themselves. He urged law enforcement, regulators, and private firms to engage more directly with citizens to address the crimes that affect them most.

In closing, Danjean called for inclusive collaboration, innovation, and a commitment to protecting human rights in the digital age, reinforcing INTERPOL's leadership in developing blockchain investigative guidebooks, training programs, and global standards to combat financial crime.

Vincent Danjean, Head of Cyberspace and New Technologies Laboratory
INTERPOL

1.4 Setting the Foundation for Professional Blockchain Intelligence and Harmonised Standards

Dr. Victor Vevera, Director of ICI Bucharest, opened his keynote by underlining the importance of building a trusted ecosystem around blockchain technology, particularly as its applications expand beyond crypto-assets into digital identity, public registries, and critical infrastructure.

He described ICI Bucharest's landmark public-private partnership with blockchain intelligence firm ChainArgos and the creation of the Blockchain Intelligence Academy, which has as its mission "training in service of the truth" as a key foundational step in establishing rigorous, independently verifiable standards for blockchain intelligence.

Vevera emphasized that building blockchain intelligence capabilities requires a balance between technological innovation, human expertise, and ethical governance. He recognized how Bucharest emerged as a strategic hub for blockchain intelligence leadership, with ICI Bucharest playing a central role in promoting data interoperability, fostering law enforcement cooperation, and facilitating academic collaboration.

Closing his address, Vevera invited stakeholders to join a Working Group to help establish the role of the blockchain analyst as a recognized profession, expressing confidence that through collaboration, blockchain technologies can enhance economic growth, social trust, and bolster the fight against financial crime.

Dr. Victor Vevera, General Director
National Institute for Research & Development in Informatics - ICI Bucharest

Advancing research and development to establish robust standards for blockchain intelligence and data sharing.

Developing strong, evidence-based training programs to build a skilled workforce.

Formalizing blockchain intelligence as a recognized profession with active efforts to include it in the European Skills, Competences, Qualifications and Occupations framework.

1.5 From Black Boxes to Open Standards: A Call for Accountable Blockchain Intelligence

Patrick Tan, General Counsel for ChainArgos and co-founder of the Blockchain Intelligence Academy, delivered an impactful keynote underscoring the critical challenges facing the blockchain intelligence field. As blockchain technology and crypto-assets increasingly intersect with criminal activity, the current state of blockchain tracing, with its lack of transparency, open standards, and reproducible outcomes, is problematic.

Blockchain tracing frequently operates in "black boxes," relying on methodologies that are not always transparent or rigorously tested, despite which, findings can still be used to impact fundamental human rights.

To address these challenges and advance the integrity of the blockchain intelligence discipline, Patrick advocated for a collective commitment by stakeholders to three fundamental pillars:

1. Blockchain Data Interoperability: The ability to seamlessly exchange and understand blockchain data across platforms and jurisdictions is paramount. Achieving this requires broader standardization efforts, to establish universally acceptable data formats and taxonomies in order to unlock the power of shared intelligence and allow stakeholders to independently verify results.

2. Transparency and Open Standards: Blockchain intelligence must be built on established math and forensic science, moving away from untested pseudo-science and questionable methods. This commitment is crucial for ensuring findings are independently reproducible, and withstand scrutiny in court, particularly where civil liberties are impacted.

3. Robust, Rigorously Tested Methodologies: Analyzing blockchain activity should be approached as a data science task, and not one based on subjective opinion. This necessitates leveraging advanced tools and techniques that are subject to rigorous and resilient testing to ensure insights are based on independently verifiable scientific principles, and not just intuition.

In closing, Patrick highlighted ChainArgos' commitment to sign the pledge proposed by the Blockchain Intelligence Professionals Association, urging all industry stakeholders to support these principles, to elevate the standards of the blockchain intelligence discipline to serve as a force for good, grounded in collaboration, transparency, and scientific rigor.

Patrick Tan, General Counsel and Co-Founder
ChainArgos, Blockchain Intelligence Academy

1.6 The Blockchain Intelligence Centre of Excellence

Dr. Paul Gilmour introduced the Blockchain Intelligence Centre of Excellence (BICE). The University of Portsmouth is proud to collaborate with the National Institute for Research & Development in Informatics - ICI Bucharest and ChainArgos, a partnership that will position the university as the UK's only Blockchain Intelligence Centre of Excellence and further strengthen the global reach and impact of the Blockchain Intelligence Academy. Together with ICI Bucharest and ChainArgos, the BICE aims to:

- Engage global partners, prosecutors, financial institutions and other industry professionals to deliver professional certification and forensic training programs to equip students with the skills needed to meet employer demand for expertise in tracing illicit crypto-asset payments and combating cybercrime and economic crimes.
- Establish global standards for admissible evidence reliant on blockchain intelligence
- Support research in blockchain technology whilst strengthening the impact on international policy and practice.

Blockchain technology is decentralized and borderless. However, law enforcement agencies are sitting in silos in their respective jurisdictions, left to face the onslaught of economic crime wrought by permissionless, pseudonymous transactions facilitated by blockchain. It is hoped that the BICE can provide a safe space for global cooperation and collaboration between law-enforcement agencies, and former students of the BICE, who would have developed their openness and camaraderie as a result of their shared learning experience.

Dr Gilmour highlighted the close existing ties that the University of Portsmouth has with government, law enforcement and industry professionals that will enable the delivery of robust in-person and distance learning training. With a large student market in criminology, this partnership is a great opportunity for the university to provide academic expertise and ensure blockchain intelligence training is delivered effectively to a global audience of students.

Dr. Paul Gilmour, Senior Lecturer
University of Portsmouth

1.7 Standardising Crypto-Asset Data Exchange for Scalable Blockchain Intelligence

Bernhard Haslhofer provided a data-driven keynote addressing the growing complexity facing blockchain intelligence professionals as crypto-asset transaction volumes and investigative challenges continue to increase exponentially. Drawing from a decade of experience, he argued that the future of blockchain investigations lay not merely in improving tracing tools, but in controlling and standardizing the underlying data.

Haslhofer identified the critical role played by attribution tags—data points that link blockchain addresses to real-world entities—as essential for scaling investigations and making blockchain intelligence effective. He explained that without reliable, standardized tags, investigations risk inconsistency and inefficiency.

Key initiatives he highlighted included:

- The creation of TagPacks, an open standard developed with INTERPOL for structured data exchange;
- The establishment of a Darknet and Virtual Assets Taxonomy for blockchain services and abuses, enabling interoperability across investigative platforms; and
- Collaboration with legal scholars to ensure that blockchain intelligence methodologies meet global legal standards and produce evidence that is verifiable and admissible in court.

Haslhofer used a striking analogy – just as astronomers moved from using telescopes manually to analyzing vast data sets through automated systems, blockchain intelligence must evolve in the same way—transitioning from manual investigation to automated, scientifically rigorous data analysis at scale.

He concluded by reaffirming that automation, interoperability and empirical methodologies are not optional luxuries, but necessary foundations for blockchain intelligence to remain effective and credible in the face of rapidly growing complexity.

Bernhard Haslhofer, Co-Founder
Iknaio

2. Panel Discussions

In addition to the keynote presentations, the Forum featured a series of in-depth panel discussions that examined blockchain intelligence from diverse operational, regulatory and supervisory angles.

These sessions brought together senior investigators, financial regulators, legal experts, and blockchain analytics professionals to share practical experiences, highlight challenges and co-develop solutions.

The panels provided a platform to deepen the Forum's central themes, enhancing cross-border cooperation, strengthening compliance frameworks and driving the evolution of blockchain intelligence into a mature and professional discipline.

The following summaries distill the key insights and contributions from each panel.

Monica Guy, Senior Specialist, Communications and External Relations, **Basel Institute on Governance** (Moderator), **General Antonio Mancazzo**, Commander, Privacy Protection and Technological Fraud Unit, **Guardia di Finanza, Italy**, **Major Francesco Venditti**, Deputy Officer, Fraud Protection and Technological Fraud Special Unit, Guardia di Finanza, Italy, **Daniel Leon**, Cryptocurrency Specialist, **Europol EC3** (Digital Support Unit - Cyber Intelligence), **Marian Müller**, Head of Education, **Caudena**, **Oleksii Geyko**, Senior Detective, **National Anticorruption Bureau of Ukraine**, **Alexandru Donciu**, Specialist, Financial Investigations - Virtual Assets, **Basel Institute on Governance**.

2.1 Overcoming Obstacles in the Use of Blockchain Intelligence for Law Enforcement and Asset Recovery Efforts

This panel led by the Basel Institute on Governance brought together senior investigators, financial crime specialists, and blockchain analytics experts to discuss the challenges in maximizing the potential of blockchain intelligence for criminal investigations and asset recovery.

According to the moderator, experts of the Basel Institute's International Centre for Asset Recovery (ICAR) find that law enforcement agencies face significant challenges in dealing with the growing use of blockchain technologies to transfer and launder money linked to corruption and other serious crimes. There are gaps in human resources, skills, knowledge and tools. Low-income jurisdictions find it difficult or impossible to access costly private-sector blockchain analysis tools and services or to obtain appropriate training.

Through case studies in Ukraine and Italy, the panelists demonstrated the potential of blockchain intelligence to contribute to investigations and increase asset recovery success rates. For example, in a single tax evasion case, Italy's Guardia di Finanza was able to successfully seize EUR 130 million in assets. The representatives explained how they now use blockchain intelligence not only as part of ongoing cases, but to actively search for potential cases of tax evasion and other crime.

Daniel Leon of Europol explained that the use of crypto-assets for crime has now spread to every single crime area, in contrast with the past, when it was mainly used for cybercrimes. He and other panelists emphasized the urgent need for law enforcement to improve capabilities, cooperation and data interoperability with regard to blockchain intelligence.

A specific challenge mentioned was access to sophisticated blockchain analytics tools. Aside from their often high cost, panelists also noted that different private-sector tools have different strengths and weaknesses. For example not all are powerful enough to support investigations into large organized crime cases. Decision makers are often disconnected from operational realities in law enforcement to understand how a particular tool can be useful. This leads to blockages in acquiring the right tools and training personnnel to use them.

The panel also discussed the critical shortage of trained personnel who understand both blockchain technology and forensic investigative techniques. Without clear standards or training pathways, it is difficult for agencies to build up their specialist capabilities or to collaborate efficiently on multi-agency investigations. Investment in practical multi-agency and cross-sector training programs, such as those offered by the Basel Institute and ICAR, was endorsed as a pressing need.

Panelists noted that blockchain crime investigations often stall because jurisdictions differ sharply on regulatory requirements, legal definitions, and enforcement capabilities. International cooperation is vital here, including through events and initiatives such as the Blockchain Intelligence Forum and the Global Conference on Criminal Finances and Cryptoassets, which is organized annually by the Basel Institute, Europol and UNODC.

2.2 Towards Data Exchange Standards and Interoperability - CEO Level Discussions

This high-level panel gathered CEOs from various blockchain analytics firms to address the fundamental challenges in standardizing blockchain intelligence data exchange across the financial, law enforcement and regulatory sectors.

The discussion opened with the recognition that fragmentation in blockchain data standards is a major barrier to effective cross-border investigations and supervision. While blockchain data is theoretically public, differences in attribution methods, analytics models, and evidential standards often undermine cross-border cooperation and slow investigations.

Several CEOs emphasized that without common frameworks for interpreting blockchain data, investigators and compliance officers risk 'speaking different languages' when sharing intelligence across jurisdictions or between institutions.

Panelists underlined that blockchain intelligence needs to move beyond proprietary silos and that interoperability must be integrated into the very foundation of blockchain intelligence systems, not added as an afterthought.

Key challenges identified included:

- Inconsistent data labeling and attribution practices among blockchain analytics providers;
- Legal and regulatory divergences—such as differing standards for what constitutes “suspicious activity” or “ownership” of digital assets;
- Technological incompatibilities in case management and evidence preservation systems, which hamper coordinated action.

Emerging solutions discussed included:

- The development and adoption of open-source standards for blockchain data classification and metadata annotation, such as the TagPacks standard;
- Efforts to create regulatory frameworks that mandate minimum interoperability standards for blockchain intelligence within financial institutions and service providers;
- Encouraging analytics providers to align voluntarily with initiatives like the Blockchain Intelligence Improvement Pledge, launched during the Forum.

The panel concluded with a strong consensus that interoperability is not merely a technical challenge but a governance, legal, and strategic priority. Only by aligning definitions, data models and investigative protocols can blockchain intelligence become a truly global tool for crime prevention, financial stability, and regulatory oversight.

Javier Paz, Director of Data and Analytics, **Forbes** (Moderator), **Jonathan Reiter**, CEO, **ChainArgos**, **Dhirendra Shukla**, CEO, **Gray Wolf Analytics**, **Karl Zettl**, CEO, **Iknaio**, **Nate Tuganov**, CEO, **Caudena**, **Marina Khaustova**, COO, **Crystal Intelligence**.

Sundri Khalsa, Intelligence Specialist, CEO and Founder, **PaperBallotchain** (Moderator), **Patrick Tan**, General Counsel, **ChainArgos**, **Tamar Latsabidze**, Chief Specialist of VASPs, AML Inspection and Supervision, **National Bank of Georgia**, **Yehuda Shaffer**, Former Chief, **Israel Financial Intelligence Unit** (FIU) and Former Deputy State Attorney, **Dylan Cuschieri Tonna**, Senior Manager (Financial Crime Compliance), **Financial Services Authority of Malta**, **Peter Engering**, CEO and Founder, **Compliance Champs**, **Maksym Dragunov**, Director for Policy and Advisory, **Crystal Intelligence**, **Matthias Bauer-Langgartner**, Head of Policy (Europe), **Chainalysis**.

2.3 AML, CFT, and Sanctions Evasion - How does blockchain intelligence fit in?

This panel gathered regulatory experts, blockchain analytics professionals, and financial investigators to explore the evolving threat landscape of crypto-asset-enabled money laundering, terrorist financing (CFT) and sanctions evasion.

A key theme was that while blockchain transparency offers investigative opportunities, criminals increasingly exploit anonymity-enhancing techniques such as:

- Layering transactions across multiple chains ("chain-hopping");
- Using privacy coins and decentralized mixers;
- Leveraging DeFi protocols that lack Know Your Customer (KYC) controls.

Panelists stressed that traditional compliance frameworks, such as existing Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) rules, are ill-suited to counter these new laundering models. There was broad agreement that blockchain-specific investigative capabilities must be embedded directly into standard AML/CFT compliance programs to be effective.

The panel also discussed significant regulatory gaps, highlighting the uneven global adoption of the Financial Action Task Force (FATF) Travel Rule, particularly among Virtual Asset Service Providers (VASPs) and pointed out that inconsistent implementation creates exploitable loopholes.

There were also concerns around the lack of clarity regarding beneficial ownership of crypto-asset wallets, which complicates enforcement, and asset freezing.

Delays in freezing illicit assets– caused by complex, multi-jurisdictional legal hurdles–were identified as a persistent problem. Some panelists noted that while blockchain tools can detect suspicious activity early, legal systems are often too slow to act on the intelligence.

Emerging best practices shared included:

- Integrating blockchain analytics into transaction monitoring systems for real-time detection of laundering typologies;
- Enhancing collaboration between compliance teams, blockchain forensic firms and law enforcement;
- Training financial crime units in interpreting and preserving blockchain evidence that meets judicial standards for admissibility.

The panel concluded by underscoring that AML, CFT, and sanctions enforcement frameworks must evolve to match the speed, complexity and innovation of crypto-asset-enabled financial crimes, with blockchain intelligence playing a central role in future regulatory and enforcement strategies and frameworks.

2.4 The Role and Regulation of Multifunction Crypto-Intermediaries (MCIs)

This panel focused on the challenges and solutions related to the supervision of Multifunction Crypto Intermediaries (MCIs), including exchanges, custodians, wallet providers, and other entities that facilitate crypto-asset transactions.

The discussion opened by acknowledging that MCIs occupy a pivotal position in the crypto-asset ecosystem, acting as gateways between decentralized blockchain networks and traditional financial markets.

However, weaknesses in MCIs' compliance controls—particularly regarding customer due diligence (CDD) and transaction monitoring—continue to expose financial systems to risks of money laundering, terrorist financing, and sanctions evasion.

Panelists emphasized that regulatory supervision models for MCIs remain uneven across jurisdictions, creating vulnerabilities that criminals can exploit. Several panelists discussed the ongoing issue of regulatory arbitrage, where crypto-asset firms relocate to jurisdictions with the weakest regulatory oversight to avoid scrutiny.

The panel also highlighted the problem of delayed or inconsistent reporting of suspicious transactions, which hampers enforcement efforts.

Technological challenges were also raised, with many MCIs lacking integrated blockchain intelligence capabilities within their compliance monitoring systems. This technological gap was identified as a key barrier to proactive risk detection and mitigation.

Emerging solutions discussed included:

- Mandating the adoption of blockchain analytics as part of MCIs' AML/CFT frameworks;
- Developing risk-based supervisory models that account for crypto-asset-specific threats and evolving typologies;
- Encouraging international regulatory collaboration to prevent jurisdiction "shopping" and promote harmonized standards;
- Fostering a culture of compliance within crypto-asset intermediaries that positions blockchain intelligence not as a regulatory burden, but as a strategic asset for building trust and resilience.

The panel concluded that MCIs must not only meet baseline regulatory requirements but also proactively invest in blockchain intelligence capabilities to strengthen the security, integrity and credibility of the broader digital finance ecosystem.

Nico Di Gabriele, Senior Team Lead, **European Central Bank** (Moderator), **Maha Al-Saadi**, Head of Regulatory Affairs, Financial Services, **Qatar Financial Centre**, **Skyler Pinna**, Director and Technical Advisor, **New York State Department of Financial Services**, **Luke Wilson**, Global Head of Public Sector, **Allium**, **Dr. Bernhard Haslhoffer**, Co-Founder, **Iknaio**, **Christian Miccoli**, CEO, **Conio**, **Andrea Minto**, Professor, **University of Venice and Stavanger**.


THE ROLE AND
REGULATION OF
MULTIFUNCTION
CRYPTO-
INTERMEDIARIES
(MCIS)
ANCOM
PARAPH
smart alliance

2.5 The Role of Blockchain Intelligence in Law Enforcement

This panel gathered senior representatives from INTERPOL and Europol to explore how blockchain analytics are being integrated into traditional investigative frameworks and facilitate international policing cooperation.

A key theme that emerged was how blockchain analytics has become central to modern investigations. Both Daniel Leon (Europol) and Vincent Danjean (INTERPOL) highlighted that blockchain intelligence now plays a critical and expanding role across cybercrime, financial crime, and organized crime investigations. Law enforcement agencies increasingly rely on blockchain analytics for both strategic intelligence and evidential support in criminal cases.

Panelists underscored that while on-chain data is immutable and trusted, the attribution of blockchain addresses to real-world entities remains a persistent challenge.

The need for investigators to rigorously validate attribution claims, particularly when relying on private-sector blockchain analytics providers was stressed. Panelists also warned of the over-reliance on probabilistic clustering or opaque methodologies when using blockchain analytics tools. Daniel Leon from Europol described standardization as a "prerequisite" for building trust and effectiveness in blockchain intelligence, even rating its importance as "11 out of 10."

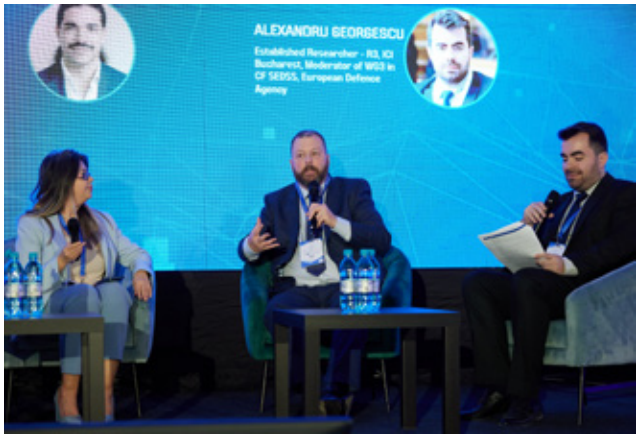
The need for harmonized standards and interoperability was a recurring focus of the panel discussion. Both INTERPOL and Europol emphasized that common definitions of clusters, wallet types, and attribution heuristics are essential to enable seamless collaboration between investigative teams and tools. The panel also discussed the limitations of current law enforcement tools, which are often inadequate for real-time blockchain investigations.

INTERPOL in particular highlighted the importance of developing features such as real-time cooperation alerts to notify investigators across different jurisdictions when they are unknowingly working on the same wallet address or entity.

Emerging challenges around smart contracts, DeFi protocols and complex multi-chain financial structures were also explored. Panelists agreed that these evolving areas require new investigative methodologies, developed in close partnership with blockchain experts from the private sector. Despite the challenges, the panel expressed optimism about the future of blockchain intelligence collaboration. They noted parallels with the early days of Malware Intelligence Sharing (MIS)—such as the development of the MIS platform—and emphasized that regulators, industry leaders, and law enforcement agencies are increasingly aligned in their goals of harmonization and knowledge sharing.

The session concluded with a strong call to action–blockchain intelligence must become an embedded, standards-driven discipline within law enforcement worldwide, transforming from a niche capability into a core pillar of modern policing.

Javier Paz, Director of Data and Analytics, **Forbes** (Moderator), **Vincent Danjean**, Head of Laboratory, **INTERPOL**, **Daniel Leon**, Cryptocurrency Specialist, **Europol EC3** (Digital Support Unit - Cyber Intelligence).



Alexandru Georgescu, Researcher, R3, ICI Bucharest (Moderator), Dr. Paul Gilmour, Senior Lecturer in Economic Crime, University of Portsmouth, Tomasso Diddi, Information Engineer, Hermes Bay, Diana Stetiu, Attorney, Sergiu Vasilescu, Founder and Managing Partner, VD Law Group, Sebastian Cochinescu, CEO, Anima Felix.

2.6 Using Blockchain Technology to Develop a Trusted and Transparent Beneficial Ownership System

How can governments implement effective registers of beneficial ownership? What technical infrastructure is needed to ensure that law-enforcement agencies, regulators, or banks and other obliged entities have lawful and proportionate, and ready access to reliable ownership data–without undermining individual privacy or data protection rights? This panel explored these questions and related issues.

Secretive tax havens cost the global economy $200 billion annually and the lack of beneficial ownership transparency undermines authorities' capacity to identify illicit activity and gather evidence to combat fraud, money laundering and tax evasion. Scandals, like the "Panama Papers" (involving over 11 million leaked documents from Panama-based law firm Mossack Fonseca) highlighted the widespread abuse of the financial system and intensified public scrutiny surrounding the transparency of corporations and their offshore business dealings.

Global transparency campaigners have justifiably been critical of strong tax avoidance schemes that benefit large multinational companies, the wealthy or political elite. Such schemes often involve concealing the real beneficial owner who ultimately owns or controls company assets. This is not necessarily the same person listed as the legal or official company owner. Therefore, transparency campaigners and governments have called for public, central registers of beneficial owners to enhance the transparency of corporate tax affairs and prevent illicit activities, like money laundering and tax evasion.

Yet, research led by Dr Paul Gilmour has identified that these registers are fraught with trust, privacy, and compliance issues, and relevant verification infrastructure is needed to check beneficial ownership data accordingly. Identifying the real beneficial owner of company assets can also prove onerous and costly for regulated businesses. Greater corporate transparency relies on an effective system involving the accurate disclosure of beneficial owners, robust verification procedures, and ongoing monitoring.

Future research should identify the characteristics of blockchain technology that would support a decentralized register of beneficial ownership, and examine how such a system might enhance accountability, trustworthiness, and transparency of beneficial ownership. Adequate technological infrastructure, resourcing and trust is essential to implementing an open beneficial ownership system.

The cryptographic process underpinning blockchain technology provides for a highly secure and immutable blockchain environment and ensures data is verified. Blockchain has the potential to support global compliance and anti-money laundering efforts through verifiable data recording. It is already supporting electronic government databases, maintaining licensing records, and even handling legally binding contractual matters. Through blockchain's consensus protocol, blockchain could facilitate the global sharing of beneficial ownership information between jurisdictions that have previously been unlikely to share records due to strict domestic secrecy laws. Moreover, a global beneficial ownership system in future will improve the use of blockchain technology as a crucial tool in the fight against financial crime.

3. Speakers' Reflections

Following a day of inspiring and insightful keynote speeches and panel discussions, the Forum gathered reflections from participating delegates, experts, and speakers.

The following insights highlight practical experiences, regional challenges and forward-looking ideas from stakeholders across the blockchain intelligence community, providing a complementary perspective on the Forum's central themes.

Alexandru Donciu, Basel Institute on Governance

Alexandru Donciu of the Basel Institute on Governance emphasized the importance of hands-on, case-based training for investigators, prosecutors, and judges working in low-regulation jurisdictions. He advocated simplifying technical concepts and ensuring all stakeholders understand the limitations and expectations of blockchain-based evidence.

Karl Zettl, CEO of Iknaio

Karl Zettl, CEO of Iknaio, described his platform as the "Google Maps of blockchain transactions," highlighting the potential of automation and open-source tools in reducing investigator workload. He advocated for a "train-the-trainer" model and warned against black-box analytics, stressing the importance of open standards, process transparency, and interoperability for credible blockchain investigations.

Dhirendra Shukla, CEO of Gray Wolf Analytics

Founder of Gray Wolf Analytics, Dhirendra Shukla spoke passionately about the need for transparent attribution models and deeper public-private collaboration. He emphasized that blockchain intelligence must be treated as a layered investigative tool, not a silver bullet and that sharing data and building trust across jurisdictions are essential to staying ahead of criminal innovation.

Dylan Cuschieri Tonna, Malta Financial Services Authority

Representing the Malta Financial Services Authority, Dylan Cuschieri Tonna outlined Malta's multi-agency approach to supervising VASPs. He highlighted the importance of regulatory adaptability, risk-based supervision, and the proactive use of analytics and outreach to stay ahead of emerging threats in the crypto-asset space.

Gabriela Alina Popescu, Blockchain Intelligence Professionals Association (BIPA)

As the community engagement manager of the professional association, Gabriela Alina underlined the importance of the Blockchain Intelligence Forum as a soft diplomacy initiative for advancing serious discussions about standards and interoperability. On a practical note, current dynamics of Blockchain intelligence require a framework for open discussions across jurisdictions, involving professionals from different sectors, with a long term view to clarify the potential operational implications for traditional financial institutions and new market players.

Professor Andrea Minto, University of Venice

Andrea Minto, Professor of Law at the University of Venice, spoke about the urgent need to address supervisory fragmentation in the European Union and beyond. He stressed the importance of multidisciplinary training for future blockchain intelligence professionals, combining legal, financial, and data science literacy to ensure institutions and businesses can keep pace with rapidly evolving technology.

Diana Patrut, Blockchain Intelligence Professionals Association (BIPA)

As Project Manager for the first ever EU professional initiative to set standards for the Blockchain Analyst occupation, Diana underlined the importance of blockchain intelligence to combat illicit finance, and its ability to generate added-value output for better decision-making, especially when combined with traditional intelligence techniques. However, true value emerges when blockchain data is interoperable and integration across platforms enables comprehensive analysis. Interoperability is a strategic necessity for effective operations, intelligence-led investigation and supervision.

Heinz Konzett, Office for Digital Innovation of Liechtenstein

Heinz Konzett from Landesverwaltung Liechtenstein highlighted that the European MiCA is a crucial and necessary step for harmonizing crypto-asset regulation in Europe. But financial market regulation only works properly if the legal foundation is also settled. In Liechtenstein, the TVTG law provides that foundation – the defined Token Container Model ensures that any token, whether a payment token or a tokenized commodity, is legally defined, transferable and enforceable. That makes MiCA not just a regulation, but a practical tool within the financial system.

Dr. Joseph Lee, University of Manchester

Dr. Joseph Lee, University of Manchester law professor and legal adviser, stressed that investor protection is foundational to sustainable financial markets. While praising the MiCA Regulation as a major step forward, he cautioned that critical gaps remain, particularly in relation to DeFi and legal clarity and urged collaboration between regulators, academia, and the financial sector to build shared understanding and confidence.

Maksym Dragunov, Crystal Intelligence

Maksym Dragunov, Director of Policy at Crystal Intelligence, outlined the rising prominence of sanctions enforcement in blockchain intelligence. He emphasized the need to connect on-chain behavior with off-chain events and noted that attribution and evidence-building must be clear, defensible, and grounded in rigorous methodology to hold up in court.

Marian Müller, Caudena

Marian Müller, Head of Education at Caudena, discussed the evolution of blockchain crime typologies and the shift from cluster-based approaches to deeper intelligence rooted in raw blockchain data. He highlighted Caudena's focus on advanced law enforcement training and stressed the importance of understanding blockchain technology at a fundamental level to avoid misinterpretation and improve evidentiary reliability.

Marina Khaustova, Crystal Intelligence

COO of Crystal Intelligence, Marina Khaustova explored the balance between innovation, compliance and traceability. She stressed the urgency of solving cross-border data-sharing barriers, praised zero-knowledge protocols as an unexpected investigative asset, and issued a firm call to integrate AI into compliance efforts, warning that "you cannot fight AI-enabled crime with yesterday's tools."

Mico Curatolo, Banca Sella

Mico Curatolo, Digital Assets Lead at Banca Sella, explained how his team sits at the intersection of business, regulation, and technology. He emphasized the foundational role of custody in tokenized finance and called for cultural and technical investment within banks to prepare for MiCA implementation, cross-border blockchain integration, and e-money tokenization.

Oleksii Geyko, National Anti-Corruption Bureau of Ukraine

Detective Oleksii Geyko from Ukraine's National Anti-Corruption Bureau outlined the dual pressures of fast-evolving crypto-asset technologies and slow-moving national legislation. He emphasized the urgent need for formal regulation, international cooperation and upskilling law enforcement to keep pace with crypto-savvy actors, particularly in a country where blockchain use is widespread and often unregulated due to ongoing conflict.

Nate Tuganov, Caudena

Nate Tuganov, CEO of Caudena, discussed the shift from single-chain analytics to tracing across multi-chain bridges and stablecoins. He stressed that AI models are already transforming investigation workflows, enabling pattern discovery and automation, but made clear that human interpretation remains critical, especially when dealing with the noise and ambiguity inherent in complex transaction graphs.

Maha Al-Saadi, Qatar Financial Centre

Maha, the Head of Regulatory Affairs for Qatar Financial Centre noted how multifunction crypto intermediaries (MCIs) pose significant systemic risks to the financial system, often greater than the risks posed by current financial institutions because MCIs own the entire value chain. MCI's promise of access to instant liquidity, can very rapidly lead to financial and systemic instability. She recognized the key bridging role stablecoins play between traditional finance and web3, and how it is important for regulators and policymakers to understand both the challenges and opportunities.

Peter Engering, ComplianceChamps

Peter Engering, CEO of ComplianceChamps, reflected on his early efforts to craft crypto-asset policy in Dutch banking. He described the cultural and regulatory resistance he encountered and emphasized that most AML tools remain unprepared for crypto-asset complexity. He called for pragmatic regulators, better education, and a compliance culture that sees crypto-assets not as a threat, but as a new financial reality.

Sundri Khalsa, PaperBallotChain

CEO of PaperBallotChain and a U.S. Marine Corps veteran, Sundri Khalsa discussed how blockchain innovation must blend decisiveness with resilience. She proposed a hybrid voting system combining paper ballots and blockchain to preserve both transparency and voter anonymity, offering a novel solution to long-standing vulnerabilities in digital democracy.

Severin Kranz, 21X

Severin Kranz, co-founder of 21X, shared his experience launching a fully regulated on-chain trading venue. He identified education, not regulation or technology, as the main barrier to adoption and stressed the need for financial institutions to rethink internal workflows. He also outlined the firm's success in obtaining 17 regulatory exemptions, allowing for real-time securities settlement via stablecoins and CBDCs on public blockchains.

Thomas Droll, Deutsche Bundesbank

Thomas Droll from Deutsche Bundesbank highlighted the legal uncertainty surrounding tokenized securities in the EU and stressed the need for a Digital Capital Markets Union to create a level playing field. He emphasized that central banks must support the ecosystem by advancing wholesale CBDCs and integrating DLT securities into mainstream financial operations, while working closely with the EU Commission to harmonize regulatory frameworks.

Yehuda Shaffer, Former Head of Israel's Financial Intelligence Unit

Former Head of Israel's Financial Intelligence Unit, Yehuda Shaffer offered a balanced view of blockchain analysis tools, noting both their strengths and their limitations. He stressed that while they are useful for identifying trends and typologies, real impact comes only when paired with off-chain data and specialist training. He advocated for broader interoperability, better legal frameworks and targeted capacity building across FIUs, police, prosecutors, and judges.

SPECIAL CONTRIBUTIONS

Blockchain Intelligence as a Data Science Task

Javier Paz

Director for Data and Analytics, Forbes

Director of Data and Analytics at Forbes, Javier is a seasoned blockchain intelligence analyst. An expert in blockchain transaction data, Javier has personally overseen some of the world's largest crypto-asset investigations for Forbes. He has uncovered some of the industry's biggest frauds and traced billions of dollars' worth of illicit crypto-asset flows used by terrorist organizations and rogue states.

Javier was also the first to pioneer a crypto-asset exchange ranking system for Forbes, allowing investors to make informed decisions on counterparties and trading venues.

Known for his investigative acumen, Javier was graced the inaugural Blockchain Intelligence Forum not only with his presence, but with his contribution to the event by moderating multiple panels, and hosting insightful fireside chats with the CEOs of top blockchain intelligence firms, as well as leaders from law enforcement's premier global agencies Europol and INTERPOL.

"We need to recognize blockchain intelligence for what it is - a data science task that needs a data science approach. Only then can we extract meaningful insight from pseudonymous blockchain transaction data."

Javier Paz

The Urgent Need for Standards for Blockchain Intelligence

Patrick Tan
General Counsel, ChainArgos

A recent slew of civil and criminal cases have highlighted the limitations and risks when admitting blockchain tracing as evidence in court. Victims have been unable to recover their misappropriated crypto-assets, even while potentially innocent defendants are convicted on the back of questionable blockchain tracing "evidence." There is an urgent need to shift blockchain tracing from pseudo science to data science, and into the realm of blockchain intelligence:

Transparent Methods

Stakeholders deserve to understand blockchain tracing methodologies and attribution techniques before such analysis should be admissible in court, instead of relying on "black boxes."

Establish standards

Blockchain meta data, such as wallet address labels, and the taxonomies of such labels needs to be standardized to enable cross-border analysis and co-operation between law enforcement agencies.

Rigorous Testing Required

Current blockchain tracing methods and wallet attribution have not been subject to any testing and what limited testing has been performed has typically omitted false positives and/or false negatives when convenient. Blockchain tracing needs to be recognized as a data science task and treated accordingly, subjecting it to rigorous empirical analysis.

As crypto-assets, stablecoins, and tokenized assets continue to grow, the blockchain tracing industry needs to develop as well to provide independently verifiable and reproducible outcomes in order to add value, or risk being irrelevant.

Better Information-Sharing Networks for Better Blockchain Intelligence

Luke Wilson
Global Head of Public Sector, Allium

There is a growing demand from public sector stakeholders for blockchain transaction data solutions that provide them with the versatility to develop their own unique and mission-specific solutions, that are interoperable between agencies.

While not every public sector agency will have the necessary resources to develop their own solutions individually, regulatory overlap, especially with the growth of tokenized assets and stablecoins, will require a holistic effort to tackle an otherwise intractable torrent of blockchain transaction data that grows exponentially every day.

There is a need for better information-sharing frameworks not just between public sector agencies, but also between the public and private sectors, to exchange best practices, jointly develop appropriate blockchain data frameworks, and build effective blockchain intelligence applications.

The sheer volume and rate of growth in blockchain transaction data means that AI will eventually become indispensable in simplifying complex multi-chain investigations while reinforcing the indispensable role of human judgment.

Because the same crypto-asset can exist and be hypothecated across multiple blockchains, it's important for stakeholders to be able to perform analysis instantaneously across multiple blockchains.

This is why forums such as the Blockchain Intelligence Forum are so critical as they provide a venue for such discourse. The interoperability of blockchain transaction data, and the development of open standards and frameworks are key steps for the continued development of blockchain intelligence.

Towards a Data-Driven Blockchain Intelligence Future

Bernhard Haslhofer

Co-Founder Iknaio and CryptoFinance Research Group Lead at the Complexity Science Hub, Vienna

Current blockchain intelligence practices will not scale with the growing data volume and complexity. A more data-driven approach is needed. Key steps include:

Raise awareness

Technical experts understand that data availability is crucial for effective investigations. The same awareness must be built among decision-makers. Just as modern astronomy moved beyond manual telescopes, blockchain intelligence requires advanced data tools to explore this new financial universe.

Establish standards

Interoperability standards, file formats, data-sharing protocols, and contractual frameworks—are essential for a maturing field. These are common in other domains and urgently needed here.

Develop computational methods

We need scalable, transparent, and verifiable methods to extract insights from large datasets. Openness, as seen in digital forensics, drives broader innovation and trust.

Generalize knowledge

Blockchain intelligence is a collection of methods, not a tool. Training should focus on underlying principles, enabling professionals to adapt across platforms. Also this is standard practice in more mature fields.

These steps will emerge naturally as the field matures, but it's critical to begin moving in this direction now.

The Importance of Interoperability in Blockchain Analytics

Tamar Latsabidze

Chief Specialist, Division of Inspection and Supervision of Payment Service Providers and Virtual Asset Service Providers, Money Laundering Inspection and Supervision Department, National Bank of Georgia

Blockchain technology is driving a paradigm shift in AML/CFT supervision. While core AML/CFT principles remain technology-agnostic, the tools and methods for monitoring financial crime risks are rapidly evolving to address the unique characteristics of the blockchain ecosystem. Unlike traditional finance (TradFi), transactions on public blockchains are transparent and publicly traceable, yet also pseudo-anonymous. This nature presents both new opportunities and significant challenges for effective oversight.

Blockchain analytics tools play a critical role in this space by helping to navigate the pseudo-anonymous environment. These tools identify suspicious patterns, map transaction flows, and link wallet addresses to known actors. Their capabilities are increasingly supporting regulators, law enforcement agencies, and Crypto Asset Service Providers in understanding and responding to risks in this dynamic and fast-evolving ecosystem.

As blockchain analytics tools gain wider adoption, stakeholders across the ecosystem are engaging in more thoughtful and forward-looking dialogue: What features are essential to support compliance, supervision, and investigations? How can we explain the differing risk ratings or attributions assigned to the same wallets across different tools? To what extent can these outputs be verified or used as evidence in regulatory or legal contexts? And how can we enable consistent, effective information-sharing among stakeholders using different analytics platforms?

Selecting between blockchain analytics tools in the absence of widely accepted standards or benchmarks is like choosing from a set of maps—each offering valuable insights, yet portraying the same landscape in different ways. Without a common framework, making informed decisions becomes more complex.

DISCLAIMER: The views expressed herein are those of the author in a personal capacity and do not necessarily reflect the official position or opinion of any affiliated institutions or organisations.

EMERGING THEMES

Several cross-cutting themes emerged that captured the collective priorities of the Forum's stakeholders.

Senior figures such as Nico Di Gabriele, Patrick Tan and Bernhard Haslhofer underscored the urgent need for blockchain intelligence to evolve into a fully professionalized, standards-driven discipline.

Other contributors, including law enforcement leaders like Vincent Danjean and Dr. Victor Vevera, reinforced the call for enhanced collaboration between investigative agencies, regulators and blockchain analytics providers.

The following thematic sections distil these strategic insights, offering a forward-looking vision for advancing blockchain intelligence on the global stage.

The Future of Blockchain Intelligence Training and Professionalization

One of the dominant themes emerging from the Blockchain Intelligence Forum 2025 was the urgent need to formalize blockchain intelligence as a professional discipline, supported by recognized training pathways, certification standards, and ethical frameworks.

Blockchain intelligence today relies primarily on a small cohort of specialists with diverse, self-taught skills, or commercially provided training programs with inconsistent standards.

This informal structure cannot scale to meet the growing demand from law enforcement, regulators, financial institutions, and private sector compliance teams.

Without structured education and professionalization for blockchain intelligence, critical gaps in investigative capabilities, analytical rigor and ethical integrity will persist.

Speakers and panelists highlighted several key priorities for the professionalization of blockchain intelligence, including the need to define core competencies, develop structured training programs, build ethical standards, and create career pathways and institutional support frameworks.

Defining Core Competencies

Blockchain intelligence professionals must possess a blend of:

- Technical literacy (blockchain protocols, crypto-assets, DeFi structures)
- Investigative skills (evidence preservation, attribution, forensic tracing)
- Financial crime expertise (AML/CFT, sanctions compliance, fraud typologies)
- Ethical governance awareness (data privacy, proportionality, legal admissibility)

Developing Structured Training Programs

Broad consensus was established that training should be:

- Multidisciplinary, combining legal, financial, technological, and investigative modules.
- Practical and skills-based, not just theoretical.
- Internationally benchmarked, drawing on best practices from fields like anti-fraud, cybersecurity, and financial intelligence.

Several panelists referenced the success of models like the Certified Fraud Examiner (CFE) and Certified Anti-Money Laundering Specialist (CAMS) frameworks, suggesting that blockchain intelligence should follow a similarly structured and globally recognized path to professionalization.

Building Ethical Standards

Blockchain intelligence operates at the intersection of privacy, security, and enforcement. Therefore, ethical codes and professional standards must be embedded into training and practice, covering issues such as:

- Responsible attribution of identities
- Safeguarding privacy rights
- Avoiding data manipulation or investigative overreach
- Ensuring reproducibility and integrity of evidence

Creating Career Pathways and Institutional Support

Government agencies, financial institutions and major analytics providers must work together to:

- Recognize blockchain intelligence as a distinct professional domain.
- Offer clear career pathways, specializations, and leadership opportunities.
- Fund scholarships, training programs, and research initiatives to grow the talent pool.

A major initiative launched during the Forum to support this professionalization effort was the Blockchain Improvement Pledge, inviting blockchain analytics providers and stakeholders to commit to building transparent, interoperable and ethically-governed blockchain intelligence practices.

The message from the Forum was clear - blockchain intelligence must evolve from an emerging skill into a recognized global profession, with the standards, training, and credibility needed to protect financial systems, public safety and digital innovation.

ENHANCING BLOCKCHAIN

Compliance, Enforcement, and Interoperability

Blockchain's decentralized nature offers unique challenges and opportunities for financial crime prevention, regulatory supervision and law enforcement operations.

Speakers and panelists at the Blockchain Intelligence Forum 2025 stressed that building strong compliance and enforcement capabilities requires addressing both technological and institutional gaps.

While blockchain transparency can support traceability, fragmented regulatory frameworks, inconsistent compliance standards and lack of data interoperability continue to undermine investigations, and risk management efforts.

Four critical areas for enhancement emerged clearly from the Forum discussions:

1. Integrating Blockchain Intelligence into Compliance Systems

Financial institutions, crypto-asset service providers and Multifunction Crypto Intermediaries (MCIs) must:

- Embed blockchain analytics tools into their transaction monitoring systems.
- Adopt dynamic risk scoring models that account for DeFi exposure, privacy coin usage and cross-chain activity.
- Align internal compliance frameworks with FATF Travel Rule requirements and evolving EU MiCA regulations.

This integration must be proactive and predictive, enabling early detection of suspicious transaction patterns rather than relying solely on post-incident investigations.

2. Accelerating Cross-Border Enforcement Cooperation

Panelists consistently stressed that crypto-asset-related investigations require real-time intelligence sharing.

National jurisdiction barriers can delay asset freezing or seizure by hours, often enough for illicit funds to move beyond recovery.

Key proposals included:

- Creating secure, interoperable data exchange platforms between law enforcement agencies and regulators.
- Establishing rapid attribution protocols to link on-chain activity to real-world identities across borders
- Harmonizing evidential standards to facilitate cross-jurisdictional prosecutions.

3. Standardizing Data Attribution and Blockchain Analytics Practices

Today's blockchain analytics industry suffers from inconsistent attribution methodologies, with providers applying different heuristics, labels, and thresholds.

The Forum highlighted the need for:

- Open-source standards for address attribution and metadata tagging.
- Voluntary alignment initiatives, such as the Blockchain Intelligence Improvement Pledge, to encourage the establishment and adoption of best practices among blockchain analytics providers.
- Third-party validation and certification of blockchain intelligence methodologies.

Without these steps, blockchain intelligence risks remaining fragmented and difficult to integrate into legal and compliance systems.

4. Balancing Automation and Human Oversight

Automation and machine learning are essential to scale blockchain intelligence, particularly given the complexity and speed of on-chain activity.

However, several speakers stressed that human oversight remains critical, particularly for:

- Validating automated findings.
- Ensuring explainability and reproducibility in investigative reports.
- Maintaining the chain of custody for judicial admissibility.

Regulators and law enforcement agencies must invest in hybrid systems that combine automated pattern detection with rigorous human analysis.

The Blockchain Intelligence Forum 2025 clearly demonstrated that the future of effective compliance and enforcement lies not just in better tools, but in better cooperation, better standards, and better training.

Building scalable, interoperable and ethically sound blockchain intelligence infrastructures is now a global imperative.

Both Patrick Tan of ChainArgos, and Bernhard Haslhofer of Iknaio reinforced the need for blockchain intelligence to evolve beyond fragmented, proprietary solutions calling for the professionalization of the field through open standards, scientifically validated methodologies. and transparent attribution practices. Their perspectives underscored the critical importance of embedding interoperability and evidential integrity at the core of blockchain training, compliance and investigative practices.

CONCLUSIONS

Strategic Recommendations

The Blockchain Intelligence Forum 2025 set a clear vision for the future of blockchain intelligence. A future where technological innovation is matched by professional discipline, international cooperation, ethical governance, and proactive enforcement capabilities.

Across keynote speeches, panel discussions and informal exchanges, a consistent message emerged that blockchain intelligence is no longer a peripheral skill, it is a critical pillar for safeguarding global financial systems, public trust and digital innovation. The Forum recognized that while challenges remain–fragmentation, skills shortages, cross-border complexities–there is now an extraordinary opportunity to build a harmonized, professional, and resilient blockchain intelligence ecosystem.

Based on the key insights and discussions, the following strategic recommendations have been proposed:

1. Accelerate the Professionalization of Blockchain Intelligence

- Establish recognized training and certification frameworks.
- Define core competencies blending technical, financial, investigative and ethical skills.
- Embed blockchain intelligence career pathways within government, regulatory, and private sector institutions.

2. Foster Standards for Data Attribution, Analytics and Compliance

- Promote voluntary industry alignment through initiatives such as the Blockchain Intelligence Improvement Pledge.
- Develop open-source standards for blockchain address labelling, forensic methodologies and interoperability protocols.
- Ensure analytics models meet explainability and judicial admissibility thresholds.

3. Build International Intelligence Cooperation Networks

- Invest in real-time, cross-border blockchain intelligence data sharing platforms.
- Harmonize evidential standards to support asset recovery and prosecutions across jurisdictions.
- Encourage multi-stakeholder collaboration between regulators, law enforcement, financial institutions and analytics providers.

4. Balance Technological Innovation with Ethical Oversight

- Balance Technological Innovation with Ethical Oversight
- Support the integration of AI and automation in blockchain intelligence but maintain strong human oversight.
- Uphold principles of privacy, proportionality and evidential integrity in all blockchain intelligence activities.
- Build public confidence through transparent governance structures.

The future of blockchain intelligence is being written now.

The Forum has issued a clear call to action for supervisory authorities and blockchain intelligence providers to collaborate in upcoming interoperability projects, standard-setting initiatives, and the advancement of formal professional recognition for blockchain analysts. This collaboration is central to ensuring that blockchain intelligence evolves into a trusted, global discipline.

The Blockchain Intelligence Forum 2025 was not just a milestone event, it was a catalyst for collective action. The momentum generated in Bucharest must now translate into sustained investment, policy innovation and professional leadership.

It is our shared responsibility to ensure that blockchain intelligence is built on the foundations of skill, integrity, cooperation, and impact.

The Forum made clear that blockchain intelligence is maturing into a professional, standards-driven global practice, a discipline essential to the resilience of future financial systems, and the credibility of digital innovation. Blockchain intelligence is not merely a forensic necessity, it is an integral part of the future financial and regulatory infrastructure.

The Forum's central messages – including the need for global standards, transparency, and rigorously-tested blockchain intelligence – have already been amplified in international media, notably in the recent opinion article in Financial Times: Banking Risk & Regulation by ICI Bucharest's General Director, Dr. Victor Vevera. However, awareness is only the first step, and what comes next is even more critical.

Beyond the recognition of the problem, measures are already in place to pursue the goals of the Forum, from the drafting of the Blockchain Intelligence Improvement Pledge to the formation of the Working Group to establish the role of the blockchain analyst as a recognized occupation in the European Union.

No doubt the Forum is a significant milestone, but perhaps only the first step in a journey to improve and elevate the level of discourse for blockchain intelligence.

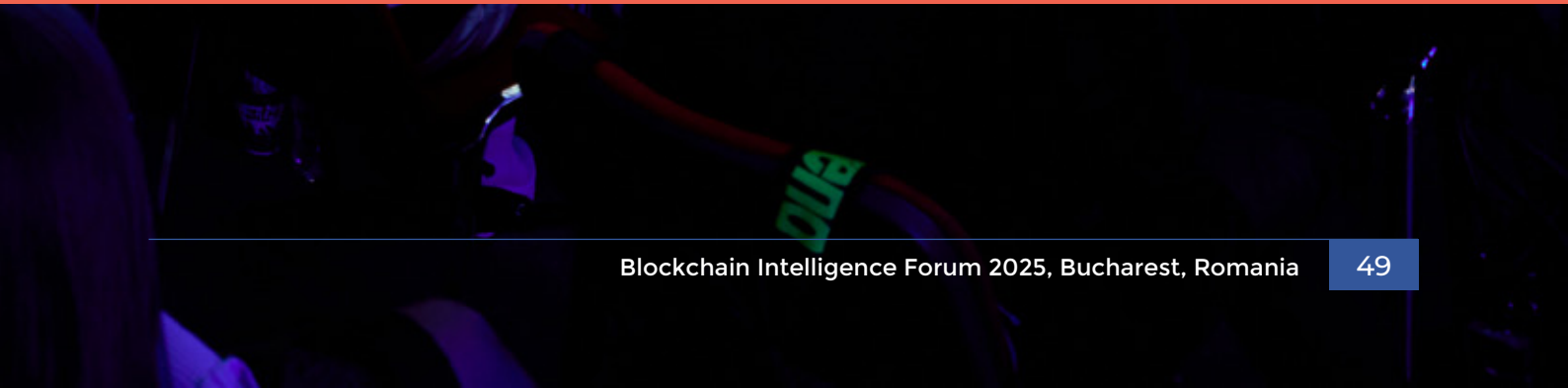
Looking Ahead

Building on the success of the 2025 Forum, ICI Bucharest, BIPA, and international partners remain committed to advancing the professionalization of blockchain intelligence. Plans are already underway to expand collaboration, refine global standards, and deepen engagement across the enforcement and compliance community.

The Forum's momentum will continue to drive meaningful progress, laying the groundwork for future gatherings that strengthen international cooperation and the collective fight against financial crime.

HOW CAN YOU CONTRIBUTE?
TAKE UP THE CALL TO ACTION.

The strategic recommendations from the Forum are intended to reach far beyond the confines of Bucharest's Palace of the Parliament. Stakeholders and interested individuals can still contribute to ensure the strategic mission of the Forum endures.



Take up the call.

Join the Blockchain Data Interoperability Project ("BDIP")

Ambitious but achievable, in collaboration between public and private sector partners, the BDIP will propose industry guidelines for the standardization of blockchain data, including, but not limited to, the methodologies for attribution of wallet addresses, and the nomenclature of such labels, in collaboration with both private and public sector partners.

The BDIP will seek to standardize all aspects of blockchain transaction data and identifiable meta data that can be attached to otherwise anonymous blockchain addresses, to facilitate the use of standardized datasets by both public and private sector stakeholders.

Following the example of the development of Unicode, which arose from the need for a universal comprehensive character encoding system for programming that could handle all languages and symbols, the BDIP will be a collaborative effort, that allows the maximum value to be extracted from otherwise pseudonymous blockchain transactions.

Stakeholders and contributors are requested to join the BDIP by reaching out via email to:

contact@blockchaintelligence.com

Join the Working Group for ESCO Recognition of the Blockchain Analyst Profession

Measures have already been initiated to support the official recognition of the role of the blockchain analyst by the European Skills, Competences, Qualifications and Occupations (ESCO). The ESCO helps make the European labor market more effective an integrated, by identifying, articulating, and classifying professional occupations and skills relevant for the EU labor market.

The practice of blockchain intelligence has evolved organically to become a disjointed, poorly defined, and piecemeal discipline, without common skillsets, training standards, or accreditation.

A Working Group is being formed to ensure the input of both public and private sector stakeholders, to contribute to coherent and consistent definitions for the role of a blockchain analyst, under the auspices of the ESCO.

Official recognition of the blockchain analyst profession by the ESCO will significantly raise the level of professionalism, improve hiring prospects, and ensure recognition of competent and skilled blockchain intelligence professionals.

Stakeholders and contributors are requested to join the ESCO Working Group by reaching out via email to:

contact@blockchaintelligence.com

Engage with the Blockchain Intelligence Academy

Born out of the landmark public-private partnership between the blockchain intelligence firm ChainArgos and the National Institute for Research & Development in Informatics – ICI Bucharest, the Blockchain Intelligence Academy (BIA) has as its foundational mission to deliver training in service of the truth.

As blockchain transactions have exploded in volume, a cottage industry to support the interpretation of otherwise pseudonymous transaction data has risen in its wake.

Most blockchain intelligence training programs are based on commercially derived solutions, with private accreditation and certification, and with little scrutiny over the quality of the syllabus, or the accuracy of attribution, let alone the integrity of methodologies.

The BIA was created to provide transparency for training, methodologies, and limitations of blockchain intelligence, to provide training in service of the truth. Trainees are taught not just the practical skills of dissecting blockchain transactions, but the inherent limitations to interpreting such data.

Critically, trainees develop critical thinking skills enabling them to ask better quality questions when interpreting blockchain transaction data, and identifying the gaps that need to be filled to develop comprehensive and defensible analysis.

For more information about the BIA and its training programs, please reach out via email to:

contact@bi.academy

Join the Blockchain Intelligence Professionals Association (BIPA)

The Blockchain Intelligence Professionals Association (BIPA) is a global body for certified blockchain intelligence professionals from both the public and private sectors.

Headquartered in Bucharest, Romania, BIPA members seek to:

- Develop a community of Blockchain Intelligence Professionals
- Promote Blockchain Intelligence awareness
- Facilitate open discussion and sharing of best practices to reduce the use of blockchain technology for illicit activity

BIPA organizes and hosts quarterly, invite-only workshops, providing members an opportunity to engage and share industry best practices and the latest developments in blockchain intelligence with high-level delegates and experts from government agencies, law enforcement, financial institutions, blockchain intelligence firms and front-line practitioners with hands-on experience.

BIPA co-hosts the annual Blockchain Intelligence Forum (BIF) with ICI Bucharest, during the Digital Innovation Summit Bucharest. BIPA members are invited to speak and participate in the BIF.

To express interest in becoming a BIPA member, please reach out via email to:

contact@blockchaintelligence.com

Build Skills in Crypto and Financial Crime Investigations with the Basel Institute on Governance

Two decades of hands-on training in countering financial crime, tailored for law enforcement and policymakers

A key takeaway from the Blockchain Intelligence Forum was the urgent need for sustained, effective capacity building to counter crypto-enabled crime. Not just tool-specific instruction, but comprehensive training based on common standards. Training that helps actors across sectors understand the technologies, risks and roles involved.

For over 20 years, the Basel Institute on Governance and its International Centre for Asset Recovery have supported law enforcement and other public institutions with hands-on training and mentoring in financial investigations, asset recovery and related fields. Increasingly, we also support private-sector and civil society partners.

What sets our training approach apart is its emphasis on practical skills and real-life cases and challenges. Participants don't just study theories and investigative methods, they apply them directly in simulated case scenarios. Cases are tailored to national or sector contexts, such as environmental crime or crypto money laundering schemes.

This gives participants the chance to "follow the money" by tracing funds, gathering and analyzing evidence – including from blockchains – and cooperating with counterparts across agencies and borders.

Current Learning Opportunities

Basel LEARN – Free eLearning and More

- **Free, self-paced online courses** for law enforcement, anti-money laundering and compliance professionals, focused on practical skills for tackling financial crime and corruption.
- **Topics** include open-source intelligence, financial analysis, international cooperation and combating terrorism financing. A virtual assets course is coming soon.
- **Interactive, scenario-based modules** help users "learn by doing" through simulated investigations and real-world case exercises

To get started, go to:

learn.baselgovernance.org

Training for Public Agencies

- **Tailored, case-focused training** for law enforcement, prosecutors and other public officials, focused on investigating financial crime and recovering illicit assets.
- **Topics include financial investigations,** international cooperation, illicit enrichment and non-conviction based forfeiture.
- **Most courses include a crypto module,** although a dedicated course is also available on blockchain intelligence and crypto-asset tracing
- **Train-the-trainer programs** help expand capacity building by certifying local practitioners to train their peers.

To get started, go to:

baselgovernance.org/asset-recovery/training-programmes

Introduction to blockchain: Crypto investigation and AML compliance

- **An online, trainer-led course** introducing blockchain, crypto-assets and AML compliance, with a strong focus on practical investigation of illicit crypto flows.
- **Combines theory with a hands-on money laundering case scenario,** helping participants trace transactions and assess compliance risks in real time.
- **Designed for a wide audience** including law enforcement, compliance professionals, regulators, journalists and legal practitioners.
- **Delivered live by expert instructors** through video conferencing over four days, with three hours per day.

To get started, go to:

baselgovernance.org/crypto-aml-training

Basel STUDY: Postgraduate Courses for Professionals

- **Six-month postgraduate courses** combining academic expertise from the University of Basel with the Basel Institute's practical experience in anti-corruption and financial crime.
- **Designed for working professionals,** with live virtual seminars and optional in-person sessions in Basel.
- **Courses launching in 2025/26** include Mastering Today's Anti-Corruption Challenges and Combating Financial Crime Through Asset recovery.
- **Ideal for early-career professionals,** career changers or practitioners seeking a deeper understanding of anti-corruption and asset recovery, including crypto.

To get started, go to:

baselgovernance.org/study

Join the Project to Build a Beneficial Owners Registry Using Blockchain Technology

Dr. Paul Gilmour of the University of Portsmouth is leading a proof-of-concept project, in collaboration with ICI Bucharest, to explore the use of blockchain technology in addressing the challenges of complex beneficial ownership.

This project will develop how blockchain technology will support accurate, verifiable, and open records of beneficial ownership information through relevant stakeholder engagement.

Many international governments and anti-money laundering bodies call for public, central registers of beneficial owners towards strengthening corporate transparency, with the aim of preventing criminals concealing illicit wealth through obscuring the real beneficial owner behind companies used to launder money and evade taxes.

Yet, research has identified that these registers are fraught with trust, privacy, compliance and legal issues and relevant verification infrastructure is needed to check beneficial ownership data accordingly. This project will provide a better understanding for governments, regulators and businesses towards building a more trusted, transparent and effective beneficial ownership system.

The Project aims to develop a framework for the disclosure of beneficial owners that will drive future improvements in blockchain application and impact on government policy, anti-money laundering regulations, and related law.

The Project seeks your views and insight in the following areas:

- The disclosure of beneficial ownership.
- The technological, social and legal challenges in implementing a decentralised register of beneficial owners based on blockchain.
- What these insights mean for business, governments, regulators, law enforcement and wider society.
- How such a system work in practice. How to adopt the technical infrastructure, mitigate concerns around trust, data privacy, sharing of information and verification and compliance issues.
- Establishing a clear pathway to a future more global beneficial ownership system being implemented.

Dr. Paul Gilmour is a Senior Lecturer in Economic Crime, course leader of the MSc Economic Crime (campus) degree, and lead of the Economic Crime Research Group at the University of Portsmouth. Prior to this, he served for nearly 20 years in the UK police service, most recently, as a detective specialising in criminal investigations. He serves as Editor-in-Chief of the Journal of Financial Crime and Journal of Money Laundering Control.

We are inviting interested stakeholders, from government, business, technology, and the regulated sectors, to be involved in this project to contact Dr. Paul Gilmour at:

paul.gilmour@port.ac.uk

Engage with the Blockchain Intelligence Centre of Excellence - Education Partnership

We are inviting interested stakeholders from government, law enforcement, industry and the private sectors, along with interested students, to contribute ideas on the strategic direction of the new Blockchain Intelligence Centre of Excellence (BICE).

The University of Portsmouth is proud to have partnered with the ICI Bucharest and ChainArgos (the Blockchain Intelligence Academy) in creating the BICE towards professionalizing the blockchain intelligence field.

We seek your views on:

- The role of blockchain intelligence in investigating and prosecuting cybercrimes and economic crimes.
- The needs of your industry, organisation, or sector towards the BICE delivering relevant professional certification and forensic training programmes on the use of blockchain intelligence.
- How to best equip students with the skills needed to meet employer demand for expertise in tracing illicit crypto payments and combatting cybercrimes and economic crimes.
- The establishment of global standards for admissible evidence reliant on blockchain intelligence.
- Supporting research in blockchain technology whilst strengthening the impact on international policy and practice.

With a large student market in criminology, this partnership is a great opportunity for the BICE to provide academic expertise and ensure blockchain intelligence training is delivered effectively to a global audience of students.

Blockchain technology is decentralised and borderless. However, law enforcement agencies are sitting in silos in their respective jurisdictions, left to face the onslaught of economic crime wrought by permissionless, pseudonymous transactions facilitated by blockchain.

It is hoped that the BICE can provide a safe space for global cooperation and collaboration between law-enforcement agencies, and former students of the BICE, who would have developed their openness and camaraderie as a result of their shared learning experience.

We are inviting interested stakeholders, from government, law enforcement, industry and the private sectors, along with interested students, to contribute ideas on the strategic direction of the new Blockchain Intelligence Centre of Excellence (BICE) to contact Dr. Paul Gilmour at:

paul.gilmour@port.ac.uk

Join the Blockchain Intelligence Forum (BIF) 2026

The second edition of the BIF will focus on both sharing and scaling best practices in regulation, authorisation, supervision and investigation across jurisdictions. The 2025 Forum crystallised the need for harmonised standards. 2026 must demonstrate how those standards translate into day-to-day operations, to move from conceptual alignment to operational excellence.

The second edition of the BIF will focus on operationalizing the standards needed for blockchain intelligence to become a mature, widely-accepted profession.

Working Themes:

- From standards to best practice: embedding blockchain intelligence in global finance & security;
- Operationalising blockchain intelligence: best practices for regulation, supervision & investigation;
- Towards professionalization: setting standards for investigations, organizations and qualifications.

Objectives:

- To present data interoperability standards and drive their adoption;
- To showcase different proven frameworks for licensing, supervision, compliance & transaction monitoring, data sharing & investigative cooperation;
- To benchmark both tools and methodologies against real world case studies in order to highlight both gaps and lessons learned;
- To expand professionalisation efforts by unveiling a draft EU level qualification standard for “Blockchain analyst” profession.

Tracks:

- **Data and interoperability:** data formats, taxonomies, data exchange protocols
- **Regulation and Policy Harmonisation:** MiCA implementation, Travel Rule alignment, DeFi and staking policy, and other related policy considerations
- **Authorisation and Licensing:** risk-based fit and proper models, prudential requirements, whistleblower channels
- **Supervision and Compliance:** on-chain liquidity risk, real-time market abuse detection
- **Investigation and Enforcement:** cross-chain tracing, asset recovery playbooks, evidential standards for AI driven analytics

Special Track (Academic):

Global universities still offer limited, if any, formal education in blockchain technology and blockchain transaction data analysis, forcing most students and professionals to pick-up their knowledge from social media, short online courses, or blockchain intelligence service providers.

The BIF's 2026 Academic Track will bring together lecturers, researchers and training designers to bridge the blockchain intelligence skills and capabilities gap, developing independently-verifiable blockchain intelligence training and education of the highest standards. Together, stakeholders will draft a hands-on curriculum that blends the basics of blockchain tech with real-world crime-fighting cases, finance rules, and legal know-how. They'll also outline clear job profiles, such as a "Blockchain Analyst" profession and create fair ways to test skills and ethics.

Target Participants: Regulators and Policymakers , Financial Supervisory Authorities and Central Banks, Law Enforcement, Market Crypto Intermediaries and TradFi institutions, Academia and Standards Bodies.

We are inviting interested stakeholders, from government, business, technology and the regulatory sectors to be involved in the Blockchain Intelligence Forum 2026 by reaching out via email to:

contact@blockchaintelligence.com

Upcoming Events

Building on the momentum of the Blockchain Intelligence Forum in 2025, the Blockchain Intelligence Professionals Association (BIPA) will be organizing workshops throughout the rest of 2025 and into early 2026 before the next edition of the Blockchain Intelligence Forum.

Rethinking Transaction Monitoring

BIPA Workshop in Vienna, Austria on 27 November 2025

The Blockchain Intelligence Professionals Association (BIPA) will be organizing a workshop "Rethinking Transaction Monitoring" on 27 November 2025, in Vienna, Austria.

While Crypto-Assets Service Providers (CASPs) appear to be the firms dealing most directly with crypto-assets, financial institutions and other intermediaries may unwittingly be exposed to crypto-assets and stablecoins through their customers. Financial institutions also need to be able to provide services to new customer segments, including those whose wealth has been derived from crypto-assets.

Doing so requires access to new tools, and importantly, new thinking.

However, current practices for identifying and measuring risks posed by crypto-assets and stablecoins are often opaque, non-reproducible, and are rarely validated by independent third parties.

As the crypto-asset industry matures, new standards are needed to move from ad hoc, vendor-specific solutions towards globally-accepted risk metrics and standards.

What will attendees get?

This workshop marks a first step towards rethinking blockchain transaction monitoring and will provide a forum for regulators, financial institutions, and industry stakeholders to:

- explore methods to safely service new customer segments whose wealth has been derived from crypto-assets,
- understand the different tools available for achieving effective crypto-asset compliance, and how they work,
- design effective frameworks for crypto-asset and stablecoin compliance regimes that balance innovation and systemic risks.

Who should attend?

- Regulators and Policymakers
- Financial Supervisory Authorities
- Central Banks
- Law Enforcement
- Market Crypto Intermediaries
- Financial Institutions

Stakeholders and contributors are invited to join the workshop by reaching out via email to:

contact@blockchaintelligence.com

Practical and Effective Blockchain Intelligence Training

BIPA Workshop in Paris, France on 17 February 2026

The Blockchain Intelligence Professionals Association (BIPA) will be organizing a workshop "Practical and Effective Blockchain Intelligence Training" on 17 February 2026, in Paris, France.

Blockchain intelligence training and certification is fragmented and quality is inconsistent.

Blockchain intelligence training solutions and certification has been dominated by private firms whose vested interest to drive the sale of their own software solutions, has shaped training curriculum to reflect such agendas.

With the growth of crypto-assets, stablecoins, and the rising tokenization of assets, there is an urgent need to develop organic blockchain intelligence capabilities and effective training solutions to manage both the risks and seize the opportunities provided by blockchain technology.

What will attendees get?

Understanding the opportunities and risks from crypto-assets and tokenization are critical in an ever-growing number of industries and attendees can expect to receive:

- the ability to determine appropriate blockchain intelligence training frameworks, curriculum, and coursework
- practical case studies that demonstrate how effective blockchain intelligence training resulted in positive commercial and law enforcement outcomes
- an understanding of the the limitations of blockchain intelligence as it applies to compliance and commercial considerations

At the end of the workshop, attendees should be better-positioned to design appropriate blockchain intelligence training programs, and have a better understanding of the industry.

Who should attend?

- Regulators and Policymakers
- Financial Supervisory Authorities
- Central Banks
- Law Enforcement
- Market Crypto Intermediaries
- Financial Institutions
- Educational and Training Institutes

Stakeholders and contributors are invited to join the workshop by reaching out via email to:

contact@blockchaintelligence.com

Media Coverage

The Blockchain Intelligence Forum 2025 attracted significant international media attention, with journalists and reporters from all over the world in attendance.

General Director of ICI Bucharest, Dr. Victor Vevera, was requested by the Financial Times Specialist: Banking Risk and Regulation to pen an op-ed for the highly-regarded specialist publication.

The inaugural Blockchain Intelligence Forum drew global media attention, drawing journalists from all over the world to attend the event. Here is some selected media coverage following the successful first edition of the Blockchain Intelligence Forum:

Financial Times: Banking Risk & Regulation
Blockchain Tracing Needs Standards to Win Trust

In response to the success of the Blockchain Intelligence Forum, the Financial Times: Banking Risk & Regulation invited Dr. Victor Vevera of ICI Bucharest, organizer of the inaugural event, to write an op-ed discussing the key issues raised from the Forum.

Vevera's op-ed underscored the urgent need for interoperable standards, transparency, and evidence-based practices in blockchain investigations.

With blockchain analytics tools proliferating, and without any regulatory oversight, Vevera called for global alignment on ethical usage, accuracy, and regulatory consistency in applying blockchain intelligence. Vevera noted that the Forum should serve as a a watershed moment, to steer the blockchain intelligence discipline away from opaque and unverified practices, towards greater transparency and global standards.

Vevera stressed that if financial institutions, law enforcement agencies and blockchain analytics providers are to combat crypto-asset-enabled crime effectively, they must invest in training, open standards, and scientific rigor.

The Financial Times: Banking Risk and Regulation amplified the Forum's core message – blockchain intelligence must evolve into a structured, trusted discipline that supports both tthe public interest and financial integrity, with the op-ed providing international recognition of the Forum's thought leadership.

The article is available here:

https://www.bankingriskandregulation.com/blockchain-tracing-needs-standards-to-win-trust/

Other coverage:

- Blockchain analytics must improve to hold up in court
  https://www.compliancecorylated.com/news/blockchain-analytics-must-improve-to-hold-up-in-court/
- Blockchain analytics requires professionalisation, collaboration, more data
  https://www.compliancecorylated.com/news/blockchain-analytics-requires-professionalisation/

ACKNOWLEDGEMENTS

Special appreciation goes to ICI Bucharest and the Blockchain Intelligence Professionals Association (BIPA) for their leadership, vision and commitment to advancing the professionalization of blockchain intelligence, as well as ChainArgos, who contributed significantly to the preparation of this report.

We would like to thank the Basel Institute on Governance for supporting the Forum. We are glad that the Basel Institute endorses the wider mission to collaboratively develop Blockchain intelligence standards and advance professional development and data interoperability in this area.

We are also grateful to all keynote speakers, panelists and delegates who contributed their expertise, insights and collaborative spirit to make the Forum a landmark event in shaping the future of blockchain intelligence, regulation and financial crime prevention.

Their contributions have helped define a shared path forward, reinforcing the importance of transparency, ethical governance and global cooperation in the blockchain intelligence ecosystem.

LEGAL DISCLAIMERS

THE INFORMATION CONTAINED IN THESE MATERIALS IS FOR INFORMATION PURPOSES ONLY AND NOT INTENDED TO BE RELIED UPON.

The information contained herein includes opinions and perspectives by individuals and/or entities that may not reflect the views of the National Institute for Research and Development in Informatics – ICI Bucharest ("ICI Bucharest") and/or the Blockchain Intelligence Professionals Association ("BIPA"), collectively referred to as the "Organizers."

The information herein has not been independently verified or audited and is subject to change, and neither the Organizers nor any other person, is under any duty to update or inform you of any changes to such information. No reliance may be placed for any purposes whatsoever on the information contained in this communication or its completeness. No representation or warranty, express or implied, is given by, or on behalf of the Organizers or any of their members, directors, officers, advisers, agents or employees or any other person as to the accuracy or completeness of the information or opinions contained in this communication and, to the fullest extent permitted by law, no liability whatsoever is accepted by the Organizers or any of their members, directors, officers, advisers, agents or employees nor any other person for any loss howsoever arising, directly or indirectly, from any use of such information or opinions or otherwise arising in connection therewith. In particular, no representation or warranty is given as to the reasonableness of, and no reliance should be placed on, any forecasts or proposals contained in this communication and nothing in this communication is or should be relied on as a promise or representation as to the future or any outcome in the future.

This document may contain opinions which reflect current views with respect to, among other things, the information available when the document was prepared. Readers can identify these statements by the use of words such as "believes", "expects", "potential", "continues", "may", "will", "should", "could", "approximately", "assumed", "anticipates", or the negative version of those words or other comparable words. Any statements contained in this document are based, in part, upon historical data, estimates and expectations. The inclusion of any opinion should not be regarded as a representation by the Organizers or any other person. Such opinion statements are subject to various risks, uncertainties and assumptions and if one or more of these or other risks or uncertainties materialize, or if the underlying assumptions prove to be incorrect, projections, analysis, and forecasts may vary materially from those indicated in these statements. Accordingly, you should not place undue reliance on any opinion statements included in this document.

By accepting this communication you represent, warrant and undertake that you have read and agree to comply with the contents of this notice.