Advocates
Mediators
Arbitrators

Palladium
LEGAL

MUMBAI DELHI LONDON

Palladium Asset Freezing

Author: Harry Kenny, Clarb, IIMA, LLB
International Arbitrator & Mediator

| February 2025

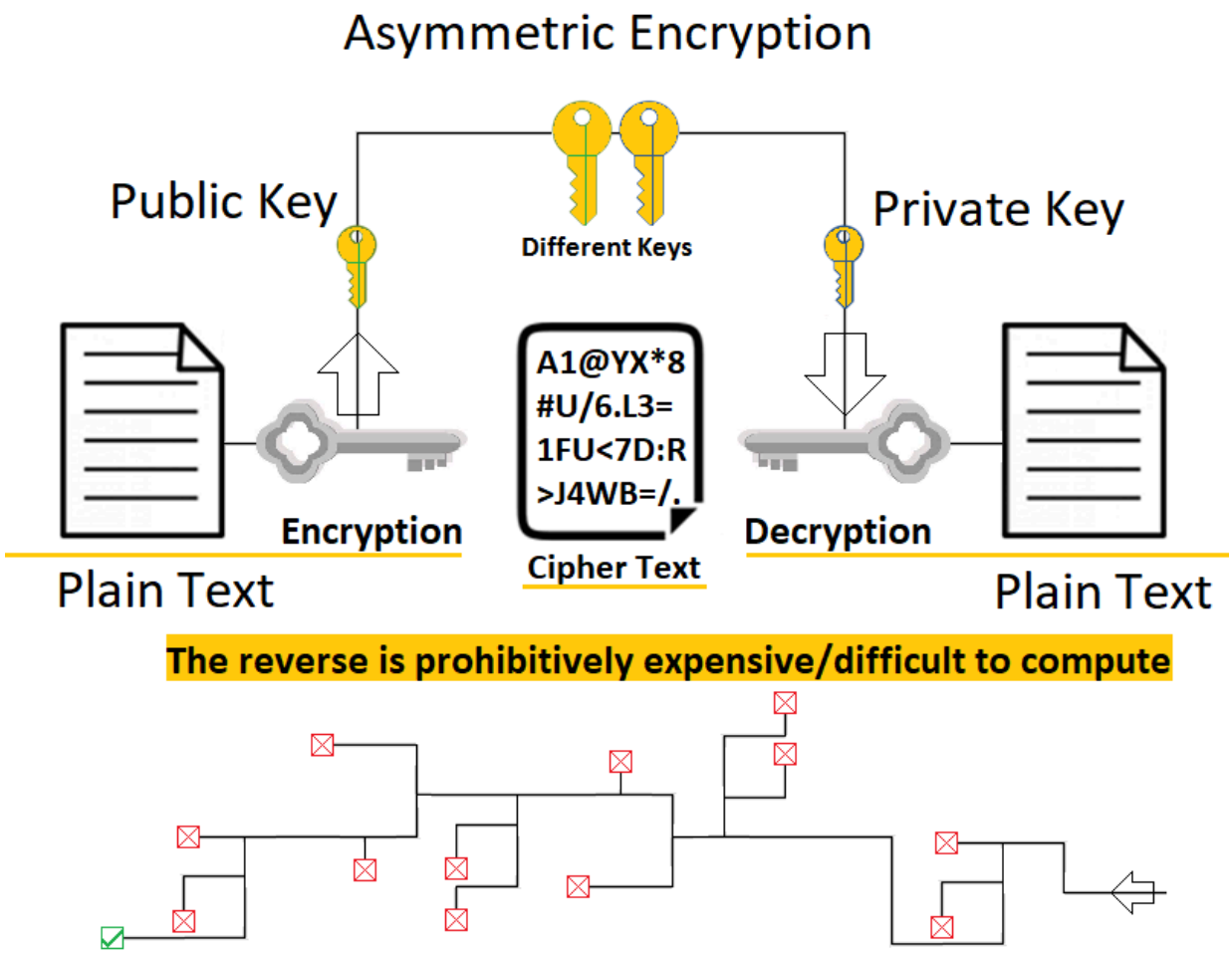
Outline

Cryptocurrency: Trust, Breach and Security

With the rise in use of crypto assets, typically Bitcoin, Ethereum and other virtual cryptocurrencies, with any contended assets cases comes the inevitable issue of capital flight. Vital considerations have been made across mainly family, commercial, trust, insolvency and tax law in this regard. It is becoming increasingly common to see these assets used as genuine stores of value to be contested over, as opposed to investment vehicle oddities in a portfolio. The advent of less and less traceable crypto assets had become the subject-matter of fierce, unprecedented and extensive debate regarding proper taxation and distribution for assets of any entity. Within the context of family law alone, for example one unearths serious doubts as to the equitable distribution of matrimonial assets in cases of divorce, maintenance funds and provision for furtherment of education. This article provides an abridged explanation of the blockchain, its uses, traceability issues, volatility depreciation concerns and remedies available to aggrieved parties. This includes legal analysis of the relative impotence of a worldwide proprietary or freezing order against certain crypto assets, and how one can protect oneself when conducting business dealings involving such assets.

Virtually all jurisdictions have now acknowledged these assets as decentralised digital currency, providing asset security through as yet unbreakable cryptographic hash functions or other deterministic puzzles. The majority of worthwhile cryptographic asset projects are stable or deflationary, and have a unique identity or utility that precludes them from being directly compared to any other form of investment activity or means to provide consideration to any client. The complexity and mathematical certainty of the functions inherent to each network transaction ensures secure electronic destination addresses, “wallets”, with unbreakable and certain means of trading, with blockchain or peer-to-peer verification of asset transfer, as opposed to mere trust in institutions.

This provides a certain outcome to transacting, as the combination of encryption, and ownership of private keys by each party to a contract, is impossible to circumvent in any traditional sense. Depending on the blockchain, an attacker hoping to interfere would find it likely more expensive than the value transferred, or completely impossible to decode before the transaction is complete, with many encryption methods requiring some of the most powerful computers in the world and several human lifetimes to break an unlike hash or symmetric encryption, key compromise only affects the party that has unfortunately suffered compromise of their key, allowing a lowered risk in transacting if one is confident in one’s own security measures.



Anyone who wants to send or receive cryptocurrency creates a “cryptographic key” — a file containing a random secret code — that can then be used to authorise transactions from their cryptocurrency wallets. If a bad actor gets access to that key, they instantly gain control of the cryptocurrency wallet as if they were the owner. That’s why it’s critical to protect your keys if you manage them yourself, as the human element is the only point of failure in such a system. Let us compare this to old-world physical guarantees, reliant on a legal guarantee between contracting parties and provided by a given legal system. In cases of breach, these are ministered to by auditors to provide facts to be decided or negotiated upon by courts or arbitrators within a chosen jurisdiction. It is impossible to deny that enforcement occurs on probability, contingent on a large element of chance when so many human-driven factors and potential points of failure are introduced. This can be aggravated when a certain party to proceedings has influence within a framework, which leads to unfair leanings or even judgements.

This is exemplified in history time and time again; ranging from everyday lies about solvency status going unquestioned to the detriment of creditors to an entity, to full blown Ponzi schemes, where active avoidance of objective truth about the nature of an scheme (which floats only on the reputation of those running it!) ruins lives, and trust in the system. When used as a means of transacting, rather than a mere investment vehicle, cryptocurrencies provide this same prophylaxis

against dishonesty to all users, no matter how small or disconnected from traditional financial systems they might be. After all, this reliance on cryptography is already a part of life, with reliance on the cryptographic guarantee against failure, if complex enough, offers encryption systems useful from messaging apps, to banking, to secure payments, when offered

Anybody with a phone or PC and internet connection can access deterministic truth when their assets are involved, rather than (in reductionist terms), simply trusting "someone" through a legal framework.

In obtaining injunctive relief or any other pecuniary remedy, one must first prove the law in a given jurisdiction recognises these assets as "property". As of the time of writing, only El Salvador provides a constitutional definition of a crypto asset or cryptocurrency. Other jurisdictions can only rely on a short and in many cases contradictory history of legal precedent and recently drafted regulation and statute, given the novel nature of this asset class. There is a marked absence of a true international consensus on a specific definition of "property", with the European Convention on Human Rights (ECHR) referring directly to "possessions" and "property" without defining these terms. By contrast, the Inter-American Court of Human Rights has directly attributed a definition of property to the IACHR Article 21 rights pertaining to property derived from The Case of the Mayagna (Sumo) Awas Tingni Community v. Nicaragua (August 31, 2001, Inter-Am. Ct. H.R., (Ser. C) No. 79 (2001)).

"Property can be defined as those material things which can be possessed, as well as any right which may be part of a person's patrimony; that concept includes all movables and immovables, corporal and incorporeal elements and any other intangible object capable of having value".

This general definition covers virtually all cryptocurrencies, but is of no help to those seeking remedy and serves only to protect the right of owners of these assets. Establishing a legal recourse in a given country at the moment can range from nigh impossible to quite feasible, depending solely on the extent of established or national jurisprudence in this area. Foreign jurisprudence can assist in developing the legal structures necessary in this space. With the UK's supreme court relying on foreign judgements in approximately a third of its cases, it is no stretch to imagine the same cooperation between similar legal systems accelerating the journey to proper redress for the wronged. Any legislature attempting to stem this exodus to virtual currency with restrictions, bans or turning a blind eye will find itself worse off and its citizens deprived of justice. Policies must be built around the philosophy and effect of the blockchain, as attempting to apply established precedent to these systems results in overwhelming incompatibility.

As an example, in England and Wales (the seat of proceedings and arbitration in a large percentage of international commercial contracts), HMRC considers cryptocurrency to be a taxable asset, with no specificity as to enforcement. When, exactly, can one define any tax liability having arisen (a "taxable event")? Should this be viewed in respect of realising the investment as part of any financial settlement, or simply when selling a crypto asset back to any major fiat currency? Do transfers between private wallets or exchanges matter? What if such transfers constitute attempts to

avoid lawful taxation or obligations, such as inheritance tax or spousal maintenance? The problem worsens when cryptocurrency mining in all its forms, or staking/liquidity provision, must be considered. A cryptocurrency as straightforward as Bitcoin is simple to regulate, and precedent is already well established. However myriad projects or tokens simply do not fit the formal criteria as to property laid out in National Provincial Bank v Ainsworth [1965] AC 1175 by Lord Wilberforce, being:

1. Definable,

2. Identifiable by third parties,

3. Capable in their nature of assumption by third parties, and

4. Having some degree of permanence.

Criterion 1 is satisfied as virtually all cryptocurrencies are definable, as most are self-perpetuating functions upheld by a network, immutable to change without consent of at least 51% of said network, not centrally controlled assets subject to change or increases in supply from a central authority .

Criterion 2 begins to separate the wheat from the chaff; defining currencies such as XMR (Monero) is possible, but not by third parties per se, as whilst a given transaction is still visible to all network users and viewers, they are completely anonymised, with wallets being impossible to trace to an individual by virtue of the network alone. In fact, the Internal Revenue Service of the US Government issued a bounty of $625,000 over 2 years ago for cracking this particular currency, which remains unclaimed. Such currencies can only realistically be acquired in large amounts via peer-to-peer transfers, requiring a pre-existing reason to transfer value, or via exchanges, making one point of traceability viable. However, once taken off this exchange and transferred through at least two more peers, no court can hope to enforce a freezing order, having no entity to serve proceedings upon.

Crypto assets by their very nature are capable of assumption by third parties, but not always openly so. With value kept secure behind private keys (remember, these are a mere string of numbers!), which may only be held in the human memory of the asset holder, any transaction of value will require the full cooperation of the asset holder if an exchange or other intermediary cannot be held liable. Trusts can be set up, sending these keys to *any* party with *any* trigger, including simply not accessing the funds for some time, without the involvement of any legal requirements to a trust, including the absence of any (human) trustee, executor, residual beneficiary or any other statutory formalities to a trust established in any jurisdiction.

The Ainsworth criteria—definability, identifiability, transferability, and permanence—continue to anchor judicial reasoning, even as courts confront the unique challenges posed by blockchain's decentralised architecture. In our first landmark case, Ruscoe v Cryptopia Ltd (in liquidation) [2020] NZHC 728, the doors to equitable interest in crypto assets were opened by the High Court of New Zealand, which held, that digital assets of a cryptocurrency exchange constituted "property" and (in

that case) were capable of being held on trust for account holders on that specific exchange. Recent decisions reflect a global convergence toward recognising cryptocurrencies as property. 3. In Tulip Trading Limited v. Bitcoin Association for BSV & Others [2023] EWCA Civ 83 (England and Wales), The Court of Appeal considered whether developers of blockchain networks owe fiduciary duties to users who have lost access to their cryptocurrency. While the court did not definitively rule on the existence of such duties, it acknowledged, obiter, that cryptoassets like Bitcoin could be treated as property under English law. This case highlights the evolving legal landscape concerning the responsibilities of those who maintain blockchain networks. In Blockchain Tech Pty Ltd [2024] VSC 690, Australia's Supreme Court of Victoria ruled that Bitcoin satisfies these criteria under bailment law, emphasising its immutable ledger and transactional finality. This aligns with England's landmark D'Aloia v Persons Unknown [2024] EWHC 2342 (Ch), where the High Court held that USD Tether (USDT) constitutes traceable property, enabling freezing orders against anonymised wallets. The fact that this was a fiat-pegged "stablecoin" may complicate matters when this precedent is deployed in more esoteric holding structures divergent from fiat curreny's characteristics, such as is widely seen with Decentralised Autonomous Organisations (DAOs). The court's reliance on blockchain analytics to pierce pseudonymity underscores a judicial willingness to adapt traditional remedies to digital assets, but this may be less feasible with DAOs.

Hong Kong's Re Gatecoin Limited (In Liquidation) [2023] HKCFI 914 and Chan Wing Yan v. JP-EX Crypto Asset Platform Ltd [2024] HKDC 1628 further cement this trend. The former recognised crypto assets as trust property in insolvency proceedings, while the latter affirmed that unauthorised transfers of USDT by exchanges trigger fiduciary duties, granting victims recourse akin to traditional breach of trust claims. These rulings complement Singapore's CLM v CLN [2022] SGHC 46, which endorsed the Commonwealth view of crypto's proprietary status, enabling courts to apply equitable principles like tracing and constructive trusts.

Even criminal law has evolved: in New York v. Armstead [2024], the court classified cryptocurrency theft as grand larceny, reinforcing its treatment as tangible property under penal statutes. Yet challenges persist with privacy-centric coins like Monero, where anonymised wallets and "burn functions" frustrate enforcement. As noted in your original analysis, the IRS's unclaimed bounty for cracking Monero's encryption epitomises the tension between cryptographic security and legal accountability.

"Burn functions", depending on their specific integration into a blockchain, allow virtually limitless plausible deniability regarding falsifying asset ownership attribution or value depreciation, but only on more recent and far less adopted tokens when compared with current market leaders. These functions have the effect of sending the assets to a wallet that nobody has or can have access to, or otherwise permanently remove them from circulation. They are not solely negative, however, and are used for myriad purposes, including controlling inflation on a given network or even reducing the power consumption of mining. "Proof of burn" mechanisms, effect an initial sacrifice of value having the result of upgrading a virtual mining machine of sorts, constituting a very promising direction for eco-friendly decentralised currencies, whilst still awarding early adopters willing to invest in potential return.

An ever-increasing regulatory concern of late given Bitcoin's outdated version of a "proof of work" system, which requires increasingly powerful computers and more electricity to generate new tokens as time goes on, with the consequence of increased cooling requirements further raising the bar to entry for any would-be miner. This is due to the increasingly complex mathematical problems that must be solved in exchange for value, as well as to uphold the network by validating transactions. This has led to small-scale electricity theft from public grids all the way to pre-ban industrial-scale mining facilities in China and elsewhere, powered mostly by coal power plants, and putting tremendous additional pressure on the market for high-end graphics processing units, run by a 2-company (AMD and NVIDIA) worldwide oligopoly, in the process. It is foolish to attempt to exclude the possibility of development and eventual requirement for regulation over any novel or increasingly adopted existing consensus ("proof of x") mechanisms governing token issuance. If someone tampers with a transaction recorded in a bitcoin blockchain block, for example, it alters the digital signature and unlinks that block, with these consensus mechanisms governing data that can be recorded the shared, final ledger. Newer solutions to authenticating users include "proof of stake" and the similar "proof of authority", with countless other examples to fix specific problems with utility projects, such as "proof of humanity", "proof of coverage" and Thankfully, those tokens non-compliant with this definition of property have not been subject to proceedings yet, but it is a matter of time, and the law will need to recognise the huge benefits and carbon savings afforded by such measures alongside their risks to traceability.

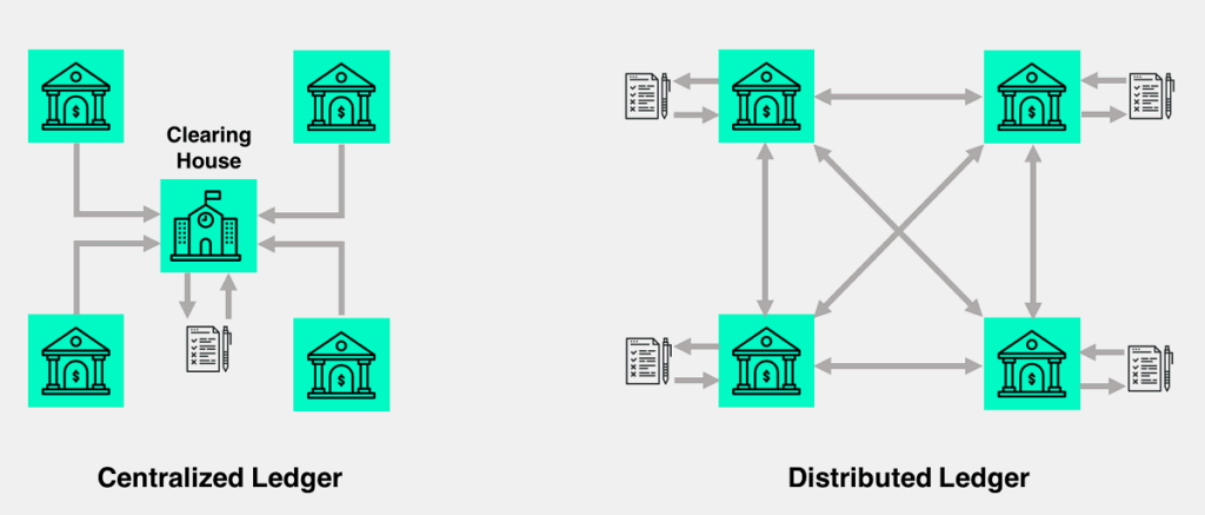
Now we at least have a solid basis for arguing that the majority of these assets, including virtually all common or retail tokens owned by a layperson and purchased through an exchange, meet the required qualities to constitute "property" under English law. We must move on to the practical concerns of whom to serve proceedings to, as injunctions such as Mareva injunctions are internationally applicable and famously well-enforced. After all, cryptocurrency wallets merely bear resemblance to bank accounts insofar as they are stores of value, and diverge greatly in function and definition beyond this point.Because they are held across a distributed ledger of asset holders in a self-sustaining and decentralised network, there is no immediately obvious party on whom to serve proceedings.

The law always has the starting point of the thief or wrongdoer, however associates, abetters or enablers and a varying degree of dishonesty or guilt in such associated parties seriously muddies the waters. In Robertson v Persons Unknown, Moulder J relied upon an analysis provided by a specialist company similar to the aforementioned Chainalysis. This analysis traced 80 Bitcoin to a wallet/account/address held by Coinbase.[1] More recently, in D'Aloia (2024), exchanges were also compelled to disclose wallet data. A given wrongdoing respondent must make disclosure, but how should this be sought from an anonymised wallet? The standard form for a worldwide freezing order mandated that the respondent provide information as to the "value, location and details of all such assets". As stated above, the defining nature of a distributed ledger[2] is the dispersed nature of assets as part of normal system operation. Ascertaining those in possession of a private key to the asset concerned, and tracing any third-party transfers outside exchanges requires discovery of the

1

2

transaction code or hash by which the coins were wrongfully acquired[3], which only becomes more difficult with more users on a network, or with newer networks that, by accident or design, obfuscate such codes so far that successfully tracing becomes impossible, or at least more expensive than the value of the assets in seeking to be recovered.



In the context of private international law, which focuses on tangible goods, it is prescribed that establishment of rights or entitlement should be governed by the law of that location in which the property or claim to property is found; the lex situs.[4]

The concept of a single situated store of value for the asset, not even physical, let alone geographical, simply cannot apply to such digitised assets or assets constituted on a distributed block chain or network. One naturally must ask the question of jurisdiction, therefore, as how can a law govern the exercise of seeking to trace and recover the crypto asset, when said asset cannot be linked to any jurisdiction, or linked to many if passing through different exchanges?[5] A network can span the breadth of several jurisdictions, legal frameworks and even national stabilities without risk to asset integrity and, in the case of fully decentralised ledgers, there is no central authority or validation point. It may be problematic to continue to rely on the doctrine of lex situs, with a choice of law rule or lex fori being used in preference, in cases where adequate remedy can be found through tracing or restitution alone.[6]

An elective situs could be an elegant and equitable solution to disputes or conflicts of law with regard to these tokens. Tokens such as PNK (on the Kleros network) requires established proof of humanity before joining the ranks of decentralised jurors upholding the system and involves complex game theory to ensure the most reasonable decision is made, discouraging participants seeking a rapid pay out and eliminating cognitive biases through the appeals process. Whether the question at hand is distribution of available evidence to jurors via blockchain, or pre-settlement

3
4
5
6

arbitration to save the time and costs associated with court (as is practised widely already through in-person arbitration), or elective identification of appropriate situs for the facts at hand.

In regulatory frameworks we have seen a slow move from fragmentation to cohesion, dissected in the following jurisdiction-specific sections.

In October 2020, the U.S. Department of Justice (DOJ) released the "Cryptocurrency Enforcement Framework," which outlines the risks associated with cryptocurrency and the strategies employed to combat illicit activities. The framework emphasises that while the DOJ supports the advancement of legitimate cryptocurrency technologies, it will enforce laws to protect the public from misuse.
The Securities and Exchange Commission (SEC) has been active in regulating cryptocurrency exchanges. In June 2023, the SEC filed charges against major exchanges like Binance and Coinbase for operating without proper registration and mishandling customer funds. These actions highlight the SEC's stance on enforcing securities laws within the crypto industry.
In February 2025, the SEC formed a bipartisan working group to develop policies favouring the growth of digital assets, aiming to provide clarity on a regulatory framework for cryptocurrencies.

The EU has implemented the Markets in Crypto-Assets (MiCA) regulation, which provides a comprehensive framework for crypto-assets, covering issuance, trading, and custody. MiCA aims to protect consumers and ensure financial stability by imposing requirements on crypto-asset service providers, including the need for authorisation and adherence to transparency and governance standards. MiCA came into full effect in December 2024, marking a significant step in unifying crypto regulations across EU member states.

The UK has been progressively developing its regulatory framework for cryptocurrencies, aiming to balance innovation with consumer protection and financial stability.
Regulatory Developments: In September 2024, the UK government introduced the Property (Digital Assets etc) Bill, which, for the first time, recognised digital holdings, including cryptocurrencies and non-fungible tokens (NFTs), as personal property under the law. This legislation aims to provide greater legal protection to crypto asset owners.
Financial Conduct Authority (FCA) Oversight: The FCA has been proactive in regulating the crypto sector. In August 2022, it granted registration to Crypto.com as a crypto asset service provider, indicating a move towards formalising the operations of crypto firms within the UK.
Future Roadmap: In October 2023, the FCA outlined a roadmap for cryptocurrency regulation, with comprehensive rules expected to come into force by 2026. The focus is on creating a regime that ensures fair, transparent, and efficient trading, while considering the unique characteristics of crypto assets.
India's approach to cryptocurrency regulation has been cautious, with significant developments in recent years.

Taxation and Compliance: In 2024, the Indian government imposed a 30% tax on income generated from the transfer of cryptocurrencies, along with a 1% tax deducted at source (TDS) on transactions

above ₹50,000. These measures aim to formalise the market and generate revenue, while discouraging tax evasion.

Regulatory Reassessment: As of February 2025, India is reassessing its cryptocurrency stance due to evolving global perspectives, particularly influenced by recent crypto-friendly policy announcements in the United States. This re-evaluation may delay the release of a discussion paper on cryptocurrencies initially scheduled for September 2024.
Market Adoption: Despite stringent regulations and high trading taxes, India has led the global adoption of cryptocurrencies for the second consecutive year, as reported in September 2024. This indicates a robust interest and participation in the crypto market among Indian investors.

The United Arab Emirates (UAE) has established itself as a world-leading progressive hub for cryptocurrency and blockchain technology, implementing a comprehensive regulatory framework to foster innovation while ensuring consumer protection and financial stability.
In 2022, Dubai enacted Law No. (4) of 2022, establishing the Virtual Assets Regulatory Authority (VARA) to oversee virtual asset activities within the emirate. VARA's mandate includes licensing and regulating virtual asset service providers (VASPs), ensuring compliance with anti-money laundering (AML) and counter-terrorist financing (CTF) standards. At the federal level, the Securities and Commodities Authority (SCA) has collaborated with VARA to create a unified supervisory framework for VASPs. This framework mandates that firms operating in or from Dubai obtain a license from VARA, which concurrently provides registration with the SCA, enabling them to offer services across the UAE.

The Central Bank of the UAE (CBUAE) has been proactive in integrating digital assets into the financial ecosystem. In 2024, the CBUAE approved the Payment Token Services Regulation, establishing a comprehensive framework for licensing and supervising digital payment services, including the issuance and management of stablecoins. Additionally, the CBUAE has initiated its Central Bank Digital Currency (CBDC) strategy, aiming to explore the feasibility of a digital dirham for domestic and cross-border payments, thereby enhancing the efficiency and resilience of the payment infrastructure.
The UAE's financial free zones have also developed tailored regulatory frameworks for digital assets: Abu Dhabi Global Market (ADGM): ADGM has implemented a comprehensive regime for digital assets, providing clear guidelines for the issuance, custody, and trading of cryptocurrencies. This framework has attracted numerous crypto firms to establish operations within the free zone. Dubai International Financial Centre (DIFC): The Dubai Financial Services Authority (DFSA) within the DIFC has introduced the Crypto Token Regime, regulating the offering, issuance, and trading of crypto tokens. The regime includes provisions to protect retail clients and ensure market integrity. The UAE's favorable regulatory environment has attracted significant industry players: Standard Chartered has commenced offering digital asset custody services in the UAE, citing the country's balanced approach to digital asset adoption and regulation. Tether announced plans to launch a stablecoin pegged to the UAE dirham, reflecting the growing demand for Gulf currency-backed

digital assets. Brevan Howard has established a significant portion of its crypto trading operations in the UAE, attributing this move to the country's sensible and supportive regulatory framework.

Finally, from an international perspective, The Financial Action Task Force (FATF) has expanded its recommendations to include virtual assets and service providers, urging member countries to regulate these entities under anti-money laundering (AML) and counter-terrorist financing (CFT) frameworks. The FATF's guidance includes the "Travel Rule," requiring virtual asset service providers to collect and share information about the originators and beneficiaries of virtual asset transfers.

The 2020–2024 period has seen remarkable progress. Courts now routinely apply property law to crypto, regulators enforce cross-border AML standards, and legislatures codify digital asset rights. However, tensions persist between decentralisation and accountability. As the Tulip Trading case illustrates, unresolved questions about blockchain developers' liabilities and the environmental costs of consensus mechanisms (e.g., proof-of-work vs. proof-of-stake) demand ongoing dialogue.

Over-reliance on state actors to litigate disputes also fails to afford universal protection; edge-case justice in this area of law, especially with claims lower on the scale of severity or value, may be ironically saved by another cryptographic project, or the versatility of the blockchain itself. Given that those suffering petty debts are currently gravely under-served, these shifts might provide some long-overdue relief in the field of ADR, especially with many projects having mandatory dispute resolution clauses in their smart contracts, owing to wider enforceability under the New York convention.

Policymakers must continue integrating blockchain's technical realities into legal frameworks, ensuring remedies keep pace with innovation. The alternative—piecemeal or reactive regulation—risks stifling growth while failing to protect users. The path forward lies in harmonising global standards, leveraging tools like MiCA and the Cryptocurrency Enforcement Framework, and embracing judicial cooperation to uphold justice in a decentralised world.

Related Articles:

Hurdles of International Arbitration in India↗

For further information please visit contact us page on our website.:

www.palladium-legal.com/contacts/

