BEYOND THE BREACH

THE EVOLVING LANDSCAPE OF CRYPTO ASSET SECURITY AND LITIGATION

Authored by: Phillippa Ellis (Principal Associate), Charlotte Dawes (Senior Associate) and Freya Piper (Trainee Solicitor) - Capital Law

Cryptocurrency has changed the financial landscape, providing new ways online transactions can occur. While digital assets are no longer ‘emerging’ and firmly here to stay, the UK is still developing a regulatory framework to cover the dynamic sector. The volatile ecosystem faces significant security risks, as evidenced by the recent data breach at WazirX, a major Indian cryptocurrency exchange. This incident is part of a troubling trend of sophisticated cyberattacks specifically targeting the crypto sector.

The Nature of Cryptocurrency

Cryptocurrency is a digital payment system that operates independently from banks to verify transactions. It functions as a peer-to-peer network, allowing individuals anywhere in the world to send and receive payments without the need for physical money.

Cryptocurrency exists solely as digital entries in an online database detailing specific transactions. These are recorded in a public ledger when cryptocurrency funds are transferred and stored in digital wallets.

The term “cryptocurrency” stems from the use of encryption to verify transactions, involving advanced coding to securely store and transmit data between wallets and public ledgers. This encryption aims to ensure security and safety. Much of the interest in cryptocurrencies comes from trading for profit, with speculators sometimes driving prices to extreme highs and also extreme lows.

In traditional financial systems, transactions are directly tied to the identities of the individuals involved. By contrast, cryptocurrency transactions are recorded on the blockchain with addresses that do not reveal the user’s identity. This pseudonymity enhances privacy but complicates regulatory compliance. While the transparency of blockchain allows for the tracing of transactions, linking these transactions to individuals poses an issue. This anonymity afforded often attracts criminal activities such as money laundering, tax evasion, and ransomware attacks. Regulatory bodies around the world are grappling with how to balance the benefits of cryptocurrency with the need to prevent its misuse. This tension between privacy and regulation is a core challenge facing the crypto industry.

What Was The Breach?

In June 2024, WazirX a large crypto platform experienced a data breach involving its multisig wallet. The company reported the breach compromised the personal information of millions of users. Hackers accessed sensitive data, including names, email addresses, and transaction details, exposing its users to the possibility of identity theft and financial fraud.

The breach was only detected after various users began reporting suspicious activity in their accounts. WazirX promptly investigated the reports and took steps to secure its systems, but in many cases damage had already been done.

The breach sent shockwaves through the crypto sphere as it showed the vulnerabilities that even major cryptocurrency exchanges face. Despite investing in advanced security measures, WazirX was unable to prevent the breach, causing many to raise questions about the adequacy of current security protocols in the crypto industry. The incident also highlighted the need for exchanges to not only focus on securing digital assets but also to protect user data comprehensively.

Recent Trends

The WazirX breach is not an isolated incident. It is part of a broader pattern of increasingly sophisticated cyberattacks targeting the crypto sector. In recent years, there have been numerous high-profile breaches that have resulted in significant financial losses and shaken user confidence.

An example of this type of activity is the 2019 attack on Binance, one of the world's largest cryptocurrency exchanges. The breach resulted in the loss of 7,000 bitcoins, worth approximately $40 million at the time. The attackers used a combination of phishing, viruses, and other techniques to gain access to user accounts and withdraw the funds.

These attacks are becoming more complex, often involving advanced tactics like social engineering, exploitation of vulnerabilities and insider threats. As the value and popularity of cryptocurrencies continue to rise, so too does cyber threats. This ongoing threat underscores the need for continuous improvement in security measures and practices within the crypto industry.

Possible Legal Implications

The anonymous nature of cryptocurrency presents significant legal challenges, particularly in the context of data protection and regulatory compliance. The WazirX breach highlights the tension between the need for user privacy and safeguarding sensitive information.

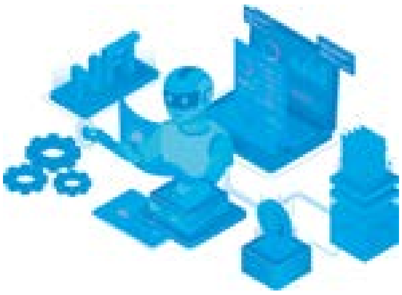
The General Data Protection Regulation (GDPR) mandates stringent data protection standards, including the requirement for companies to implement appropriate measures to secure personal data. Non-compliance can result in heavy fines and penalties. The very nature of cryptocurrency makes it difficult to align with such regulations, as the very structure of blockchain technology can conflict with GDPR requirements, such as the right to be forgotten.

In India, the legal landscape is still evolving. The Personal Data Protection Bill, which aims to regulate the processing of personal data, is yet to be enacted. The absence of comprehensive data protection legislation complicates the regulatory environment for cryptocurrency exchanges like WazirX.

It is likely this breach may accelerate efforts to establish more rigorous cybersecurity frameworks and data protection laws, balancing innovation with security.

There are significant challenges to litigation in cryptocurrency cases, but these are slowly being addressed. In the UK, courts have developed mechanisms for handling cases where the identity of a fraudster is unknown. Claims can be brought against "Persons Unknown," allowing proceedings to commence without identifying specific defendants. This is crucial in cryptocurrency cases, where the pseudonymous nature of transactions complicates identification. Courts categorise "Persons Unknown" into groups such as unauthorised accessors, knowing receivers, and innocent receivers of stolen assets, ensuring legal actions can target responsible parties while protecting those unintentionally involved.

Yet another layer of complexity is added by the global nature of cryptocurrency. Cyberattacks often involve individuals from multiple jurisdictions, making it challenging to coordinate legal responses and investigations. International cooperation and the development of standardised regulations are crucial to addressing these issues effectively. Furthermore the challenge of serving legal notices on unknown individuals from different jurisdictions has been addressed by UK courts allowing alternative approaches such as serving notices via email, through crypto exchanges, or even using Non-Fungible Tokens (NFTs) sent to fraudsters' wallets. This flexibility demonstrates the legal system's adaptability to the unique challenges of cryptocurrency fraud, particularly when dealing with cross-border jurisdiction and asset recovery.



The Way Forward

The WazirX data breach serves as a stark reminder of the vulnerabilities in the ever-evolving cryptocurrency industry. While digital currencies offer transformative potential, they also present significant security and regulatory challenges. As cyber threats become more prominent, it is imperative for organisations to bolster their defences and for policy makers to develop robust legal frameworks that protect users without preventing innovation.

The future of cryptocurrency depends on finding a balance between security, privacy, and regulatory compliance. As the industry develops, it must prioritise the protection of user data and the implementation of best practices in cybersecurity. Simultaneously, regulatory bodies must strive to create an environment that supports innovation while safeguarding users.