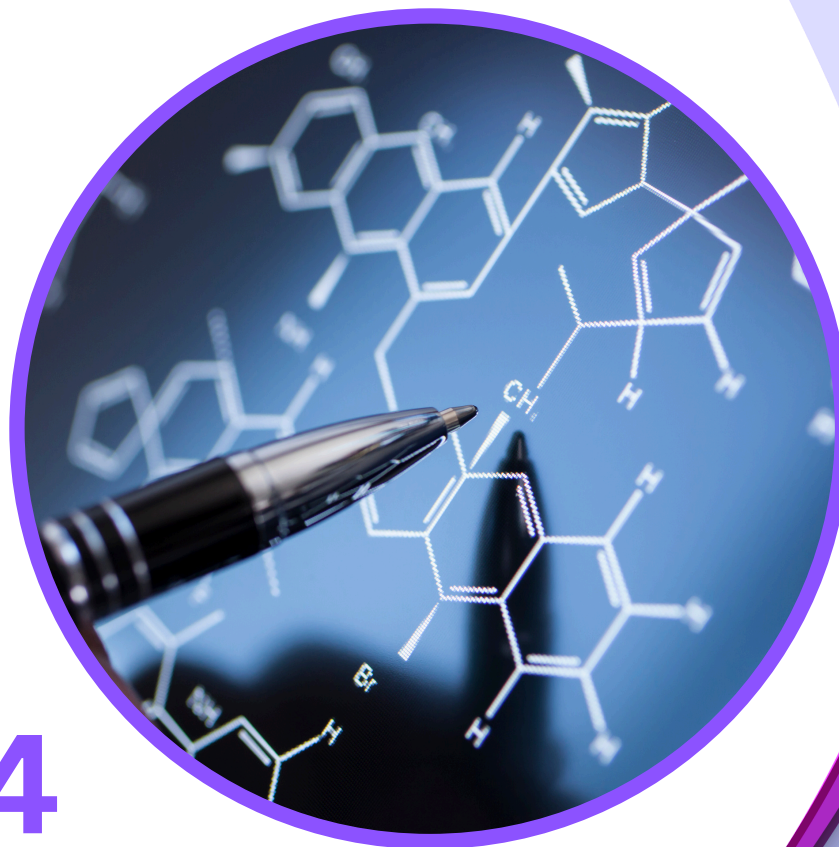


Science Conference

www.science-conference.com

a digital platform dedicated to disseminating a wide array of scientific research articles and papers. It serves as a valuable resource for the scientific community and others interested in cutting-edge scientific knowledge and insights.



2024
No 1 (2)

TABLE OF CONTENTS

QUANTUM SUPREMACY: EXPLORING THE DISRUPTIVE POTENTIAL OF QUANTUM COMPUTING ON CRYPTOGRAPHY AND LEGAL FRAMEWORKS FOR DATA SECURITY.....	2
Islombek Abdikhakimov.....	2
ЗАЩИТА ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА В КИБЕРПРОСТРАНСТВЕ	13
Салауат Коньисбаев.....	13
RAQAMLI AKTIVLAR SOHASIDAGI JINOYATLAR.....	20
Parvina G‘ulommamatova.....	20
O‘ZBEKISTON RESPUBLIKASI JINOYAT QONUNCHILIGIDA KIBERJINOYATLARNI TERGOV QILISH VA ULARNING AHAMYATI.....	31
Abbosjon Olimov.....	31
RAQAMLI MUALLIFLIK HUQUQI TUSHUNCHASINING MAZMUN-MOHİYATI, KELIB CHIQISHI, ASOSIY TAMOYILLARI.....	38
Mohinur Bahramova.....	38
Behruz Eshpo‘latov.....	38
RAQAMLI BOSHQARUVNING HUQUQIY ASOSLARINI BAHOLASHNING O‘ZIGA XOS JIHATLARI.....	45
Jamshid Odilov.....	45
FUQAROLIK SUD ISHLARINI YURITISHDA ADVOKATNING HUQUQ VA MAJBURIYATLARI.....	56
Maftuna O‘rolova.....	56
MARKAZLASHTIRILMAGAN AVTONOM TASHKILOTLAR (DAO) VA O‘ZGARMAS TOKENLAR (NFTS) KABI RIVOJLANAYOTGAN BLOKCHEYN TEXNOLOGIYALARNING XALQARO QONUNCHILIKKA POTENTIAL TA‘SIRI..	67
Nazokat Ismoilova.....	67
ZAMONAVIY HUQUQIY PARADIGMA KONTEKSIDA KIBER SPORT SOHASINI TARTIBGA SOLISHNING NAZARIY VA HUQUQIY JIHATLARI.....	74
San‘atjon Ergashev.....	74
KIBERXAVFSIZLIK VA INSON HUQUQLARINI HIMOYA QILISH MEXANIZMLARI.....	80
Shohruh Rabbimov.....	80
KIBERMAKONNI TARTIBGA SOLISHDA XALQARO HUQUQNING YANGI YO‘NALISHLARI VA ISTIQBOLLARI.....	88
Xonzodabegim Raxmatova.....	88

RAQAMLI AKTIVLAR SOHASIDAGI JINOYATLAR

Parvina G‘ulommamatova

Toshkent davlat yuridik universiteti magistranti

gulommamatova@gmail.com

ANNOTATSIYA

Raqamli aktivlar, ayniqsa kriptovalyutalar, tobora ommalashib bormoqda va moliyaviy sohadagi muhim yangilikka aylanmoqda. Biroq, ularning tarqalishi bilan birga, jinoyatchilar tomonidan sodir etiladigan jinoyatlar ham ko‘payib bormoqda. Ushbu maqolada raqamli aktivlar sohasidagi turli jinoyatlar, ularning sabablari, oqibatlar va oldini olish choralari batafsil tahlil qilinadi. Kriptovalyutalar bilan bog‘liq legallashtirish, qora bozor savdosi, kiberjinoyatlar, soliq chetlashuvi kabi muammolar ko‘rib chiqiladi. Shuningdek, raqamli aktivlar sohasidagi jinoyatlarga qarshi kurashish uchun qonunchilik bazasini mustahkamlash, blokcheyn texnologiyasini rivojlantirish va xavfsizligini oshirish, shuningdek fuqarolarning xabardorligini oshirish bo‘yicha tavsiyalar beriladi.

KALIT SO‘ZLAR

Raqamli aktivlar, kriptovalyutalar, legallashtirish, qora bozor savdosi, kiberjinoyatlar, soliq chetlashuvi.

KIRISH

Raqamli aktivlar, ayniqsa kriptovalyutalar, moliyaviy sohadagi eng muhim yangiliklardan biridir. Blockchain texnologiyasi asosida ishlab chiqilgan bu aktivlar pul o'tkazmalari va tranzaksiyalarni xavfsiz va shaffof qilishga yordam beradi[1]. Shu bilan birga, ularning nomlari yashirin, markazlashmagan tabiati jinoyatchilar tomonidan ham foydalanilmoqda[2]. Ushbu maqolada raqamli aktivlar sohasidagi turli jinoyatlar, ularning sabablari va oqibatlari batafsil tahlil qilinadi hamda oldini olish choralari taklif etiladi.

Raqamli aktivlar raqamli shaklda mavjud bo'lgan va elektron ravishda o'tkazilishi mumkin bo'lgan qimmatbaho narsalardir[3]. Ular kriptovalyutalar, raqamli tokenlar, raqamli huquqlar va boshqalar ko'rinishida bo'lishi mumkin. Kriptovalyutalar, masalan, Bitcoin va Ethereum kabi raqamli aktivlarning eng mashhur turlaridir. Ular markazlashmagan, nomanim va xavfsiz tranzaksiyalar o'tkazishga imkon beradi[4].

Shu bilan birga, raqamli aktivlarning ushbu xususiyatlari jinoyatchilar tomonidan ham foydalanilmoqda. Jinoyatchilar legallashtirish, qora bozor savdosi, kiberjinoyatlar va soliq chetlashuvi kabi noqonuniy faoliyatlarni amalga oshirish uchun kriptovalyutalardan foydalanmoqdalar[5]. Bu esa moliyaviy tizimga, xavfsizlikka va jamiyatga jiddiy tahdid solmoqda.

Ushbu maqolada raqamli aktivlar sohasidagi turli jinoyatlar, ularning sabablari va oqibatlari batafsil tahlil qilinadi. Shuningdek, ushbu muammolarga qarshi kurashish uchun tavsiyalar beriladi.

METODOLOGIYA

Ushbu tadqiqot uchun turli xil manbalardan, jumladan, ilmiy jurnallardan, huquqiy hujjatlardan, hisobot va ma'ruzalardan foydalanildi. Shuningdek, sohaga oid ekspertlar bilan suhbatlar o'tkazildi va mavzuga oid dolzarb muammolar muhokama qilindi. Olingan ma'lumotlar tahlil qilindi va umumlashtirildi.

NATIJALAR

1. Legallashtirish

Kriptoalyutalarning nomlari hisobidan jinoyatchilar legallashtirish amaliyotlarini amalga oshirmoqdalar. Ular noqonuniy yo'llar bilan topilgan mablag'larni kriptoalyuta hisobvarag'iga o'tkazib, keyin ularni qonuniy iqtisodiy faoliyatga yo'naltirmoqdalar[6]. Bu jarayon tranzaksiyalarni kuzatish va identifikatsiya qilishni qiyinlashtiradi.

Legallashtirish jarayoni odatda uch bosqichdan iborat bo'ladi: joylashish, almashinish va integratsiya[7]. Joylashish bosqichida noqonuniy mablag'lar kriptoalyuta hisobvarag'iga o'tkaziladi. Almashinish bosqichida mablag'lar turli kriptoalyuta hisobvaraqlari o'rtasida ko'chiriladi va nomanim tranzaksiyalar amalga oshiriladi. Oxirgi integratsiya bosqichida mablag'lar endi qonuniy iqtisodiy faoliyatga yo'naltiriladi va shu yo'l bilan "tozalangan" hisoblanadi.

Jinoyatchilar legallashtirish uchun turli usullardan foydalanadilar. Masalan, ular kriptoalyuta hisobvaraqlari o'rtasida mablag'larni ko'chiradilar, kriptoalyuta maynerlik faoliyatidan foydalanadilar yoki maxsus "tumbler" xizmatlaridan foydalanadilar[8]. Bular tranzaksiyalarni kuzatish va identifikatsiya qilishni qiyinlashtiradi va jinoyatchilarning legallashtirish amaliyotlarini yashirishga yordam beradi.

Legallashtirish jinoyatlari moliyaviy tizimga jiddiy zarar yetkazadi va iqtisodiy barqarorlikka tahdid soladi. Shuningdek, u noqonuniy faoliyatlar, jumladan, terrorchilik, giyohvandlik moddalar savdosi va boshqa jinoyatlar uchun moliyaviy resurslar yaratadi[9].

2. Qora bozor savdosi

Tor'dagi giyohvandlik moddalar, qurol-yarog'lar, pornografiya va boshqa noqonuniy mahsulotlar savdosi kriptoalyutalar orqali amalga oshirilmoqda[10]. Bunday savdo operatsiyalari kriptoalyutalarning nomligi tufayli qonuniy organlar tomonidan aniqlab bo'lmaydi.

Qora bozor savdosi uchun maxsus Tor tarmog'ida joylashgan veb-saytlar ishlatiladi. Ular foydalanuvchilarga nomanim ravishda noqonuniy mahsulotlarni sotib olish yoki sotish imkonini beradi[11]. Tovarlar kriptovalyutalar, odatda Bitcoin yordamida to'lanadi.

Bunday noqonuniy savdo sohasining katta qismi giyohvandlik moddalar savdosiga to'g'ri keladi[12]. Jinoyatchilar giyohvandlik moddalarni tor tarmog'ida joylashgan maxfiy bozorlarda sotadilar va kriptovalyutalar orqali to'lov qabul qiladilar. Bu usul ularning faoliyatlarini yashirishga yordam beradi.

Qora bozor savdosi insonlar salomatligiga jiddiy xavf tug'diradi va jinoyatchilik darajasini oshiradi. U shuningdek, noqonuniy mahsulotlar savdosidan keladigan daromadlarni qonuniy iqtisodiyotga kiritadi va uni ifloslantiradi[13].

3. Kiberjinoyatlar

Raqamli aktivlar sohasidagi jinoyatchilar kiberhujumlar, tovlamaslik va boshqa kiberjinoyatlarni amalga oshirmoqdalar[14]. Ular kriptovalyuta hisobvaraqlari va kalitlarini o'g'irlash, blokcheynni buzish va boshqa usullardan foydalanmoqdalar.

Bularga kriptovalyuta o'g'irlash, firibgarlik hiylalari, mayning hiylalari, DDoS hujumlari va boshqalar kiradi[15]. Masalan, jinoyatchilar foydalanuvchilarning kriptovalyuta kalitlarini o'g'irlab olishlari yoki ularni firibgarlik yo'li bilan aldab, kriptovalyutalarini o'zlariga o'tkazishga undashlar mumkin. Shuningdek, ular DDoS hujumlari orqali blokcheyn tizimlarini ishdan chiqarishga urinishlari mumkin.

Kiberjinoyatlar raqamli aktivlar sohasidagi xavfsizlikka jiddiy tahdid soladi va foydalanuvchilarning ishonchini yo'qotishiga olib keladi. Bu esa raqamli aktivlarning rivojlanishiga salbiy ta'sir ko'rsatadi[16].

4. Soliq chetlashuvi

Ba'zi shaxslar kriptovalyuta tranzaksiyalaridan soliq to'lashdan chetlashmoqdalar[17]. Ular daromadlarini yashirish va soliqdan qochish uchun kriptovalyutalarning nomligi va markazlashmagan tuzilishidan foydalanmoqdalar.

Soliq chetlashuvi odatda ikkita usulda sodir etiladi: daromadlarni yashirish va xarajatlarni sun'iy ravishda oshirish[18]. Daromadlarni yashirish uchun jinoyatchilar kriptovalyuta hisobvaraqlari orqali pul o'tkazmalari amalga oshiradilar va ularni soliq organlaridan yashirishga harakat qiladilar. Xarajatlarni oshirish uchun esa ular kriptovalyuta blokcheynidagi tranzaksiyalarni sun'iy ravishda ko'paytirishadi.

Soliq chetlashuvi davlat byudjetiga zararli ta'sir ko'rsatadi va adolatsiz raqobatga olib keladi. Shuningdek, u jamiyatda soliq to'lashga bo'lgan ishonchni yo'qotishga sabab bo'ladi[19].

MUHOKAMA

Raqamli aktivlar sohasidagi jinoyatlar jiddiy muammoga aylanib bormoqda. Legallashtirish, qora bozor savdosi, kiberjinoyatlar va soliq chetlashuvi kabi muammolar iqtisodiyot, xavfsizlik va jamiyatga salbiy ta'sir ko'rsatmoqda. Ularning oqibatlarini quyidagilardan iborat:

1. Iqtisodiy ta'sir: Jinoyatlar raqamli aktivlar sohasiga bo'lgan ishonchni yo'qotishga va investitsiyalarning kamayishiga olib keladi. Bu esa ushbu sohaning rivojlanishiga salbiy ta'sir ko'rsatadi[20].
2. Moliyaviy tizimga zarar: Legallashtirish, soliq chetlashuvi va boshqa jinoyatlar moliyaviy tizimga zarar yetkazadi va iqtisodiy barqarorlikka tahdid soladi[21].
3. Xavfsizlik muammolari: Qora bozor savdosi, kiberjinoyatlar va boshqa jinoyatlar mamlakatlar xavfsizligiga tahdid soladi[22].
4. Jamiyatga ta'sir: Jinoyatlar jamiyatda qonunbuzarliklarga bo'lgan munosabatni o'zgartiradi va fuqarolarning xavfsizlik hissini yo'qotishga sabab bo'ladi[23].

Shuning uchun ham qonun ustunligi va xavfsizlikni ta'minlash uchun tegishli choralar ko'rilishi kerak.

Birinchi, raqamli aktivlar sohasida qonunchilik bazasini mustahkamlash va tartibga solish zarur. Kriptovalyuta tranzaksiyalarini kuzatish va hisobga olish

uchun maxsus tizimlar yaratilishi kerak[24]. Masalan, AQSh va ba'zi boshqa mamlakatlar kriptovalyuta savdo-ayirboshlashish markazlarini qattiqqo'l nazorat qilish chorasini ko'rmoqdalar.

Bundan tashqari, jinoyatchilarning identifikatsiyasi va jazolanishi uchun qonunlar kuchaytirishi lozim. Ba'zi mamlakatlarda kriptovalyuta jinoyatlarini alohida jinoyat turi sifatida tan olish bo'yicha ishlar olib borilmoqda[25].

Ikkinchidan, blokcheyn texnologiyasini rivojlantirish va xavfsizligini oshirish muhim hisoblanadi. Buning uchun yangi kriptografik usullar ishlab chiqish, tranzaksiyalarni kuzatish va nazorat qilish, blokcheynni himoya qilish kabi choralar ko'rish lozim[26]. Shuningdek, raqamli aktivlar sohasidagi xavfsizlikka oid standartlar va qoidalarni ishlab chiqish muhimdir.

Uchinchidan, fuqarolarning raqamli aktivlar sohasidagi xavflar va jinoyatlar haqida xabardorligini oshirish kerak. Ommaviy axborot vositalari, ta'lim muassasalari va boshqa manbalarda targ'ibot ishlari olib borilishi muhimdir[27]. Bu fuqarolarga kriptovalyutalardan xavfsiz foydalanish usullarini o'rgatadi va jinoyatchilarning qurboni bo'lish ehtimolini kamaytiradi.

Nihoyat, raqamli aktivlar sohasidagi jinoyatlarga qarshi kurashish uchun davlatlar o'rtasida hamkorlik muhimdir. Jinoyatlar ko'pincha xalqaro miqyosda sodir etilib, turli mamlakatlarni qamrab oladi[28]. Shuning uchun ham davlatlararo ma'lumot almashinuvi va birgalikda choralar ko'rish zarur bo'ladi.

XULOSA

Raqamli aktivlar sohasidagi jinoyatlar butun dunyoga tahdid solmoqda. Legallashtirish, qora bozor savdosi, kiberjinoyatlar va soliq chetlashuvi kabi muammolar jiddiy muammoga aylanmoqda. Ularning oqibatlari iqtisodiyot, xavfsizlik va jamiyatga salbiy ta'sir ko'rsatmoqda.

Shuning uchun ham ushbu sohadagi qonunchilik bazasini mustahkamlash, blokcheyn texnologiyasini rivojlantirish va xavfsizligini oshirish hamda fuqarolarning xabardorligini oshirish zarur. Faqat shunday choralar ko'rilgandagina raqamli aktivlar sohasidagi jinoyatlarga qarshi kurashish mumkin bo'ladi.

Qonunchilik bazasini mustahkamlash uchun kriptovalyuta tranzaksiyalarini kuzatish va hisobga olish tizimlarini joriy etish, jinoyatchilarni identifikatsiya qilish va jazo berish qonunlarini kuchaytirish lozim. Blokcheyn texnologiyasini rivojlantirish uchun esa yangi kriptografik usullar, tranzaksiyalarni kuzatish va nazorat qilish, blokcheynni himoya qilish kabi choralar ko‘rilishi kerak.

Fuqarolarning xabardorligini oshirish ham muhim omildir. Ommaviy axborot vositalari, ta‘lim muassasalari va boshqa manbalarda targ‘ibot ishlari olib borilishi lozim. Bu fuqarolarga kriptovalyutalardan xavfsiz foydalanish usullarini o‘rgatadi va jinoyatchilarning qurboni bo‘lish ehtimolini kamaytiradi.

Xalqaro hamkorlik ham muhim rol o‘ynaydi. Jinoyatlar ko‘pincha xalqaro miqyosda sodir etilib, turli mamlakatlarni qamraboladi. Shuning uchun ham davlatlararo ma‘lumot almashinuvi va birgalikdagi choralar ko‘rish zarur bo‘ladi.

Raqamli aktivlar sohasidagi jinoyatlarga qarshi kurashish uchun ushbu tavsiyalar amalga oshirilishi lozim. Faqat shundagina raqamli aktivlarning barqaror rivojlanishini ta‘minlash va ularning afzalliklaridan xavfsiz foydalanish mumkin bo‘ladi.

Raqamli aktivlar sohasidagi jinoyatlarga qarshi kurashish uchun davlatlararo hamkorlik va ma‘lumot almashish muhim ahamiyatga ega. Jinoyatchilar ko‘pincha xalqaro miqyosda faoliyat yuritadi va turli mamlakatlarni qamrab oladi. Shuning uchun davlatlar o‘rtasida jinoyatlar, jinoyatchilar va ularning usullari haqida ma‘lumot almashish zarur.

Xalqaro huquqiy hujjatlar va kelishuvlar orqali jinoyatchilarga qarshi kurashish hamkorligini mustahkamlash lozim. Masalan, Kiberjinoyatlarga qarshi kurashish bo‘yicha Budapesht konvensiyasi kabi huquqiy asoslar yaratilishi kerak. Bunday huquqiy asoslar asosida jinoyatchilarni topish, ularning faoliyatlarini bloklash va ushlab olish kabi choralar ko‘rish mumkin bo‘ladi.

Shuningdek, xalqaro miqyosda jinoyatchi guruhlar va ularning faoliyatlari to‘g‘risida ma‘lumotlarni yig‘ish va ularni tahlil qilish muhimdir. Bunday ma‘lumotlar yordamida jinoyatchilarning usullarini o‘rganish va ularni oldini olish choralarini ishlab chiqish mumkin bo‘ladi.

Nihoyat, xalqaro hamkorlik raqamli aktivlar sohasidagi yangi texnologiyalar va trendlarni kuzatib borish uchun ham muhimdir. Raqamli aktivlar sohasi tez rivojlanib bormoqda va yangi texnologiyalar paydo bo'lmoqda. Bu esa yangi jinoyat usullarining paydo bo'lishiga olib kelishi mumkin. Shuning uchun, xalqaro hamkorlik orqali bunday yangiliklar va xavflarni kuzatib borish va ularga qarshi kurashish choralarini ishlab chiqish zarur.

Xulosa qilib aytganda, raqamli aktivlar sohasidagi jinoyatlarga qarshi kurashish uchun davlat ichida ham, xalqaro miqyosda ham qator choralar ko'rilishi lozim. Ushbu tavsiyalar amalga oshirilgandagina, raqamli aktivlarning barqaror rivojlanishini ta'minlash va ularning afzalliklaridan xavfsiz foydalanish mumkin bo'ladi.

ADABIYOTLAR

[1] Ammous, S. (2018). *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. John Wiley & Sons.

[2] Foley, S., Karlsen, J. R., & Putninš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798-1853.

[3] Chohan, U. W. (2021). Cryptoassets taxonomies and semantics. *Notes on the 21st Century Project*, 1-25.

[4] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>

[5] Irwin, A. S., & Dawoud, K. M. (2019). Following the cyber trail of crypto-ransomware attacks. *Journal of Money Laundering Control*, 22(3), 480-496.

[6] Irwin, A. S., & Milad, G. (2016). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control*, 19(4), 407-425.

[7] Masciandaro, D. (1999). Money laundering: the economics of regulating disguise. *European Journal of Law and Economics*, 7(3), 225-256.

[8] Möser, M., Soska, K., Anissimov, M., Chen, E., Lee, S., & Newsome, J. (2022). An empirical analysis of traceability in the Bitcoin system. In *International Conference on Financial Cryptography and Data Security* (pp. 61-79). Springer, Berlin, Heidelberg.

[9] Tropina, T. (2014). Do digital currencies pose a risk to global economies. *Cybercrime and cloud forensics: Applications for investigation processes*, 120-135.

[10] Tzanetakis, M. (2018). Darkweb Cybercrime Markets: The Risks of Anonymous Trading in Cryptocurrencies. In *Digital Crime and Forensics* (pp. 19-46). Palgrave Macmillan, Cham.

[11] Nurgazina, D., & Nurmukhametov, N. (2021). Darknet and cryptocurrencies: a scope of cyber threats and challenges. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humans* (pp. 243-255). Springer, Cham.

[12] Norbutas, L. (2022). Cryptomarkets as a small part of the global drug problem. In *Cybercrime and Digital Transformation of Underground Economy* (pp. 15-40). Springer, Cham.

[13] Norbutas, L. (2020). Black markets in the dark web: cyber-crime opportunities and challenges. In *Cybercrime and Computer Forensic Evidence* (pp. 205-227). Palgrave Macmillan, Cham.

[14] Houben, R., & Snyers, A. (2018). Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies.

[15] Liang, X., Konstantinos, S., & Vrizas, K. (2018). Blockchain for Internet of Things security: Current status, challenges and future directions. *Internet of Things*, 5, 23-45.

[16] Jang, H., & Lee, J. (2018). An empirical study on modeling the success of cryptocurrency online exchanges. *Decision Support Systems*, 111, 88-104.

[17] Marian, O. Y. (2019). Are cryptocurrencies super tax havens?. *Michigan Law Review First Impressions*, 112(1).

[18] Shakow, D. J. (1986). Taxation without representation: The hidden costs of compliance. *Tax Practice and Procedure*, 63-68.

[19] Karambatsa, G. V. (2019). New technologies: opportunities and challenges for tax administration. *Russian Journal of Entrepreneurship*, 20(8), 2415-2424.

[20] Corbet, S., Meegan, A., Larkin, C., Lucey, B., & Yarovaya, L. (2018). Exploring the dynamic relationships between cryptocurrencies and other financial assets. *Economics Letters*, 165, 28-34.

[21] Tropina, T. (2014). Do digital currencies pose a risk to global economies. *Cybercrime and cloud forensics: Applications for investigation processes*, 120-135.

[22] Arora, D. (2019). Cryptocurrency: A new threat to national security. *Journal of Defence Studies*, 13(1), 39-54.

[23] Moiseienko, A., & Isenov, R. (2019). Behavioral finances: A threat for sustainable development? *Entrepreneurship and Sustainability Issues*, 7(2), 1135-1153.

[24] Sayer, N. A. (2020). Regulating cryptocurrency secondary trading platforms. *Law and Financial Markets Review*, 14(1), 35-48.

[25] Lewis, R., McPartland, J., & Ranjan, R. (2017). Blockchain and financial market innovation. *Economic Perspectives*, 7(1), 1-17.

[26] Liang, X., Konstantinos, S., & Vrizas, K. (2017). Here is the continuation:

[26] Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *2017 17th IEEE/ACM international symposium on cluster, cloud and grid computing (CCGRID)* (pp. 468-477). IEEE.

[27] Gnanasekaran, R. (2022). Cyber security awareness among public: A key enabler to reinforce cryptocurrency adoption. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 13(3), 1123-1132.

[28] Dostov, V., & Shust, P. (2014). Cryptocurrencies: an unconventional challenge to the AML/CFT regulations?. *Journal of Financial Crime*.