Transactions involving tokens or blockchains are different to typical corporate transactions in that they operate under different infrastructure and involve a different type of asset.

An investor to such a transaction should engage in due diligence prior to contracting and the unique risks merit a dual approach, focussing on both technical and regulatory factors.

Digital asset warranties should be included in transaction documents.

Crypto lawyers advise clients on these issues with the aim of preventing the misappropriation of their assets, mismanagement and poor governance.

This article outlines a proposed approach to the risks and the protections that are specific to corporate transactions involving tokens or blockchains and proposes warranties designed to protect buyers.

INTRODUCTION

Typically, a corporate acquisition transaction will involve the transfer of ownership of a company’s shares or assets (including its business or property) and the transaction will be recorded on a centralised database held by the company (its register of members) and, if shares are listed, on a centralised database of an intermediary (eg a bank or exchange). Conversely, where the corporate transaction is carried out on blockchain rails, the “thing” that is transferred will be a digital asset. Contracts attributable to the transaction will be executed through code and will be recorded on a decentralised ledger. Accordingly, the nature of such transactions is different; as such, they will attach different risks that should be considered when concluding the transaction documentation. The same goes for a corporate investment transaction (involving an issue of shares rather than a transfer of shares) and both an acquisition transaction and an investment transaction where assets of the target include tokens or tokenised financial instruments (in the latter case, to the extent that these instruments are native to a blockchain, rather than digital copies of traditional instruments). In each of these cases protections for the purchaser, through diligence and warranties, must take account of the nature of these assets.

(For the purposes of this article we do not engage in the argument that the time nature of a state change on a blockchain is the extinction and creation of a new asset – the commercial transaction that we are concerned with is a transfer or issue of an asset.)

What warranties are appropriate to a transaction of this nature? The answer is warranties that are directed at the underlying infrastructure and its use to where the true risks lie in such a transaction. This article will outline a proposed approach to the risks and the protections that are specific to corporate transactions involving tokens or blockchains and will propose warranties designed to protect buyers.

BACKGROUND

There are three main reasons why good practice as proposed in this article has not been followed in the market to date. First, many buyers of tokens have been specialist crypto investors that do their own diligence. Second, those buyers do not use lawyers because token issuance does not necessarily involve formal legal documentation; buyers simply connect their smart wallets and receive tokens under the terms of the smart contracts. Third, until this year demand always exceeded supply in new token issuances so Gresham’s law came to crypto and bad money drove out good. In 2023, more traditional investors are in the market, more corporate lawyers are involved and issuers have less bargaining power; therefore, the market is more institutional, more professional and more thorough in its analysis of legal and business issues.

We trust that it will be apparent from our notes below that a conventional M&A due diligence list and conventional share purchase agreement or investment agreement warranties are not sufficient for the job they need to do here.

The purpose of this article is therefore to propose an approach to suitable warranty protection that can be used as the basis of standard terms in corporate documents for digital asset transactions. We propose warranties to cover:

- technical risks;
- regulatory risks;
- service risks;
- policies required to be adopted by firms working with tokens;
- proof of reserves.

BODY 1: DILIGENCE ON TOKEN PROJECTS

Before a corporate transaction involving tokens or blockchains is conducted, an investor should carry out both technical and regulatory due diligence.

Technical due diligence includes evaluating the technology behind a project to determine its viability, security, scalability, and ability to meet its goals. The following are key areas to assess:

- **Code**: reviewing the source code to ensure it performs as intended, is secure, well-written, and free of vulnerabilities. This is work requiring collaboration between lawyers and coders (still, generally, two different people in practice).
Network: evaluating the network architecture to see if it is scalable and can handle expected usage levels;

Tokenomics: analysing the project’s token model to ensure it is fair, aligned with the project’s goals, and has sustainable incentives for the community;

Consensus mechanism: examining the consensus mechanism used by the project to determine its security, level of decentralisation, and resilience against attacks;

Development progress: reviewing the project’s development progress to see if it aligns with project roadmaps and timelines;

Security audits: checking if the project has undergone security audits and if any vulnerabilities were identified and fixed; and

Team and advisors: evaluating the experience and background of the project’s team and advisors to determine their ability to execute on the project’s vision.

Regulatory due diligence includes evaluating and assessing whether the project adheres to relevant laws and regulations in the jurisdictions where it operates, including those related to corporate finance, financial services, money transmission, information technology and consumer protection. The diligence process usually involves the following steps:

- review of the project’s tokenomics, including the project’s team and advisors to determine their ability to execute on the project’s vision.

Each of these topics, together with issues revealed in diligence, should be the subject of warranty protection in transaction documents.

Crypto lawyers are properly placed to understand the most prominent technical and regulatory risks in a project. Identifying and evaluating these risks requires an understanding of the infrastructure and economics behind the transaction. For example, recent court decisions in the US have made a distinction between “staking” products and “yield” products. Coinbase and Kraken operated products with some similarities in that they gave returns to customers. Differences in their mechanics meant that the Kraken product involving pooled funds was found to be a security, and therefore was not issued in compliance with the US Securities Act 1933. In the UK, the equivalent test relates to collective investment schemes. This is an important topic, not least because of the importance of staking to the economic model of the Ethereum system, taking into account the role of validators in that system. All these points will be familiar to an experienced crypto lawyer.

BODY 2: WARRANTIES

Corporate-style warranties elicit information and allocate risk. In addition to standard corporate warranties, we now use warranties covering the matters listed in the previous section on diligence and related matters. These include backward and forward-looking warranties:

- in relation to each of the technical risks, as appropriate based on the specifics of the project and the outputs from the diligence process;
- to have and maintain adequate procedures to prevent the target company (including directors and associated persons) from undertaking any conduct that would cause the target company to be in violation of sanctions directed towards digital asset activities;
- to obtain and disclose tax and accounting advice in respect of the likely treatment of any token in the jurisdiction of incorporation, as well as any material jurisdictions in which the project operates or tokens are held;
- that smart contracts are audited by a reputable third-party smart contract auditor, any defects or deficiencies identified in the smart contract code are remedied or addressed to the satisfaction of the investor and the investor is able to request further audits;
- to put in place and demonstrate compliance with a regulatory policy (that covers tokens and blockchains);
- to obtain, disclose and demonstrate compliance with advice on applicable consumer protection laws, relating to, for example, data security, personal data use and processing, online safety, gambling and security against hacks;
- to have advice on obligations relating to all regulatory licences and registrations and to obtain and disclose a copy of the analysis (jurisdiction by jurisdiction) to justify the licensing status of the business;
that the investor must consent before the target company can change its corporate structure, its tokenomics, its smart contracts or its wallets. (In particular, investor consent must be a pre-condition to any corporate entity becoming (or becoming operated by) a Decentralised Autonomous Organisation (DAO));

- to maintain policies relating to advertising and marketing, taking into account financial and advertising legislation;
- in relation to the basis on which the project will enter into partnerships, collaborations and strategic alliances;
- in relation to compliance with the project’s social obligations, as defined in the whitepaper or other description of the project.

These are based on a recent set of warranties in an investment transaction. They are not exhaustive and are adapted case by case. The technology, infrastructure and regulatory environment are novel, so the warranties are also novel.

BODY 3: SERVICE RISKS AND ASSOCIATED POLICIES AND PROCEDURES

In addition to technical and regulatory risks, there are matters specific to digital assets and crypto markets that should be managed. We split these into types of service risks and ways that they are dealt with (normally by way of a buyer reviewing the target’s policies). The ability to manage or influence risks, as opposed to merely identifying them is important to note. A token or blockchain developed and operated by a target is capable of (indirect) management by a buyer or investor. But a token or a blockchain in which a target is itself merely an investor may not be manageable to any significant degree. And even a developed and operated chain will become unmanageable if the project chooses to decentralise over time.

Service risks

Risks native to a digital asset service include those connected with:

- Price volatility: due to a combination of factors including lack of regulation, large market participants capable of price manipulation, fluctuations in demand and public perception, and limited liquidity in the market;
- Exchange risk: since centralised exchanges are prone to security breaches and hacking incidents which can result in the loss of funds. Decentralised exchanges offer more security through their decentralised structure but are subject to technical failures and smart contract vulnerabilities which result in the loss of funds;
- Custodian risk: due to the decentralised and largely unregulated nature of the technology and the fact that assets are stored in digital wallets, there is a risk of theft, loss or unauthorised access to the assets, as there is no central authority responsible for safeguarding them. Additionally, the lack of standardisation and interoperability between networks and platforms can lead to misunderstandings and mismanagement of assets;
- Liquidity risk: the market for these assets (that is, tokens that are not “blue chip”, namely BTC and ETH) is still relatively small and illiquid compared to traditional markets. This means that it can be difficult to buy or sell large amounts of these assets without significantly affecting the price;
- Criminal activities and fraud: digital assets are at risk of criminal activities and fraud due to the anonymity and decentralisation of transactions, lack of regulation, and potential for hacking or theft. Examples include phishing scams, Ponzi schemes (eg OneCoin, where the founder defrauded $5.8bn from investors and there was no coin at all)1 and hacking of exchanges or wallets (eg the Binance hack, where an unsecure smart contract allowed hackers to withdraw $570m from the exchange, or the Ronin Network hack, where the hacker stole $625m in ETH and USDC);2 and
- Operational changes: these include changes in technology, regulations or market conditions which can impact the functionality, security and value of digital assets. The market moves quickly and changes all the time, so it is important for all parties to stay informed of the latest developments and store assets on reliable platforms;
- Blockchain settlement risk: caused by slow transaction times and the possibility of network congestion or technical failures. These factors can lead to delays and increased transaction costs as well as potential losses. Additionally, the decentralised nature of blockchain technology means that there is no central authority to resolve disputes or reverse transactions;
- Concentration risk: caused by having a large portion of assets invested in a single currency or platform (for example, a trading fund that had a concentration of its funds on an account at FTX, although most large funds use multiple platforms) increasing the risk of financial loss in case of negative events such as market volatility, technological failures, or hacking incidents;
- Risks resulting from changes to or maintenance of software, eg ETH 2.0 “The Merge” – while this event occurred in 2022 and represented an “upgrade” in the code, it also created various risks that may affect Ethereum’s future functionality and integrity. For example:
- technical risks such as the possibility that a bad block may be produced, as well as the potential for errors to arise given the dual-layer operation of the validators and nodes;
- risks associated with “forks”, which represent a split in consensus, whereby one or more token holders will be granted identical tokens on separate blockchains. This creates uncertainty among token holders. Additionally, there is an increased risk of replay attacks; these occur where duplicate transactions are validated on different blockchains and, consequently, may facilitate the fraudulent transfer of assets;

Butterworths Journal of International Banking and Financial Law

April 2023

Page 245

WARRANTIES IN CORPORATE TRANSACTIONS INVOLVING TOKENS OR BLOCKCHAINS

Feature
general economic risks since miners may alter their activity, with such behavioural changes potentially implicating market participants, the price of ETH, and the blockchain’s hash rate itself. Additionally, the Ethereum blockchain remains subject to cyber security threats, many of which have not yet been identified; and

- **Smart contract risk**: caused by code vulnerabilities, misunderstandings in contract terms, and difficulty in updating or changing the contract. It is important to use reliable and audited smart contract templates or to seek professional assistance in creating custom smart contracts.

### Policies and procedures

Investors should require a target company to have and disclose policies to manage the service risks.¹ The policies and procedures should then be the subject of additional warranties, including in relation to:

- **The digital wallets of the target**, including lists of wallet addresses and information on contents: policies should address potential loss of a public key, a private key or a password and loss of funds – specifically including secure wallet solutions⁴ and guidance on best practices for storage and backup of private keys; regular security audits; user education; and an incident response plan;

- **Custodian service providers**: policies should address potential loss of funds due to hacks and halted withdrawals on exchanges and custodians – specifically including approved custodians or required technical standards for acceptable custodians; regular assessments of custodian security measures; and a contingency plan involving allocating funds to compensate affected users, working with the custodian to restore normal operations and conducting investigations to determine the cause of the incident;⁵

- **Smart contracts**: policies should address steps to deal with loss of funds or frozen funds due to a smart contract bug – specifically including measures that help to increase the stability and security of the smart contracts (such as regular auditing and testing of smart contracts); having a dedicated security team to monitor and address any vulnerabilities; implementing measures to limit the impact of bugs; and having clear communication channels to quickly address and resolve any incidents⁶;

- **Slashing**: policies should address steps to deal with misbehaving nodes during block validation and any process that leads to loss of staked funds – specifically including incentivisation of proper behaviour to maintain the network’s security and stakeholders’ protection by clearly defining and communicating the rules for proper behaviour; implementing a system for monitoring and detecting misbehaviour; having a mechanism for dispute resolution; and having a clear process for penalising and “slashing” the stake of misbehaving nodes⁷;

- **Risk management in relation to critical blockchain network infrastructure and providers** to ensure the integrity and stability of the network: policies should require multiple redundant systems to ensure network uptime; regular audit and testing of infrastructure; contingency plans for network failures; relationships with multiple providers to limit the dependence on a single point of failure; and a dedicated risk management team for the assessment and mitigation of emergencies⁸;

- **How decisions are made on design, supply, issuance, functionality, tokenomics and governance of digital assets issued by the target or any of its portfolio projects and underlying blockchain networks**: policies should identify a dedicated governance team to oversee and facilitate specific policies related to governance processes; involvement of relevant stakeholders; community polls and surveys; and a transparent mechanism for proposing and implementing changes, in each case, to ensure that the project remains aligned with its goals and values, adapts to the changing needs of the ecosystem, and remains accountable to its users and stakeholders. For example, many regulated funds have a policy of not voting their DAO governance tokens to reduce the risk of being found to be operating a project later found to be an unincorporated association with liability for operators (third party service providers can be engaged to vote tokens);

- **Software upgrades and other changes to protocols, perhaps made as a result of a governance vote by members of a DAO (to ensure that the project remains technologically up-to-date, adaptable, and maintains the network’s stability and security)**: policies should set out a clear process for proposing and implementing changes and a transparent mechanism for rolling out upgrades and changes. For example, in many projects roles are split between a development team that oversee technical aspects of upgrades and changes and a risk management team that assess and mitigate any potential risks;

- **Forks, bridges and airdrops**: policies should set out a clear process for proposing and evaluating risks inherent in these type of events in relation to blockchain protocols to which a company or project is exposed. For example, some projects establish a dedicated governance or community outreach team to oversee these processes with a mandate (for example) to ensure the security and stability of the network, promote interoperability and innovation, and foster community engagement and growth; and

- **Exploits (of bugs or oversights)**, hacks (taking advantage of flaws and loopholes in code) and exposure of user information; security protocols: policies should set out responsibility for monitoring and addressing potential vulnerabilities; implementing measures to limit the impact of exploits; communication channels to quickly address and resolve any incidents; and a process for reporting and investigating hacks. Security protocols should cover handling and storage of user information; security and stability of the network; integrity of the project; and overall asset owner protection.⁰
BODY 4: PROOF-OF-RESERVE WARRANTIES

Due diligence and disclosure is required to protect any assets held in custody by any third party. Many projects publish information but it is not all of the same type. For example, quarterly or monthly proof-of-reserve statements are not useful in relation to assets that can be traded by the billion in an instant. Proofs that provide information on assets but not liabilities are obviously flawed. Proofs that do not disclose related party control or trading positions are also flawed.

A proof-of-reserve mechanism verifies whether the entity holds sufficient assets to cover the totality of customer deposits; thus, the mechanism acts as an implied warranty to investors and customers of a project that it retains sufficient reserves to protect them on the occurrence of collapse or financial distress. The appropriate standard is a proof-of-reserve mechanism that is audited, autonomously, and in real time.

As a technical matter, proof-of-reserve mechanisms such as those offered by Chainlink – one of the leading decentralised blockchain oracle networks, having facilitated over $7trn worth of on-chain transactions – use “oracles” to enable autonomous auditing of collateral in real-time. A fundamental limitation of blockchain networks is an inability to fetch external data or send data to off-chain systems by itself. “Oracles” – nodes that connect blockchains to external systems – address this by enabling smart contracts to execute based upon inputs and outputs from the external sources. In other words, proof-of-reserve mechanisms backed by a decentralised network of oracles can provide smart contracts with data needed to calculate the true collateralisation of any on-chain asset backed by off-chain or cross-chain reserves. When such proof-of-reserve mechanisms are deployed for automated on-chain audits, investors and customers have a higher degree of transparency around asset collateralisation as well as real-time verifications of the reserves and liability ratio in an entity (such as one that runs a cryptocurrency exchange).

Chainlink proof-of-reserves are increasingly being used to help secure the minting, redeeming and burning of wrapped assets, whereby tokens are “wrapped up”, and their underlying value allows them to be used on another, non-native blockchain. An integration can be used to halt the minting, redeeming, and burning of wrapped tokens when Chainlink’s proof-of-reserves identifies that those wrapped tokens are undercollateralised. If the correct controls and parameters are applied, it would be technically impossible to run an undercollateralised fully on-chain business.

A short form of warranty on this point looks like this:

“The Target Company shall have and maintain in place an integration between it and [Chainlink] for the use of the Proof of Reserve function using automated audits based on cryptographic truth to verify and monitor the reserve assets that support the liquidity for the Cryptoasset Service provided by the Target Company.”

CONCLUSION

Warranties in corporate transactions involving tokens or blockchains have been unfit for purpose but that is changing. In this article we have set out a proposal for a foundational approach to the proper subject matter of buyer protections, most commonly achieved in contracts by way of warranty coverage.

The point here is that subject matter expertise in the underlying infrastructure and crypto market profile allows the lawyer advising on the deal to appropriately draft terms suited to protect a buyer in the same way that standard corporate equity warranties have been done in transactional corporate finance for many years.

The warranties are included alongside usual warranties in a share purchase agreement, investment agreement, SAFE (a simple agreement for future equity) or SAFT (a simple agreement for future tokens).

We start with standard text and adapt it to the particular project and circumstances. We work with clients and industry bodies. We would welcome comments and engagement from lawyers and digital asset experts in relation to this project. We can be reached at the email addresses above or at crypto@cms-cmno.com or idacwg.1@gmail.com.

Further Reading:
- The point of DAOs, and of crypto lawyers (2022) 11 JIBFL 739.
- Cryptographic tokens: three categories of personal property? (2023) 2 JIBFL 102.