Transcript: Virtual assets regulations fit for the future

Proofread and lightly edited using AI; may contain errors and may not be used for quotes.

Marta Olowska (Moderator):
It is my pleasure to welcome you to this session on shaping virtual assets regulation fit for the future. My name is Marta Olowska, and I work as a Crime Prevention and Criminal Justice Associate at UNODC's Corruption and Economic Crime Branch.

I would like to begin by expressing our sincere appreciation to the co-organisers of this session—the Basel Institute on Governance, the OSCE, and UNODC—for initiating this important discussion at the very first Tech Day of COSP.

With that, I have the honour of inviting Ambassador Bakyt Dzhusupov, Coordinator of OSCE Economic and Environmental Activities, to deliver the opening remarks for this session. Ambassador, the floor is yours.

Ambassador Bakyt Dzhusupov (OSCE):
Thank you very much, Marta.

Dear colleagues, distinguished participants, ladies and gentlemen, it is my pleasure to welcome you to this special event, which the Organization for Security and Co-operation in Europe is honoured to co-organise with our trusted partners, the Basel Institute on Governance and UNODC.

Thank you for joining us to discuss a topic that stands at the crossroads of innovation, regulation, and integrity.

As digital technologies transform our societies, they also offer powerful tools for strengthening transparency and combating corruption, a core priority for the OSCE. Virtual assets and blockchain-based financial technologies are reshaping how value is created and exchanged. They hold tremendous promise—improving the efficiency of payments, expanding financial inclusion, enabling new financial products, and enhancing transparency.

Yet these same features also introduce heightened risks. The speed, anonymity, and borderless nature of digital asset transactions make them attractive for money laundering, corruption, sanctions evasion, terrorist financing, and other serious crimes.

The challenge for policymakers is to enable innovation while closing the gaps exploited by criminal actors. The OSCE is committed to supporting participating States in managing these emerging risks. Through our work on mitigating money laundering risks of virtual

assets, we raise awareness and build capacity across Eastern Europe, the South Caucasus, Central Asia, and Mongolia.

We work closely with national and central banks to strengthen regulatory frameworks for virtual asset service providers, conduct tailored trainings on regulatory and investigative approaches, and support the development of national risk assessments. We also provide blockchain forensic tools to supervisory and law enforcement authorities.

Because virtual assets move seamlessly across borders, no state can address these risks alone. Effective oversight requires coordinated action among regulators, financial intelligence units, law enforcement agencies, the private sector, and international and regional organisations.

Today's discussion is therefore extremely valuable. We are fortunate to have a diverse and highly experienced group of experts representing regulatory frameworks from Qatar, Georgia, Romania, the European Union, and the private sector.

I wish you a productive discussion and encourage you to use this opportunity to exchange practical knowledge and strengthen cooperation. Together, we can ensure that digital finance develops in a way that strengthens security, transparency, and trust.

Thank you.

Marta Olowska (Moderator):
Thank you very much, Ambassador, for setting the scene for our discussion.

It is very symbolic that we are here at the Tech Day of COSP. Technology no longer sits on the margins of corruption or financial crime discussions. It is now central to how illicit economies evolve and, therefore, central to how we respond.

This conversation is deeply rooted in practice. As the Ambassador mentioned, much of the work of the OSCE and UNODC on virtual assets and digital finance responds directly to requests from Member States.

Governments across regions are grappling with the same questions: how do we structure virtual asset frameworks that support innovation without opening new doors to crime? How do we coordinate across borders when criminals can move digital value almost instantly? And how do we ensure that regulation is not only fit for today, but resilient for the years ahead?

Before we begin the first round of interventions, let me briefly introduce our speakers.

We are joined by Tamar Latsabidze, Acting Chief Specialist in the Regulation and Support Division at the National Bank of Georgia, who will share Georgia's experience building and supervising a virtual asset service provider regime.

From the National Bank of Romania, we have Bogdan Vacusta, Strategy Consultant, who will speak about leveraging data and intelligence for effective digital asset supervision and cross-border cooperation.

Joining us online is Gabriel Hugonnot, Policy Officer at the European Commission, working on digital finance policy, who will present the EU's experience with the implementation of the Markets in Crypto-Assets Regulation, MiCA.

We are also joined by Robert MacDonald, Chief Legal and Compliance Officer at Bybit, who will offer an industry perspective on operational security and compliance challenges.

Finally, we are very pleased to be joined by Maha Al-Saadi, Head of Regulatory Affairs for the Financial Services Sector at Qatar Financial Centre, who will share Qatar's approach to digital assets regulation.

When I began working on blockchain and virtual assets in 2017, particularly with tax administrations, the immediate reaction was often "blockchain equals Bitcoin equals bad." If I could make one wish for today's session, it would be that we leave this room understanding that while virtual assets pose challenges, they also present significant opportunities—if regulated correctly.

With that, I would like to start our first round of interventions.

Gabriel, could you please walk us through the core pillars of MiCA and explain what makes it a global benchmark? We would also like to hear about the new AML/CFT measures adopted in 2024 and the challenges that remain around supervisory convergence, CASP authorisation, and enforcement.

Ambassador Bakyt Dzhusupov (OSCE):
Thank you very much, Marta.

Dear colleagues, distinguished participants, ladies and gentlemen, it is my pleasure to welcome you to this special event, which the Organization for Security and Co-operation in Europe is honored to co-organize with our trusted partners, the Basel Institute on Governance and UNODC.

Thank you for joining us to discuss a topic that stands at the crossroads of innovation, regulation, and integrity.

As digital technologies transform our societies, they also offer powerful tools for strengthening transparency and combating corruption, a core priority for the OSCE. Virtual assets and blockchain-based financial technologies are reshaping how value is created and exchanged. They hold tremendous promise—improving the efficiency of payments, expanding financial inclusion, enabling new financial products, and enhancing transparency.

Yet these benefits also come with heightened risks. The speed, anonymity, and borderless nature of digital asset transactions make them attractive for money laundering, corruption, sanctions evasion, terrorist financing, and other serious crimes.

The challenge for policymakers is to enable innovation while closing the gaps exploited by criminal actors. The OSCE is committed to supporting participating States in managing these emerging risks. Through our work on mitigating money laundering risks of virtual assets, we build capacity across Eastern Europe, the South Caucasus, Central Asia, and Mongolia.

We work closely with national and central banks to strengthen regulatory frameworks for virtual asset service providers, conduct tailored trainings, and support national risk assessments. We also provide blockchain forensic tools to supervisory and law enforcement authorities.

Because virtual assets move seamlessly across borders, no state can address these risks alone. Effective oversight requires coordinated action among regulators, financial intelligence units, law enforcement, the private sector, and international organizations.

Today's discussion is therefore extremely valuable. We are fortunate to have a diverse group of experts representing regulatory innovation from Qatar, Georgia, Romania, the European Union, and the private sector.

I wish you a productive discussion and look forward to the exchange of practical insights. Together, we can ensure that digital finance develops in a way that strengthens security, transparency, and trust.

Thank you.

Marta Olowska (Moderator):
Thank you very much, Ambassador, for setting the scene.

It is very symbolic that we are here at COSP Tech Day. Technology no longer sits on the margins of corruption and financial crime discussions—it is central to how illicit economies evolve and therefore central to how we respond.

Governments across regions are grappling with the same questions: how do we structure virtual asset frameworks that support innovation without opening new doors to crime? How do we coordinate across borders when digital value moves instantly? And how do we ensure regulation is not only fit for today, but resilient for years to come?

Before we begin, let me briefly introduce our panelists.

We are joined by Tamar Latsabidze, Acting Chief Specialist at the National Bank of Georgia, who will share Georgia's experience regulating and supervising virtual asset service providers.

From the National Bank of Romania, we have Bogdan Vacusta, Strategy Consultant, who will discuss data, intelligence, and cross-border cooperation.

Joining us online is Gabriel Hugonnot, Policy Officer at the European Commission, responsible for digital finance policy, who will speak about the implementation of the EU's Markets in Crypto-Assets Regulation, MiCA.

We are also joined by Robert MacDonald, Chief Legal and Compliance Officer at Bybit, offering an industry perspective on compliance, security, and lessons learned from recent events.

Finally, we are pleased to welcome Maha Al-Saadi, Head of Regulatory Affairs at Qatar Financial Centre, who will discuss Qatar's distinctive approach to digital assets.

When I began working on blockchain and virtual assets in 2017, the immediate reaction was often "blockchain equals Bitcoin equals bad." My hope is that we leave this room understanding that virtual assets pose challenges, but also significant opportunities—if regulated correctly.

With that, I would like to start our first round of interventions.

Gabriel, could you walk us through the core pillars of MiCA and explain what makes it a global benchmark? We would also like to hear about the new AML/CFT measures adopted in 2024 and the remaining challenges around supervisory convergence, CASP authorization, and enforcement.

Gabriel Hugonnot (European Commission):
Thank you, Marta, and good morning everyone.

The EU's first legislative intervention in crypto was in the AML field. Already in 2020, AML rules brought crypto-fiat exchanges and custodial wallet providers within the scope of obliged entities. However, this approach addressed only AML risks and did not cover broader market, consumer protection, or prudential concerns.

MiCA was proposed in 2020 to fill this gap. Its objectives are to support innovation while addressing consumer protection, market integrity, and financial stability risks. MiCA distinguishes between different types of crypto-assets and focuses on regulating issuers and crypto-asset service providers rather than the technology itself.

MiCA identifies three categories of crypto-assets: asset-referenced tokens, which aim to maintain stable value by referencing multiple assets or currencies; e-money tokens,

intended primarily as means of payment and referencing a single fiat currency; and other crypto-assets, which do not reference external assets and derive value from market demand.

Certain assets fall outside MiCA's scope, including central bank digital currencies, non-fungible tokens in most cases, DeFi protocols without identifiable intermediaries, and crypto-assets already qualifying as financial instruments under existing EU law.

Issuers of general crypto-assets must publish a white paper, while issuers of asset-referenced tokens and e-money tokens must be authorized, hold reserves, offer redemption rights, and meet governance and prudential requirements. Significant stablecoins are supervised by the European Banking Authority.

Crypto-asset service providers must be licensed and are subject to conduct, organizational, and market abuse rules. Transitional arrangements apply, but by July 2026 all providers operating in the EU must hold a MiCA license.

On AML/CFT, the EU has implemented the FATF travel rule for crypto-asset transfers and adopted new AML legislation in 2024. This will prohibit anonymous crypto-asset accounts and introduce crypto-asset account registers across Member States, interconnected by 2029. A new EU Anti-Money Laundering Authority will directly supervise high-risk crypto-asset service providers starting in 2028.

MiCA is not the end of the story. In December, the Commission proposed amendments to address market fragmentation, including transferring certain supervisory powers over crypto-asset service providers to ESMA.

Marta Olowska (Moderator):
Thank you very much, Gabriel, for this comprehensive overview.

Maha, Qatar has adopted a distinctive two-track regulatory model. Could you explain how Qatar views different types of virtual or digital assets, how this model was developed, and how it supports financial crime risk management?

Maha Al-Saadi (Qatar Financial Centre):
Thank you, and good morning everyone. Apologies for joining slightly late.

Qatar has deliberately adopted a two-track regulatory approach. We focus on real-world asset tokenization and permissioned distributed ledger technology, while keeping stablecoins and cryptocurrencies out of scope for now. This allows us to build infrastructure that is fit for purpose and future-proof, while we continue to study the risks associated with unbacked crypto-assets.

We regulate use cases and services, not the technology itself. If blockchain is used as infrastructure for financial instruments, existing securities, banking, or insurance regulations apply. If blockchain is used for non-financial services, registration rather than authorization may suffice.

Our Digital Assets Framework and Investment Token Rules were issued in 2024. We deliberately avoided narrow token classifications, opting instead for a broad distinction between permitted tokens and excluded tokens. This gives us flexibility as the market evolves.

Financial crime controls apply regardless of tokenization. Institutions must comply with AML/CFT, conduct, and prudential requirements. Tokenization introduces novel risks, particularly around cybersecurity and operational resilience, which supervisors must assess carefully.

We are studying global approaches closely and expect to evolve our framework as markets mature.

Marta Olowska (Moderator):
Thank you very much, Maha.

Tamar, Georgia moved very quickly to regulate virtual assets. Could you share how the regulatory framework was tailored to Georgia's specific risk exposure and what challenges emerged during implementation?

Tamar Latsabidze (National Bank of Georgia):
Georgia has moved quickly to regulate virtual assets, initially from an AML/CFT perspective. Regulators today face a trilemma: setting clear rules, safeguarding against risks such as money laundering and fraud, and keeping pace with innovation.

Unlike earlier eras, regulators no longer have the luxury of time. Innovation evolves rapidly and often organically. Our response has been learning by doing.

We established a regulatory sandbox that allows innovative products to be tested in a supervised environment. This enables us to assess risks and adapt regulation accordingly.

A key example is tokenized deposits. By embedding compliance controls at the design stage, we can ensure traceability, consumer protection, and risk management while enabling innovation.

Coordination and cooperation are critical—between regulators, with the private sector, and internationally. Platforms such as UNODC, the OSCE, and the Basel Institute enable regulators to share lessons learned and avoid regulatory arbitrage.

Marta Olowska (Moderator):
Thank you, Tamar.

Bogdan, Romania has taken a strong intelligence-led approach. Could you tell us more about leveraging data and intelligence for effective digital asset supervision and cross-border cooperation?

Bogdan Vacusta (National Bank of Romania):
From an intelligence perspective, data alone is not enough. Intelligence transforms data into insight that supports decision-making.

Blockchain intelligence combines on-chain transaction data with off-chain information from traditional finance. This is essential for authorization, supervision, enforcement, and cross-border cooperation.

A key challenge is fragmentation and data gaps. Blockchain analytics methodologies differ across providers and are often opaque. Without standardization, supervisors must question the reliability of results.

Establishing minimum standards for blockchain analytics is essential to ensure data integrity, reduce false positives, and support trusted decision-making.

Marta Olowska (Moderator):
Thank you, Bogdan.

Robert, from the private sector perspective, what are the biggest compliance and security challenges exchanges face today, and what lessons can be drawn from Bybit's recent experience?

Robert MacDonald (Bybit):
Security and compliance are constantly evolving challenges. Threats such as phishing, deepfakes, and sophisticated hacking techniques change rapidly.

Earlier this year, Bybit was targeted by a state-linked actor. While the incident affected company funds rather than user assets, it prompted a comprehensive review of our security architecture, wallet infrastructure, and incident response processes.

Key lessons include the importance of speed, transparency, cooperation with law enforcement, and robust on-chain analytics. Standardization—both in blockchain analytics

and in law enforcement request formats—would significantly improve efficiency and effectiveness across the ecosystem.

Marta Olowska (Moderator):
I would now like to ask each of you one final question. If you could identify just one priority to make virtual assets regulation more future-proof over the next three to five years, what would it be?

Maha Al-Saadi (Qatar Financial Centre):
Only one?
I think we often speak about international cooperation, which is extremely important, but we sometimes forget cooperation within a jurisdiction. Cooperation between the securities regulator, the central bank, and law enforcement is critical.

If I had to focus on one thing, it would be this: before international cooperation, we need to get our act together nationally. We need a clear national vision on how to deal with different types of crypto and digital assets, enforcement, compliance, and risk management.

I would also hope that, through this national and international cooperation, we rethink how we assess sandboxes and innovation labs. Sandboxes are useful, but they are still tests and not real life. We need to move from testing environments to controlled live simulations with limited use cases, users, and thresholds.

This is the only way we can be prepared and develop regulation that is proportionate, fit for purpose, and does not require constant adjustment.

Marta Olowska (Moderator):
Thank you. Gabriel, from your perspective, what would be the one priority you would highlight?

Gabriel Hugonnot (European Commission):
Thank you, Marta.
Before joining the digital finance unit, I spent several years working on money laundering and on the FATF standards for crypto-assets. From that perspective, I would say that decentralized finance remains one of the biggest challenges.

Many jurisdictions, including the EU, apply a functional approach to look beyond how a platform self-identifies and determine whether there is an entity that can be considered an obliged entity. However, where no such entity exists, implementing legal obligations becomes much more difficult.

I believe decentralized finance is an area where further work and investigation are needed to understand how risks can be addressed more effectively.

From an AML perspective, FATF standards have applied to crypto-assets for more than five years. At this stage, there are very few reasons not to have at least AML legislation in place that fully complies with those standards.

We also see jurisdictions learning from one another. For example, when we look at recent U.S. legislation, we observe many similarities with MiCA. This shows that jurisdictions can draw inspiration from existing frameworks rather than starting from scratch.

Marta Olowska (Moderator):
Thank you very much. Tamar, what would be your priority?

Tamar Latsabidze (National Bank of Georgia):
One important development I would like to highlight is that, until recently, Georgia regulated virtual asset service providers mainly from an AML/CFT perspective. Now, the mandate of the National Bank of Georgia has been expanded to include prudential regulation, cybersecurity, and investor protection.

This is a significant step forward for a country like Georgia. It allows us not just to regulate more, but to safeguard investors and work more closely with the private sector to deliver innovative solutions.

We hear a lot of negative news about crypto-assets, hacks, and criminal misuse. But if we strip away the bad actors and look at the technology itself, blockchain is largely traceable and transparent. From an anti-corruption perspective, this is extremely valuable.

As regulators, we need to balance innovation and regulation carefully. We should not over-regulate, but we also need to understand and embrace the technology, because it offers significant opportunities.

Marta Olowska (Moderator):
Thank you. Bogdan, what would be your priority?

Bogdan Vacusta (National Bank of Romania):
For me, standardization in blockchain analytics is the key priority.

In recent years, I have seen many confidential discussions highlighting this challenge. It is time to speak more openly about it. Data integrity is a major issue, and as regulators and supervisors, we must be confident that the data we rely on has not been manipulated.

Blockchain transactions are traceable, but only partially. Different blockchain analytics providers use different methodologies, and there is a high level of false positives. Without minimum standards, supervisors are justified in questioning both the methodology and the results.

Standardization would help ensure transparency, consistency, and trust in blockchain analysis. This is not a challenge that any single entity can solve alone. It requires collective effort across regulators, supervisors, and the private sector.

Marta Olowska (Moderator):
Thank you. Robert, what would be your one priority?

Robert MacDonald (Bybit):
I would strongly support standardization.

First, standardization in blockchain analytics. As an exchange, we are fortunate to work with multiple analytics providers and compare their strengths and weaknesses, but not every company has that capability. Common standards would greatly improve accuracy and reduce false positives.

Second, standardization of law enforcement requests. We receive thousands of requests every week, and the quality and format vary significantly. Better standardization would help both exchanges and law enforcement understand what information is available, what can be shared, and how quickly it can be provided.

Education is also part of this. Regulators and law enforcement are still grappling with how blockchain works, and clearer standards would help bridge that gap and improve cooperation across the ecosystem.