

---

# **DUE DILIGENCE IN THE ACQUISITION OF BLOCKCHAIN STARTUPS: LEGAL AND REGULATORY CHALLENGES IN INDIA**

---

Prerana Kumari, Amity University, Noida

## **ABSTRACT**

The growth of blockchain-based startups and cryptocurrency enterprises has reshaped how mergers and acquisitions are carried out. These companies function through distributed systems, token-driven models, self-executing contracts, and cross-border digital networks, which introduces significant legal complexity to their acquisition. Standard due diligence approaches, which were created for traditional businesses, often fall short when trying to uncover hidden risks in crypto-related deals. This paper looks at the legal and regulatory problems that come up when purchasing blockchain startups, with particular attention to the situation in India. It makes the case that a buyer must look into not just the corporate framework and financial statements, but also token categorization, smart contract reliability, cybersecurity vulnerabilities, regulatory adherence, tax liabilities, and anti-money laundering responsibilities. The paper also emphasises the importance of combined due diligence frameworks and specialised contractual safeguards to minimise risks after the acquisition.

## **Introduction**

Blockchain technology and digital currencies have given rise to a new class of business entities that do not easily fit within traditional corporate legal structures. A blockchain startup might operate as a trading platform, a digital wallet service, a token issuer, a decentralised finance application, or a Web3 infrastructure provider. During an acquisition, such businesses attract buyers because of their innovative potential and growth prospects, but they also carry unusual legal uncertainties. Their operations may depend on decentralised decision-making, anonymous users, volatile digital holdings, and code-driven execution through smart contracts. These characteristics make legal due diligence considerably harder than it would be for an ordinary company.

In India, this difficulty is made worse by the lack of a comprehensive law that specifically governs cryptocurrencies. Instead, the legal landscape is shaped by a mix of court rulings, tax provisions, anti-money laundering requirements, and regulatory actions from bodies like the Reserve Bank of India, the Securities and Exchange Board of India, and the Ministry of Finance. Because of this piecemeal framework, buying a crypto business can expose the purchaser to liabilities that might not be discovered through conventional due diligence.

## **Why Conventional Due Diligence Falls Short**

Traditional due diligence concentrates on incorporation documents, ownership patterns, agreements, tax returns, outstanding liabilities, and litigation history. These matters remain relevant in crypto acquisitions, but they are not sufficient on their own. A blockchain startup may hold assets that are controlled through private cryptographic keys instead of through regular bank accounts. Its liabilities might arise from token issuances, flaws in smart contracts, or lapses in know-your-customer compliance. Its governance structure could be decentralised, with no single individual exercising clear authority. Its user base may be distributed across multiple jurisdictions, creating conflicts of law and enforcement difficulties.

For these reasons, due diligence for a blockchain startup must be carried out in an integrated manner. Legal, technical, financial, cybersecurity, and regulatory reviews need to happen together. If these reviews are conducted separately, important risks may stay hidden. For example, a token might look valuable on paper, but if the underlying smart contract contains a vulnerability, or if the token was issued in a way that could attract securities regulation, the

acquisition could become extremely risky.

### **Legal Characterisation of Crypto Assets**

One of the most significant questions in this area is how the law views the nature of cryptocurrency. Indian law has slowly moved toward acknowledging digital assets for tax and property-related purposes. The Income Tax Act treats virtual digital assets as taxable items, and the Madras High Court in *Rhuthikumari v. Zanmai Labs Private Limited* recognised cryptocurrency as property that can be owned, transferred, and protected through trust arrangements. These developments matter greatly in acquisition work because they mean that digital tokens cannot be treated as legally invisible. They may form part of the target company's assets, balance sheet, or custodial holdings.

At the same time, the law has not settled whether every token should be treated in the same way as property, a commodity, or a security. Some tokens might function like speculative investment instruments, which raises securities-law concerns. Others may be used as utilities or transactional tools. Still others may resemble commodities because of their trading characteristics in the market. This uncertainty creates a major due diligence obligation: the buyer must properly classify the token and examine the consequences that follow from that classification.

### **Regulatory Uncertainty in India**

India's regulatory environment for cryptocurrencies remains fragmented but is becoming more active. The Supreme Court's ruling in *Internet and Mobile Association of India v. Reserve Bank of India* struck down the RBI's circular that had restricted banking access, holding that the measure was disproportionate. That decision restored banking access for crypto businesses and confirmed that cryptocurrency trading is not illegal by itself under Indian law. Later, the government introduced specific tax provisions for virtual digital assets, including a flat tax regime and tax deduction at source. Additionally, anti-money laundering obligations were extended to virtual asset service providers, making exchanges and similar entities reporting entities under the Prevention of Money Laundering Act.

For a prospective buyer, these developments mean that the target's compliance history must be examined very carefully. The purchaser must verify tax filings, tax deducted at source records,

suspicious transaction reports, customer verification procedures, and any communications with regulators. Failures in any of these areas can create hidden liabilities that remain with the buyer after the deal closes.

### **Due Diligence Areas That Need Special Attention**

The discussion here shows that due diligence in blockchain acquisitions must extend well beyond ordinary checks. The first area is corporate and governance verification. This includes the certificate of incorporation, constitutional documents, shareholder agreements, board resolutions, and group structure. In crypto deals, it is especially important to identify whether token holdings, wallets, or intellectual property are held by subsidiaries, founders, or offshore entities.

The second area is contract review. Whitepapers, token sale documents, exchange listings, custody arrangements, developer agreements, and partnership contracts must be examined closely. These documents may contain promises made to token holders, revenue-sharing arrangements, or hidden obligations that affect valuation and post-acquisition risk.

The third area is regulatory compliance. The buyer must check anti-money laundering policies, know-your-customer practices, regulatory notices, tax filings, and licensing claims. In a crypto business, a compliance failure is rarely a minor issue. It may threaten the continuity of operations, attract penalties, or invite investigation.

The fourth area is litigation and dispute history. Claims brought by customers, regulators, business partners, or token holders may reveal systemic weaknesses. Because crypto businesses operate in a rapidly changing legal environment, disputes may arise from issues such as frozen wallets, failed transfers, exchange hacks, or investor complaints.

### **Technical Due Diligence and Smart Contracts**

A blockchain acquisition must also include technical scrutiny. Smart contract audits, code provenance, node architecture, wallet controls, and security history are essential. Unlike ordinary software, smart contracts can execute value transfers automatically and irreversibly. If the code contains flaws, the harm can happen immediately and be costly. A vulnerability in a smart contract can lead to unauthorised token creation, loss of funds, manipulation of governance, or a complete system failure.

That is why technical diligence must be translated into legal diligence. If the code has a known defect, the buyer must decide whether the target has disclosed it, fixed it, or taken out insurance against it. If a security audit exists, it must be reviewed in detail. If the target claims to be decentralised, the buyer must test whether that claim is genuine or merely formal. In many cases, admin keys, backdoors, or centralised control mechanisms remain hidden beneath the surface.

### **Transactional Protections**

Due diligence has practical value only when it influences the structure of the deal. In crypto acquisitions, the findings should directly inform representations and warranties, indemnities, escrow arrangements, purchase price adjustments, and closing conditions. For example, the seller should represent that it has good title to the tokens, that no undisclosed regulatory investigation is ongoing, and that smart contracts have been audited. If there are unresolved technical or legal risks, the buyer may insist on a holdback or a special indemnity.

This kind of transactional drafting is crucial because crypto assets are volatile and legally uncertain. A token may change sharply in value between the signing of the agreement and the closing of the deal. A regulatory inquiry may appear without warning. A smart contract vulnerability may only become apparent after an attack. Proper contractual allocation of risk is therefore just as important as the due diligence process itself.

### **Need for an Integrated Framework**

The main conclusion from this discussion is clear: blockchain acquisitions require an integrated due diligence framework. Legal, technical, financial, and regulatory reviews must work together. India's current legal environment, though developing, remains incomplete. The absence of a dedicated cryptocurrency statute means that buyers cannot rely on a single clear regulatory code. Instead, they must build a layered assessment strategy that examines token legality, tax exposure, anti-money laundering compliance, cybersecurity, and governance reality.

### **Conclusion**

The acquisition of blockchain startups presents unique challenges that conventional due diligence cannot fully address. Cryptocurrency businesses operate in a legal grey zone, shaped

by partial recognition, regulatory overlap, and technical complexity. Indian law now recognises important aspects of crypto activity through tax rules, anti-money laundering rules, and judicial decisions, but uncertainty continues around token classification, securities treatment, and the long-term regulatory structure.

For this reason, a purchaser of a blockchain startup must conduct a deeper and broader inquiry than would be necessary in a normal acquisition. The buyer must examine not only the company's records, but also its code, tokens, wallets, regulatory history, and compliance posture. Only then can the transaction be structured safely. The future of crypto M&A will depend on how well legal due diligence adapts to the realities of decentralised technology, and on how effectively Indian law develops to meet that challenge.