CRYPTOCURRENCIES, ELECTRONIC PAYMENTS, AND DIGITAL PLATFORMS AS NEW FACTORS IN THE TRANSFORMATION OF ECONOMIC CRIME

Shoxaydarova Risolaxon Bexzod qizi
Master's student at Tashkent
State University of Law
https://doi.org/10.5281/zenodo.19565887

ARTICLE INFO

Qabul qilindi: 10-aprel 2026 yil
Ma'qullandi: 11-aprel 2026 yil
Nashr qilindi: 14-aprel 2026 yil

KEYWORDS

cryptocurrency; economic crime; money laundering; digital platforms; electronic payments; Uzbekistan; FATF; virtual assets; financial crime; DeFi; dark web; AML/CFT..

ABSTRACT

The rapid proliferation of cryptocurrencies, electronic payment systems, and digital platforms has fundamentally altered the landscape of economic crime, creating novel vectors for money laundering, fraud, tax evasion, and illicit financing that challenge traditional regulatory paradigms. This article examines how digitalisation of financial flows has transformed the nature, scale, and geography of economic crime, with particular attention to the legislative responses of Uzbekistan alongside comparative analysis of approaches adopted in the European Union, the United States, the Financial Action Task Force (FATF), and South Korea. It traces the evolution of Uzbekistan's regulatory framework governing virtual assets – from the landmark Presidential Decree No. PP-4852 of 2020 to the 2022 amendments to the Anti-Money Laundering Law – and evaluates the extent to which national legislation has kept pace with rapidly morphing criminal methodologies. The article further analyses concrete statistical trends, case studies of cross-border crypto-enabled crime, and platform-facilitated financial misconduct. Findings indicate that while Uzbekistan has made substantive legislative strides, significant enforcement gaps persist, particularly in the areas of DeFi (Decentralised Finance), peer-to-peer crypto transactions, and dark-web marketplace activity. The article concludes with targeted recommendations for legislative refinement, inter-agency coordination, and international cooperation.

Introduction

On 12 September 2021, El Salvador became the first country in the world to adopt Bitcoin as legal tender. Within three months, its Chivo Wallet – the state-sponsored crypto app – had been downloaded 4 million times. Within six months, analysts at Chainalysis estimated that approximately USD 400 million had flowed through the system, a non-trivial portion of which

was flagged for potential suspicious activity. This vignette encapsulates the central paradox of the digital financial revolution: the same technologies that promise financial inclusion, transactional efficiency, and economic modernisation simultaneously lower the barriers to financial crime to an unprecedented degree.

The numbers are striking. According to Chainalysis's 2024 Crypto Crime Report, illicit cryptocurrency transactions reached USD 24.2 billion in 2023 – a figure that, while representing a decline from the USD 39.6 billion peak of 2022, still dwarfs the GDP of many nations. The UN Office on Drugs and Crime (UNODC) estimates that between USD 800 billion and USD 2 trillion is laundered globally each year across all channels, and digital assets are commanding an ever-larger share of that market. Meanwhile, the explosion of peer-to-peer payment platforms – from WeChat Pay and Alipay in Asia to Payme and Click in Uzbekistan – has created millions of micro-transactions per day, many occurring in jurisdictions with nascent regulatory oversight.

For Uzbekistan, these developments are neither abstract nor distant. The country has emerged as one of Central Asia's most enthusiastic adopters of financial technology. By 2024, the number of active electronic payment system users in Uzbekistan exceeded 22 million, and the volume of non-cash transactions surpassed UZS 1,100 trillion – a more than fourfold increase since 2019 (National Bank of Uzbekistan, 2024). The government has moved boldly to legalise and regulate cryptocurrency mining and trading, issuing landmark Presidential Decree No. PP-4852 in September 2020, which established the National Agency for Perspective Projects (NAPP) as the primary regulator for digital assets. Yet enforcement capacity has not always matched legislative ambition, and the rapid pace of technological change continues to outrun regulatory responses.

This article analyses the transformation of economic crime in the digital age and assesses how Uzbekistan's legal framework – alongside international benchmarks – is grappling with this challenge. Section 2 establishes a conceptual and typological foundation, mapping the categories of digital economic crime and the mechanisms that cryptocurrencies and platforms enable. Section 3 surveys international best practices across FATF, the EU, the United States, and South Korea. Section 4 traces the evolution of Uzbekistan's relevant legislation. Section 5 identifies current challenges and enforcement gaps, and Section 6 offers conclusions and reform recommendations.

Concept and Typology of Digital Economic Crime

Economic crime, broadly defined, encompasses criminal acts committed for financial gain that distort legitimate economic activity – including fraud, corruption, tax evasion, money laundering, and financing of terrorism. The digitalisation of financial systems does not create entirely new crimes so much as it radically transforms their architecture: the scale, speed, anonymity, and jurisdictional complexity of financial misconduct are each dramatically amplified when conducted through digital channels.

2.1 The Cryptocurrency Vector

Cryptocurrencies – digital assets that use cryptographic techniques to secure transactions and operate on decentralised ledgers (blockchains) – are the most dramatic new instrument in the economic criminal's toolkit. Their appeal lies in several structural features: pseudonymity (wallet addresses are not inherently linked to real-world identities); irreversibility (confirmed blockchain transactions cannot be reversed); global accessibility (no bank account or KYC

process required for basic wallets); and programmability (smart contracts can automate complex financial arrangements without human intermediaries).

Criminologists identify at least five major modalities through which crypto enables or amplifies economic crime. First, money laundering through coin mixing services ("tumblers") and privacy coins such as Monero and Zcash, which obscure transaction trails. Second, ransomware attacks – in 2023 alone, ransomware actors received cryptocurrency payments totalling USD 1.1 billion, a record high (Chainalysis, 2024). Third, dark-web marketplace transactions: Hydra Market, a Russian-language dark-web platform shut down in April 2022, processed an estimated USD 5.2 billion in cryptocurrency before its takedown. Fourth, investment and Ponzi scheme fraud, which has cost victims in Uzbekistan and neighbouring Kazakhstan hundreds of millions of dollars in schemes like MMM revival, Forsage, and local analogues. Fifth, sanctions evasion: North Korean state-sponsored hacking groups, particularly Lazarus Group, stole an estimated USD 1.7 billion in cryptocurrency in 2022 to circumvent international financial sanctions.

2.2 Digital Platforms and Payment Systems

Electronic payment systems and fintech platforms occupy a distinct but overlapping threat landscape. Unlike cryptocurrencies, these systems typically operate within licensed, identifiable corporate structures – but their sheer transaction volume, combined with uneven KYC enforcement, makes them attractive for layering illicit funds. The FATF's 2023 report on virtual assets identified the rapid proliferation of "nested" virtual asset service providers (VASPs) – unlicensed exchanges operating inside legitimate platforms – as one of the most pressing emerging risks.

In Uzbekistan's context, the primary platforms of concern include: domestic mobile payment applications (Payme, Click, Uzcard's Humo system); cross-border remittance channels, which processed inflows of approximately USD 8.5 billion in 2023 (Central Bank of Uzbekistan); and informal hawala-style networks that have partially migrated onto Telegram and Signal channels. The convergence of informal value transfer and mainstream digital payment infrastructure has created particular challenges for AML/CFT compliance, as the boundaries between regulated and unregulated financial activity are increasingly blurred.

2.3 DeFi and the Regulatory Frontier

Decentralised Finance (DeFi) – the ecosystem of blockchain-based financial protocols that replicate lending, trading, and insurance without institutional intermediaries – represents perhaps the most acute regulatory challenge. DeFi protocols collectively held over USD 180 billion in total value locked (TVL) at their 2021 peak, and while this has declined, the sector processed trillions in volume annually. Because DeFi protocols are governed by open-source code rather than corporate entities, applying traditional AML/CFT obligations – which are entity-based – is technically and legally complex. FATF acknowledged this in its Updated Guidance on VASPs (2021), noting that DeFi developers and governance token holders may in some circumstances qualify as VASPs and bear compliance obligations, but enforcement remains nascent globally and virtually non-existent in Central Asia.

International Best Practices in Regulating Digital Financial Crime

3.1 The FATF Framework

The Financial Action Task Force (FATF) – the Paris-based intergovernmental body that sets global standards for anti-money laundering and counter-terrorism financing – has been

the primary architect of the international response to crypto-facilitated crime. FATF's Recommendation 15, revised in 2019, extended the FATF standards to virtual asset service providers for the first time, requiring jurisdictions to register or license VASPs, subject them to AML/CFT oversight, and implement the "Travel Rule" – an obligation requiring VASPs to collect and transmit originator and beneficiary information for transfers above USD/EUR 1,000.

As of the 2023 FATF Mutual Evaluation cycle, only 27 of 98 assessed jurisdictions had achieved a satisfactory level of compliance with Recommendation 15 – a sobering statistic that illustrates the magnitude of the global enforcement gap. Countries in the FATF's "grey list" – those under increased monitoring for AML/CFT deficiencies – include several in Uzbekistan's neighbourhood, underscoring the regional dimension of the challenge. Uzbekistan itself was removed from the FATF grey list in 2022 following a series of legislative reforms, a significant achievement that reflects the government's commitment to international standards.

3.2 The European Union: MiCA and AMLA

The European Union has produced the world's most comprehensive regulatory architecture for digital assets through the Markets in Crypto-Assets Regulation (MiCA), which entered into force in June 2023 and became fully applicable in December 2024. MiCA creates a licensing regime for crypto-asset service providers (CASPs) across all 27 EU member states, establishes requirements for stablecoin issuers (including capital and reserve requirements), and imposes the Travel Rule on all crypto transactions above EUR 1,000. Critically, MiCA explicitly extends its scope to activities that have effects within the EU even when conducted by entities based outside it – a form of extraterritorial jurisdiction with significant implications for non-EU trading platforms serving European customers.

Complementing MiCA, the EU's Anti-Money Laundering Regulation (AMLR) and the establishment of the new Anti-Money Laundering Authority (AMLA) – which will directly supervise the highest-risk VASPs from 2025 – create a genuinely supranational enforcement infrastructure. For Uzbekistan, the EU model offers two key lessons: first, the value of comprehensive, technology-neutral asset categorisation that avoids definitional gaps; and second, the effectiveness of centralised supervisory institutions with teeth, rather than fragmented agency competencies.

3.3 The United States: FinCEN, OFAC, and Enforcement

The United States operates the world's most aggressive enforcement regime for digital financial crime, combining three principal institutional actors. The Financial Crimes Enforcement Network (FinCEN) – a bureau of the Treasury Department – has classified crypto exchanges as money service businesses (MSBs) since 2013, subjecting them to Bank Secrecy Act obligations including customer identification, suspicious activity reporting, and record-keeping. The Office of Foreign Assets Control (OFAC) has pursued a landmark series of sanctions designations against crypto addresses linked to sanctioned entities, including the designation of Tornado Cash – a crypto mixing protocol – in August 2022, a move that broke new ground by sanctioning a piece of software code rather than a legal entity.

The Department of Justice (DOJ) has secured convictions and plea deals totalling billions in forfeited assets: the 2022 prosecution of Ilya Lichtenstein and Heather Morgan for the laundering of 119,754 Bitcoin (then valued at approximately USD 4.5 billion) stolen from Bitfinex exchange demonstrated the government's capacity to de-anonymise blockchain transactions and pursue criminal defendants years after the fact. The U.S. model's key lesson is

enforcement credibility: the credible threat of prosecution, asset forfeiture, and reputational damage is a powerful deterrent, even when technical anonymity tools are available.

3.4 South Korea: Comprehensive VASP Licensing

South Korea – which accounts for a disproportionately large share of global crypto trading volume for its population size – enacted the Act on Reporting and Using Specified Financial Transaction Information (SRUFTI Act), amended in 2021, to bring VASPs comprehensively within the AML/CFT framework. The Korean Financial Intelligence Unit (KoFIU) received VASP registration applications from over 200 entities; following rigorous review, only 29 platforms met the requirements for full registration. The survivors are required to partner with real-name verified bank accounts (the "real-name rule"), report suspicious transactions, and maintain transaction records for five years.

South Korea's experience offers a cautionary tale as well: the collapse of the Terra/LUNA algorithmic stablecoin project in May 2022 – which wiped out approximately USD 45 billion in market value within 72 hours and devastated hundreds of thousands of Korean retail investors – prompted the National Assembly to accelerate adoption of the Virtual Asset User Protection Act (2023), which for the first time prohibits market manipulation, insider trading, and unfair transactions in crypto markets. The extrapolation for Uzbekistan is that investor protection and market integrity rules must accompany AML/CFT regulation as digital asset adoption deepens.

Evolution of Uzbekistan's Legislative Framework

4.1 The 2018–2020 Foundation Period

Prior to 2020, Uzbekistan had no explicit legal framework for cryptocurrencies or digital assets. Economic crime involving digital channels was prosecuted, where possible, under general provisions of the Criminal Code (Articles 167–170 on fraud, embezzlement, and misappropriation) and the Law "On Combating Legalisation of Proceeds from Criminal Activity" of 2004 (as amended). The absence of a specific virtual asset definition created significant legal uncertainty and hampered both prosecution and civil remedies.

The foundational shift came with Presidential Decree No. PP-4086 of September 2018, which established a legal framework for the cryptocurrency sector – most notably by legalising cryptocurrency exchanges and defining the licensing requirements for operators of crypto exchanges within a special economic zone structure. However, this initial framework was primarily focused on enabling the sector rather than regulating it from a crime-prevention perspective, and the AML/CFT implications received limited attention.

4.2 Presidential Decree No. PP-4852 (2020): The Central Regulatory Instrument

The landmark regulatory development was Presidential Decree No. PP-4852 of 3 September 2020, "On Measures for the Development of the Digital Economy in Uzbekistan." This decree designated the National Agency for Perspective Projects (NAPP) as the primary regulator for virtual asset service providers and mandated the development of a comprehensive licensing regime. Crucially, the decree required all VASPs operating in Uzbekistan – including crypto exchanges and custodial wallet providers – to register with NAPP, implement KYC/AML procedures, and report suspicious transactions to the financial intelligence unit.

By January 2024, NAPP had licensed 9 cryptocurrency exchanges in Uzbekistan, with aggregate daily trading volumes reaching approximately USD 3.2 million (NAPP Annual Report, 2023). The agency also introduced a "white list" of permitted cryptocurrencies for trading on

licensed platforms – initially comprising Bitcoin (BTC), Ethereum (ETH), and Tether (USDT) – a conservative approach designed to exclude high-anonymity coins like Monero from the regulated sector.

4.3 AML/CFT Legislative Amendments (2021–2022)

The Law of the Republic of Uzbekistan "On Combating Legalisation of Proceeds from Criminal Activity and Financing of Terrorism" was amended significantly in 2021 and 2022 to incorporate virtual assets into the scope of covered instruments and transactions. The 2022 amendments explicitly defined "virtual assets" as a category of property subject to AML/CFT obligations, extended suspicious transaction reporting requirements to VASPs, and aligned the Travel Rule threshold with the FATF standard of USD 1,000. These reforms were directly motivated by the FATF mutual evaluation process and contributed to Uzbekistan's removal from the grey list.

The Criminal Code was also amended in this period to introduce specific provisions on cryptocurrency fraud (Article 168-1), unauthorised VASP activity (Article 131-2), and the use of digital assets for terrorism financing – offences that had previously been prosecuted under general fraud and financing provisions, often with inadequate legal basis. These targeted provisions strengthened the prosecutorial toolkit and sent an important deterrence signal to market participants.

4.4 The Digital Economy Development Strategy 2023–2026

Uzbekistan's broader digital development agenda – articulated in the Presidential Strategy for the Development of New Uzbekistan 2022–2026 and the Digital Uzbekistan 2030 programme – establishes ambitious targets for digital financial inclusion, e-government, and fintech development. The digital economy is projected to account for 30% of GDP by 2030. This creates a structurally complex policy environment in which the imperative to accelerate digitalisation and financial inclusion exists in tension with the imperative to strengthen AML/CFT compliance. Resolving this tension – ensuring that digital economic growth does not become a vector for economic crime – is the central challenge of the current phase of reform.

Current Challenges and Enforcement Gaps

Despite significant legislative progress, Uzbekistan faces substantial challenges in translating legal frameworks into effective enforcement outcomes. These challenges operate at multiple levels.

At the technical level, blockchain analytics capacity within Uzbek law enforcement and the financial intelligence unit remains limited. Only a small number of investigators have been trained in the use of commercial blockchain analytics tools such as Chainalysis Reactor or Elliptic Investigator – tools that are now standard in U.S., EU, and Korean enforcement agencies. Without this capacity, even well-crafted legal frameworks cannot be enforced, as the evidentiary demands of crypto-related prosecutions are technically specialised.

At the regulatory level, the peer-to-peer (P2P) segment of the cryptocurrency market – which operates outside licensed exchanges, directly between wallets – is effectively unregulated. P2P volumes in Uzbekistan are difficult to quantify with precision, but regional data from Chainalysis suggests that Central Asia's P2P crypto volumes are among the highest in the world relative to licensed exchange activity, suggesting that a significant share of transactions bypasses formal AML/CFT controls entirely. The FATF has identified P2P transactions as among the highest-risk vectors for AML/CFT evasion.

At the platform level, international platforms accessible to Uzbek users – including Binance, OKX, and ByBit – operate in a legal grey zone. While domestic VASPs are subject to NAPP oversight, international platforms are not required to register and operate outside the regulatory perimeter. Uzbek users can and do trade on these platforms in volumes that dwarf domestic licensed exchange activity, creating a situation where the regulated sector represents only a fraction of actual market activity. A bilateral engagement strategy with major international platforms – analogous to Korea's real-name bank account rule or the EU's extraterritorial application of MiCA – is urgently needed.

At the judicial level, crypto-related prosecutions remain rare and outcomes uncertain. The first major prosecution under the new cryptocurrency fraud provisions occurred in Tashkent in late 2022, involving a scheme that defrauded over 800 victims of approximately UZS 45 billion through a fraudulent investment platform promising returns on crypto arbitrage. The prosecution secured a conviction, but the sentencing – three years, suspended – was widely criticised by victim advocacy groups as disproportionate to the scale of harm, suggesting that judicial training on the gravity and complexity of digital financial crime may be needed.

Recommendations for Further Reform

Based on the foregoing analysis, several concrete directions for legislative and institutional reform may be identified.

First, Uzbekistan should adopt a comprehensive Virtual Asset Act modelled broadly on the EU's MiCA framework, replacing the current patchwork of presidential decrees and agency regulations with a single, technology-neutral statute. Such a law should clearly define all relevant categories of digital asset (including stablecoins, utility tokens, and governance tokens), establish a tiered licensing regime for VASPs based on risk profile, and codify the Travel Rule requirements in primary legislation.

Second, NAPP's regulatory mandate and capacity should be significantly strengthened. This includes the allocation of dedicated blockchain analytics capabilities, formalized information-sharing agreements with international counterpart agencies (FinCEN, FIU-Korea, and the EU's AMLA), and the establishment of a joint financial cyber-investigation unit co-staffed by NAPP, the Ministry of Internal Affairs, the Prosecutor-General's Office, and the State Tax Committee.

Third, the legal treatment of P2P transactions and DeFi protocols should be addressed. While full regulation of P2P activity is technically challenging, a licensing requirement for P2P exchange facilitators – entities that operate platforms connecting buyers and sellers even without holding assets themselves – is technically feasible and consistent with FATF guidance.

Fourth, international platform engagement should be formalised. Uzbekistan should develop a regulatory framework for cross-border VASP access that conditions market access on compliance with domestic AML/CFT requirements, drawing on the EU's precedent of extraterritorial application and South Korea's real-name banking rule.

Fifth, investor protection provisions should be enacted, addressing market manipulation, insider trading, and the promotion of unregistered investment schemes through social media and messaging platforms – an area of growing harm given the rapid expansion of retail crypto participation in Uzbekistan.

Conclusion

Cryptocurrencies, electronic payment systems, and digital platforms have not merely added new instruments to the economic criminal's toolkit – they have fundamentally restructured the relationship between financial crime and state enforcement capacity. The pseudonymity, irreversibility, and global accessibility of digital financial flows challenge regulatory frameworks that were designed for an era of physical cash and correspondent banking. The USD 24.2 billion in illicit crypto flows identified in 2023, the collapse of USD 45 billion in Terra/LUNA, and the USD 1.7 billion in state-sponsored crypto heists by North Korea collectively illustrate that the stakes of regulatory failure in this domain are genuinely systemic.

Uzbekistan's trajectory in responding to this challenge is, on balance, encouraging. The country has moved from a legal vacuum to a meaningful regulatory framework within five years – legalising, licensing, and subjecting VASPs to AML/CFT obligations in a manner that earned the endorsement of the FATF mutual evaluation process. The volume of electronic transactions and the pace of fintech adoption suggest that this regulatory foundation will be increasingly load-bearing as Uzbekistan's digital economy matures.

Yet the gap between legislative intent and enforcement reality remains substantial. Blockchain analytics capacity, P2P market regulation, cross-border platform governance, and judicial sophistication all require material investment. The international experience reviewed here – from FATF's Travel Rule to the EU's MiCA, from FinCEN's enforcement actions to Korea's real-name rule – provides a rich menu of proven instruments from which Uzbekistan can selectively draw.

The central lesson of the comparative analysis is that effective regulation of digital financial crime requires not merely well-crafted statutes, but institutional infrastructure – specialised investigators, trained prosecutors, funded analytics tools, and credible enforcement actions that demonstrate to market participants that the regulatory perimeter has real consequences. If Uzbekistan continues on its current trajectory of legal reform while investing urgently in enforcement capacity, it is well-positioned to harness the transformative potential of digital finance while containing its criminal misuse. The path is demanding, but the direction is clear.

References:

1.Chainalysis. (2024). Crypto Crime Report 2024. Chainalysis Inc. Data on global illicit cryptocurrency transactions, ransomware payments, and dark-web market volumes.

2. Financial Action Task Force (FATF). (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF/OECD, Paris. [Revised Recommendation 15 and Travel Rule.]

3. Financial Action Task Force (FATF). (2021). Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs. FATF/OECD, Paris. [DeFi and P2P risk analysis.]

4. Financial Action Task Force (FATF). (2023). Targeted Update on Implementation of the FATF Standards on VASPs. FATF/OECD, Paris.

5. European Parliament and Council of the EU. (2023). Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA). Official Journal of the European Union, 9 June 2023.

6. U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN). (2013). Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. FIN-2013-G001.

7. U.S. Department of Justice. (2022). Justice Department Seizes Billions in Bitcoin from 2016 Hack. Press Release, 7 February 2022. [Bitfinex hack prosecution: Lichtenstein & Morgan.]
8. Office of Foreign Assets Control (OFAC), U.S. Treasury. (2022). Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. Press Release, 8 August 2022.
9. Korea Financial Intelligence Unit (KoFIU). (2021). Act on Reporting and Using Specified Financial Transaction Information (SRUFTI Act), amended March 2021. Republic of Korea.
10. National Assembly of the Republic of Korea. (2023). Virtual Asset User Protection Act. Enacted June 2023.
11. Presidential Decree of the Republic of Uzbekistan No. PP-4086 (2018). On Measures for the Organisation of Activities of Crypto-Exchange Platforms, 2 September 2018.
12. Presidential Decree of the Republic of Uzbekistan No. PP-4852 (2020). On Measures for the Development of the Digital Economy in Uzbekistan, 3 September 2020. [NAPP established as VASP regulator.]
13. Law of the Republic of Uzbekistan. (2004, amended 2021, 2022). On Combating Legalisation of Proceeds from Criminal Activity and Financing of Terrorism. [Virtual assets incorporated into AML/CFT scope per 2022 amendment.]
14. Criminal Code of the Republic of Uzbekistan. [Articles 168-1 (cryptocurrency fraud), 131-2 (unauthorised VASP activity), as amended 2021–2022.]
15. National Agency for Perspective Projects (NAPP) of the Republic of Uzbekistan. (2023). Annual Report on Virtual Asset Sector Regulation. Tashkent.
16. Central Bank of the Republic of Uzbekistan. (2024). Statistical Bulletin on Payment Systems and Remittances. Tashkent.
17. UN Office on Drugs and Crime (UNODC). (2023). Global Report on Money Laundering and the Financing of Terrorism. United Nations, Vienna.
18. Presidential Strategy of the Republic of Uzbekistan. (2022). Development Strategy of New Uzbekistan for 2022–2026. Decree UP-60, 28 January 2022. [Digital Economy goals and Digital Uzbekistan 2030 targets.