ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

SHADOW BANKING TO CYBER HAWALA: CRIMINOLOGICAL ANALYSIS OF UNREGULATED REMITTANCE CHANNELS AND AML ENFORCEMENT IN PAKISTAN

Adv. Attiya Shafaq Khan

attiyashafaqkhan@gmail.com)

Mahnoor

(Finance Department, Bank Alfalah)
Shiza Jamil
Tax Axis Consultants

ABSTRACT

Unregulated Informal Value Transfer Systems (IVTS) operating as trust-based hawala/hundi mechanisms, have undergone an intense structural development into cultured shadow banking. These networks function through borderless networks. In Pakistan, these digitized networks control peer-to-peer crypto-fiat supports, encoded messaging systems. These Fintech arbitrages are the practices where financial companies abuse gaps, delays, or differences in regulations, costs of capital, or market rules to gain an advantage over traditional banks. these digital shadow institutions Function in regulatory blind spots which enable capital flight, tax evasion, and illegal trade funding, evading conventional banking gaps. these practices pose serious threats to macroeconomic system of the state, foreign exchange assets, and money laundering frameworks. Routine Activity Theory, Rational Choice Theory, Strain/Anomie Theory and Techno-Criminology show the ways that criminal networks take advantage of differences between legal systems missing evidence in digital forensics and slow rules for old government systems. The paper finishes with a multi-step plan for making changes to fix this gap in how things are run and how they are regulated. This plan needs laws to be added to AMLA 10 FERA 16 and PECA 16 using computer programs to watch financial transactions better skills for digital forensics in government intelligence and better ways for the government and private companies to share financial information. At the end the study gives a plan for changing how Pakistan handles money laundering and terrorist financing taking back control over money transfers and following international rules from FATF all without harming real financial access, for people.

Keywords: *Cyber Hawala, Shadow Banking, Informal Value Transfer Systems (IVTS), Hawala/Hundi, Foreign Exchange Regulation Act 1947 (FERA), Anti-Money Laundering Act 2010 (AMLA), Financial Action Task Force (FATF), Federal Investigation Agency (FIA), Financial Monitoring Unit (FMU), Virtual Asset Service Providers, Peer-to-Peer Cryptocurrency, Trade-Based Money Laundering, State Bank of Pakistan (SBP).*

Background and Doctrinal Framework

The operational stability of Pakistan's financial system be governed by upon a strict legislative clash. The State Bank of Pakistan operates alongside a general economy under the Banking Companies Ordinance, 1962.Traditionally, this unceremonious sector relied heavily on non-bank financial mediators and traditional alternative remittance systems, primarily *hawala* and *hundi*. In south Asia formally *hawala* functioned through decentralized, trust-based networks of brokers who facilitated domestic and cross-border value transfers trade using under invoicing entirely bypassing formal clearing houses. The constitutional charter precisely prevents the use of other remittance mechanisms. The Foreign Exchange Regulation Act, 1947 (FERA) prohibits selling in foreign exchange payments outside of legal and authorized dealers or regulated banking networks. In order to bridge this gap between market demand and intransigence, the SBP implemented

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL

organizational adjustments in 2002. they subjected strict capital minimums and supervisory

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

oversight by compelling *hawaladars* to transition into regulated Exchange Companies Yet, the swift digitization of shadow banking has generated an aggressive change of this practice: "cyber *hawala*." This contemporary structure ties the outdated system of *hawala* with fresh fiscal expertise Unauthorized electronic money systems, coded peer-to-peer chat, and borderless virtual asset designs are how cyber hawala operates.

Network fusion creates legal loopholes. The SBPs Regulations, for Electronic Money Institutions regulate licensed wallets. The Prevention of Electronic Crimes Act, 2016 (PECA) tackles access and electronic fraud. Neither law adequately addresses decentralized systems. As a result, statutory definitions based on notions of deposits, currency or bank institutions find statutory definitions difficult to control dispersed digital networks. In dispersed networks economic value is transmitted without actual currency entering Pakistan's official banking channels.

Evolutionary Precedents and the Judicial Landscape

The way courts in Pakistan look at money transfers shows a change from being very strict about proof to focusing more on stopping bigger problems in the financial system. In the past when the police went after people who used hawala or hundi they mostly said these were violations of foreign exchange rules from 1947 or crimes handled by the FIA under a law from 1975. At first the higher courts wanted clear proof like actual money moving or written records to say someone was guilty. Because hawala works without paper and relies on trust it was hard to get that proof. This meant many people got off without being punished and the flow of money out of the country stayed unchecked. Then things changed after a new law came out in 2010 called the Anti-Money Laundering Act. This law along with rules from Pakistan's work with the Financial Action Task Force made courts see money transfers as part of bigger crimes like money laundering. The Supreme Court and High Courts started using rules to punish people who ran illegal money transfer services. They said even if there was no money moving around if the result was money leaving the country illegally or money being moved in a wrong way the person could still be punished. As hawala started using the internet to become hawala courts faced new problems. They now deal with evidence under an old law from 1984 and a new one from 2016. It is hard to prove who owns records stored on encrypted servers or to track how people use crypto wallets in online hawala deals. Also judges are trying to balance legal rules with the need to keep things running smoothly. They support the FIA taking action against money transfer services. They also warn that the law shouldn't be used too broadly to punish people who make the software or run the platforms if there is no clear rule saying they are breaking the law. Because there are no rules about what counts as an illegal account in the digital world different courts have different ways of handling cases. This creates confusion, between ways of dealing with money smuggling and new ways using the internet to move money.

Legislative Intent, Purpose, and Canons of Construction

I think understanding how the statutory framework applies to cyber hawala means looking at what lawmakers intended using two ways of thinking: purposive interpretation and strict text analysis. When we think about the purpose the main goal of Pakistan's banking and anti-money-laundering laws, FERA 1947, AMLA 2010 and the Anti-Terrorism Act, 1997 (ATA) is to protect the country's power its foreign-exchange reserves and the soundness of the financial system. Those

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL

who favor interpretation say Parliament made these laws to stop any illegal ways of moving money or using trade to launder money no matter what technology is used. In that view cyber hawala is simply a version of traditional hawala. That means words such as "money transmission" or "foreign exchange transaction" should be understood broadly to include token transfers, algorithmic ledger entries and peer-to-peer electronic offsets so that the law keeps working even as technology changes. On the hand modern text-based interpretation says that what the law means must come only from the words written in the statute. Texts warn that judges should not change laws to cover new digital things unless Parliament clearly changes the law. According to the rule *expressio unius est exclusio alterius*, if the law names one thing it usually leaves out the others the precise definitions of "banking transactions" and "authorized dealers" in FERA 1947 suggest that decentralized digital value transfers are not included. Also when people are charged with cyber hawala under AMLA 2010 or PECA 2016 the rule of lenity says that if the law is unclear the court must decide in favor of the person accused. Putting penalties on folks who work in the grey area of regulation like peer-to-peer digital asset traders without clear law definitions goes against the Constitution of Pakistan 1973 which protects fair notice and due process under Article 10A. Other rules that shape how the law is applied add more difficulty. The idea that laws do not automatically apply limits how much local regulators can control cyber hawala nodes that are hosted abroad unless the law says otherwise. Likewise, current administrative law rules say that regulators like the SBP and the Securities and Exchange Commission of Pakistan (SECP) must work inside the limits of the laws that give them power. Solving the problem of cyber hawala means finding a ground between the broad protective purpose of financial integrity laws and the tight limits set by textual interpretation, in Pakistani law.

Pakistani supreme court decisions have shaped four legal areas related to informal money transfer methods. In State through DG FIA v. Alif Rehman (2021 CLD 472 SC) the Supreme Court decided that people who run foreign exchange businesses without SBP permission under Sections 3A and 3AA of FERA cannot ask for the return of seized local money. Using powers under Article 187 of the Constitution the top court said that big amounts of cash not verified on premises create a strong sign that illegal Hawala or Hundi activities are happening. This level of proof was explained in Muhammad Rafique v. State (2022 PCrLJ 1234 LHC) where the Lahore High Court said that the prosecution has to show a link between the money taken and the act of trading money on purpose to avoid regular banks. In Ali Raza v. State (2019 CLD 1102 HCS) the High Court of Sindh said that people who are not allowed to trade cannot use trade rules for protection. Disputes between government groups were handled in Director General, FIA v. Kamran Iqbal (2016 SCMR 447 SC). The Supreme Court created the "nexus rule " saying that the FIA can take control of crimes only if there is a direct link to federal laws or the federal governments interests. In Directorate of I&I-FBR v. M/s Prime Traders (2020 PLD 601 SHC) the Sindh High Court canceled investigations into company tax issues saying that the FIA can't take over the special tax departments area by pretending to do general financial checks. Similarly, the Lahore High Court in M/s Associated Goods v. Federation of Pakistan (2022 PTD 1890 LHC) said that normal tax changes do not automatically mean fraud without following the law. The courts said that money laundering cases are separate in State v. Qamar Shahzad (Crl. Appeal No. S-79 of 2025 HCS). Syed Zulfiqar Ali v. State (Crl. Bail Application No. S-406 of 2021 SHC). The courts said that Section 3 of AMLA is a crime and the case under AMLA is not linked to other crimes. About bail in money transfer cases the Supreme Court said in State v. Muhammad Akram (2021 SCMR 1618 SC) and Tariq Bashir v. State (2021 SCMR 1025 SC) that normal rules of the Criminal Procedure Code apply, but courts

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL

must look at the big impact of illegal money networks. In Tariq Mehmood v. State (Crl. Bail Application No. 2388 Of 2023 HCS) and Naqash v. State (HCS Bail Orders 2020/2021) the Sindh High Court said that getting bail before or, after being arrested needs proof when bank records, digital records and account activity show fake transactions. The standard for how data's judged in court was created by the case of Ishtiaq Ahmad Mirza, v. Federation of Pakistan (PLD 2019 SC 675 / PLD 2020 SC 146). The Supreme Court made a list of twenty-one rules that decide how audio, video and electronic evidence may be used in a courtroom. The evidence must be handled carefully. These rules explain how evidence is removed and how the safety chain of evidence is maintained. These rules come from Article 164 of the Qanoon-e-Shahadat Order, 1984 and, from Section 43 of the Prevention of Electronic Crimes Act, PECA. The same rules also apply to Cyber Hawala cases. In those cases, evidence may be peer-to-peer crypto logs chat messages or digital banking records. All of these kinds of evidence must follow the rules in order to be accepted as valid in court.

Comparative Policy Metrics

Analyzing approaches shows different ways countries handle informal value transfers and virtual assets. Each country took a path with results that show what works and what doesn’t. In India the government made it mandatory for virtual asset service providers to register with FIU-IND. They also introduced a 30% tax on assets. This high tax rate and strict monitoring pushed trading volumes toward peer-to-peer platforms that do not follow local rules. This outcome shows that relying on taxes without offering market incentives can lead to more informal activity. The United Arab Emirates created the Virtual Assets Regulatory Authority or VARA. This agency set up a licensing system for virtual asset businesses. It also kept oversight on exchange houses. This approach helped reduce channels within the UAE. At the time it shifted regulatory pressure to nearby countries that act as financial corridors. The Philippines used a strategy. The central bank, BSP launched a sandbox. This allowed fintech companies to test services under supervision. The sandbox included firms and low-cost digital KYC systems for remittance corridors. As a result, formal remittance costs dropped below the 3% target set by the Sustainable Development Goals. This made people less dependent on hawala networks. Kenya built on its telecom infrastructure. M-Pesa became a tool for financial inclusion. The country introduced simplified tiered KYC processes for low-value transactions. This made formal financial services easier to use and much cheaper. The result was a shift, from domestic informal value transfers. People started using the system for everyday money movement.

Strategic Reform Roadmap

Addressing financial crimes and informal value transfer networks needs a complete change across macroeconomic, legislative, operational and judicial systems. Macroeconomic and Regulatory Realignment: Stopping the reasons that push people to use Cyber Hawala depends on the State Bank of Pakistan (SBP) managing foreign exchange rates in a way that matches the market. Keeping a difference of than one percent between the rates that banks use and the rates in the open market reduces the chances for people to take advantage of the difference and use informal ways to move money. At the time instead of banning things completely creating a new system for Virtual Asset Service Providers (VASPs) that is run by the Securities and Exchange Commission of Pakistan (SECP) and the State Bank of Pakistan (SBP) in line with FATF Recommendation 15

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL

makes a better place for digital assets. Allowing trusted companies to operate within areas where they can be watched helps bring peer-to-peer trading following the Travel Rule and crypto to fiat connections into the formal system.

Legislative Harmonization: Laws need to be updated to deal with ways of moving money digitally. Changing the Foreign Exchange Regulation Act (FERA) of 1947 and the Anti-Money Laundering Act (AMLA) of 2010 gives legal rules and punishments for Cyber Hawala, encrypted ledger transfers, algorithmic value shifts and peer-to-peer virtual asset pooling. Section 8 of the AMLA needs to be stronger so that it can freeze assets without needing a conviction and speed up taking back money that was stolen and is in accounts that are owned by others. Also connecting the Prevention of Electronic Crimes Act (PECA) of 2016 with the Qanoon-e-Shahadat Order of 1984 creates rules about the truth and how evidence from verified cryptographic hashes and block chain data can be used in court. Technological and Investigative Capacity: Operational work needs to use both skills and financial knowledge. Bringing together people from the Federal Investigation Agency's Cyber Crime Wing and the State Bank Circle to form Cyber-Financial Investigation Units (CFIUs) makes it better to take action. These units should have people who are trained in accounting and looking at block chain data. Giving police and other groups tools to track wallet groups, money moves and ways to move money between block chains helps them do their job better. A single place where the Financial Monitoring Unit (FMU) Federal Board of Revenue (FBR) SBP and FIA can all share information makes it easier to check Suspicious Transaction Reports (STRs) customs forms and fast banking transfers.

Judicial Reform and International Cooperation: Dealing with problems involving digital money needs special judges and faster ways to work with other countries. Making courts with fast tracks for cases related to AMLA, FERA and cyber-crime laws helps speed things up. Training by the Federal Judicial Academy on accounting, how to handle digital evidence and the rules from a court case called Ishtiaq Ahmad Mirza v. Federation of Pakistan helps judges understand complex financial evidence. Finally making it easier to get help from countries and setting up direct ways to share data with law enforcement, around the world digital asset exchanges and local regulators helps get digital evidence quickly and bring it back if it is needed. The shift from customary hawala and hundi practices to digital or transnational forms of Cyber Hawala represents a significant expansion in shadow banking. New technologies that including peer-to-peer cryptocurrency networks, encrypted messaging, and digitally benami payment engagements, permit assets to be move with remote and less terrestrial limits. These methods cause abuse of different jurisdictions and cause problems in procurement of digital evidence ultimately delaying the conventional law-enforcement responses. Although the Pakistani judiciary has strengthened the legal framework by recognizing money laundering as an independent offence it must evolve along fiscal regulating technologies. This will apply strict standards to digital evidence, regulatory and enforcement mechanisms. Relying primarily on the seizure of physical cash and traditional punitive measures is unlikely to be sufficient as these networks become increasingly digital. Cyber Hawala should therefore be understood as a technology-enabled socio-economic phenomenon rather than simply as an extension of traditional informal remittance systems. Addressing it effectively will require practical regulation of virtual asset service providers (VASPs), stronger digital-forensic capabilities, better coordination among relevant agencies, and policies that encourage the use of formal financial channels while protecting the stability and integrity of Pakistan's financial system.

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL
JALT

REFERENCES

Anti-Money Laundering Act, 2010 (Act No. VII of 2010), Gazette of Pakistan, Extraordinary.

Anti-Terrorism Act, 1997 (Act No. XXVII of 1997), Gazette of Pakistan, Extraordinary.

Foreign Exchange Regulation Act, 1947 (Act No. VII of 1947), Gazette of Pakistan, Extraordinary.

Income Tax Ordinance, 2001 (Ordinance No. XLIX of 2001), Gazette of Pakistan, Extraordinary.

National Accountability Ordinance, 1999 (Ordinance No. XVIII of 1999), Gazette of Pakistan, Extraordinary.

Prevention of Electronic Crimes Act, 2016 (Act No. XL of 2016), Gazette of Pakistan, Extraordinary.

Qanoon-e-Shahadat Order, 1984 (President's Order No. 10 of 1984), Gazette of Pakistan, Extraordinary.

State Bank of Pakistan. (2018). *Exchange Companies Manual and SBP Regulations on Foreign Exchange Transactions*. SBP Foreign Exchange Policy Department.

Director General, FIA v. Kamran Iqbal, 2016 SCMR 447 SC.

Ishtiaq Ahmad Mirza v. Federation of Pakistan, PLD 2019 SC 675 / PLD 2020 SC 146.

State through DG FIA v. Alif Rehman, 2021 CLD 472 SC.

State v. Muhammad Akram, 2021 SCMR 1618 SC.

Tariq Bashir v. State, 2021 SCMR 1025 SC.

Ali Raza v. State, 2019 CLD 1102 (HCS).

Directorate of I&I-FBR v. M/s Prime Traders, 2020 PLD 601 (SHC).

Muhammad Rafique v. State, 2022 PCrLJ 1234 (LHC).

M/s Associated Goods v. Federation of Pakistan, 2022 PTD 1890 LHC (W.P. No. 16567 of 2021).

Naqash v. State, High Court of Sindh (Bail Orders 2020/2021).

State v. Qamar Shahzad & Another, Crl. Appeal No. S-79 of 2025 (HCS).

Syed Zulfiqar Ali v. State, Crl. Bail Application No. S-406 of 2021 (SHC).

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL

Tariq Mehmood v. State, Crl. Bail Application No. 2388 of 2023 (HCS Bench Karachi).

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, 30(1), 47–87.

Aidoo, E. (2025). Dual-speed compliance in anti-money laundering regimes: Understanding sectoral disparities in international standard implementation. *Journal of Money Laundering Control*, 28(4), 512–529

Asia/Pacific Group on Money Laundering (APG). (2019). *Anti-Money Laundering and Counter-Terrorist Financing Measures – Pakistan, Mutual Evaluation Report*. APG Secretariat.

Carlisle, D. (2023). *The crypto launderers: Crime and crypto currencies from the Dark Web to DeFi and beyond*. Kogan Page.

Cassara, J. A. (2020). *Money laundering and illicit financial flows: Following the money and value trails*. Financial Sourcebooks.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608.

Cornish, D. B., & Clarke, R. V. (Eds.). (1986). *The reasoning criminal: Rational choice perspectives on offending*. Springer-Verlag.

De Koker, L., & Goldbarsht, D. (Eds.). (2024). *Financial crime, law and governance: Navigating challenges in different contexts*. Springer.

Ercanbrack, J. G. (2024). Differentiating hawala in criminal court: A transnational legal theory of informal financial exchange. *SOAS Law Working Paper Series*, 2(5), 1–28.

Financial Action Task Force (FATF). (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs)*. FATF/OECD.

Financial Action Task Force (FATF). (2021). *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. FATF/OECD.

Financial Monitoring Unit (FMU). (2022). *National Risk Assessment on Money Laundering and Terrorist Financing*. Government of Pakistan.

Hassan, M., & Ali, R. (2023). Cryptocurrency misuse and anti-money laundering compliance in emerging markets. *Journal of Financial Crime*, 30(3), 741–758.

Jasinski, D., Phillips, A., & Johnston, E. (Eds.). (2024). *Organised crime, financial crime, and criminal justice: Theoretical concepts and challenges*. Routledge.

ISSN E: 2709-8273
ISSN P:2709-8265
JOURNAL OF APPLIED LINGUISTICS AND TESOL

Longa, F. E. A. (2025). Cryptocurrency and money laundering: Typology, legal gaps, and systemic risk. *American Journal of Industrial and Business Management*, 15(2), 362–379.

Marzouk, M., & Hock, B. (2026). *Trade-based money laundering: Compliance and the law*. Routledge.

Meighan, S. (2026). *Money laundering and crypto-assets: A socio-technical approach to financial intelligence*. Springer Nature.

Messner, S. F., & Rosenfeld, R. (1994). *Crime and the American dream*. Wadsworth Publishing.

Passas, N. (2003). Hawala and other informal value transfer systems: How to regulate them? *Risk Management*, 5(2), 39–49.

Rehman, A., & Khan, S. (2025). Money laundering through crypto currencies in South Asia: Tracing and prevention mechanisms within the Pakistani jurisdiction. *Social Sciences & Humanity Research Review*, 3(3), 115–134.

State Bank of Pakistan (SBP). (2023). *Annual Report on the State of Pakistan's Economy: Remittance Regimes & Foreign Exchange Infrastructure*. SBP, Karachi.

Steinmetz, K. F., & Nobles, M. R. (Eds.). (2018). *Technocrime and criminological theory*. Routledge.

Sutherland, E. H. (1947). *Principles of Criminology* (4th ed.). J.B. Lippincott.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 22(6), 664–670.

Tiwari, M. (2026). *Money laundering, new technology and the law: The fight against financial crime*. Routledge.

Vlcek, W. (2018). Informal value transfer systems and the security-development nexus: De-risking and the financial exclusion of Hawala. *Global Networks*, 18(3), 421–439.

Widjaja, H., & Pratama, A. (2025). Cryptocurrency-based money laundering: Legal gaps and new threats in the digital financial world. *SHS Web of Conferences*, 221, Article 03008.