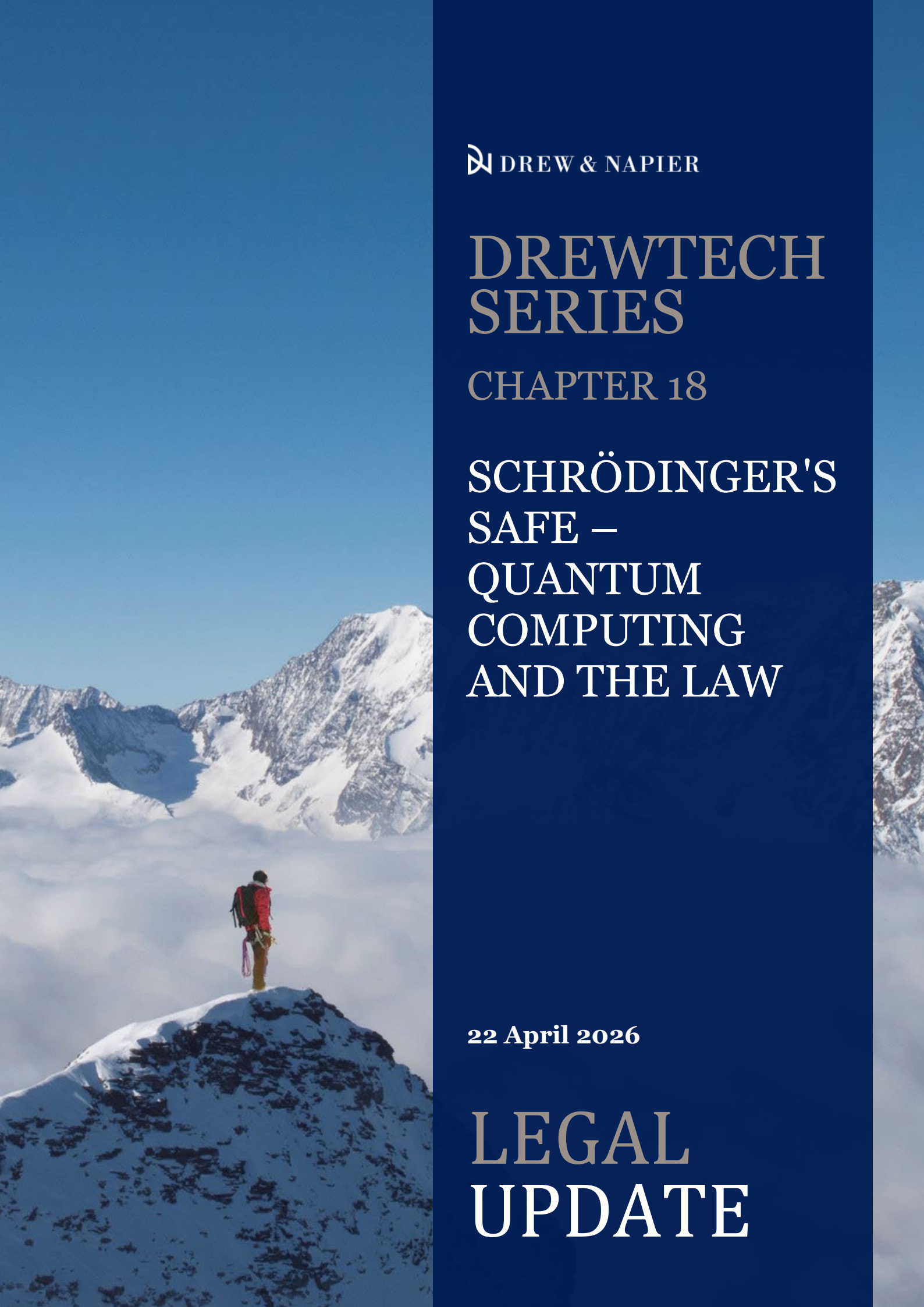




 DREW & NAPIER

DREWTECH SERIES

CHAPTER 18

SCHRÖDINGER'S SAFE – QUANTUM COMPUTING AND THE LAW

22 April 2026

LEGAL UPDATE

In this Update

Quantum computers promise extraordinary capabilities, but they also threaten the encryption that secures virtually every digital transaction. This article examines the legal implications of quantum computing, including “harvest now, decrypt later” attacks, emerging post-quantum cryptography standards, blockchain vulnerabilities, and practical steps organisations can take to quantum-proof their contracts

03
CATS, COINS, AND
COMPUTERS

04
HARVEST NOW, DECRYPT
LATER

05
NEW LOCKS FOR OLD
DOORS

05
CRACKING THE
BLOCKCHAIN

06
QUANTUM-PROOFING YOUR
CONTRACTS

06
CONCLUSION

Quantum computers exploit the strange rules of quantum mechanics to solve problems that would take today's best machines longer than the age of the universe. That sounds like a physics lecture, but the legal implications are already here: (a) Threat actors are harvesting encrypted data today in the hopes of decrypting it when quantum hardware matures; (b) International standards bodies have published the first post-quantum cryptography standards; and (c) Google has published research showing that cracking the cryptography protecting Bitcoin could require far fewer quantum resources than previously thought.

CATS, COINS, AND COMPUTERS

Every computer (and phone, smartwatch and now even a smart fridge) works by performing calculations. In classical computers, these calculations ultimately boil down to bits, which are the smallest unit of information. A bit can only exist in one of two states: 0 or 1, on or off, yes or no. A close example is a coin lying flat on a table, which can only have one side (heads or tails) facing up at once.

A quantum computer instead performs calculations using qubits, which can exist in both of these states simultaneously until you measure them. Think of a coin spinning in the air, which has neither heads nor tails facing up until it is caught. This unique property is called "superposition". Two other properties are unique to quantum computers. "Entanglement" links qubits so that measuring one instantly tells you something about other qubits, which allows quantum computers to process information in ways that have no parallel in classical computing. "Interference" allows quantum algorithms to cancel out wrong answers and reinforce right ones. Putting these three properties together gives you a machine that approaches problems in a fundamentally different way from a classical computer.

While quantum computing is still a nascent technology, it is already finding practical uses. For instance, in late 2025, HSBC used a quantum computer to improve bond trading predictions by 34%. Major global banks are also exploring quantum algorithms for option pricing, risk modelling, Monte Carlo simulations, and fraud detection. Beyond finance, the industries expected to benefit most include drug discovery, materials science, climate modelling, and logistics.

Quantum computing also has application in the AI space. It has the potential to speed the training of machine learning models, and AI-driven techniques are in turn being used to optimise quantum algorithms. For lawyers and policymakers, this raises familiar questions in unfamiliar territory: if a quantum-assisted algorithm generates losses or makes opaque decisions, how do existing risk management and AI governance frameworks apply? As we previously

observed in Chapter 4 of the DrewTech series: *"the idea of affixing liability onto the AI itself is an exercise in futility"* since AI has no legal personality. The same logic applies with even greater force to quantum-enhanced AI as a further level of apparent wizardry is added to the mix.

Quantum computers are not always better than classical computers. For everyday tasks, classical computers will remain perfectly adequate. But for certain computational problems involving very large numbers, complex simulations, or vast search spaces, quantum computers promise speed advantages that range from significant to incomprehensible. This matters for the law because one of those computational problems concerns the mathematics underlying modern encryption, which secures virtually every digital transaction.

HARVEST NOW, DECRYPT LATER

Modern encryption relies on mathematical problems that are difficult for classical computers to crack. While no quantum computer can quickly break common encryption methods today, bad actors can intercept and store encrypted data now, and wait until quantum hardware matures to decrypt it later. This strategy is known as "harvest now, decrypt later" ("**HNDL**"), and the threat it poses is ongoing.

However, the legal implications are immediate. Contractual and statutory obligations often require an organisation to take reasonable steps to protect confidential or personal data, and one aspect of this is whether an attack was foreseeable. This is directly relevant to Singapore's Personal Data Protection Act, which requires an organisation to make reasonable security arrangements to protect personal data. In light of the increasing wealth of research and warnings available on HNDL attacks, encrypted data which remains vulnerable to future quantum decryption may no longer meet the standard of reasonableness. The question is no longer just whether data was encrypted, but whether the encryption was sufficient given what was known about quantum threats at the time and the sensitivity of that information.

In 2025, the Cybersecurity Agency of Singapore ("**CSA**") released a Quantum-Safe Handbook and a Quantum Readiness Index to help organizations proactively assess their preparedness for the "quantum threat". While these do not create binding legal obligations at present, they may inform what courts and regulators consider to be reasonable security arrangements.

NEW LOCKS FOR OLD DOORS

Post-quantum cryptography refers to encryption methods designed to resist decryption from both classical and quantum computers. They run on today's classical computers and rely on different mathematical problems believed to be hard for quantum machines to solve. In August 2024, the US National Institute of Standards and Technology released the first three finalised post-quantum standards, with quantum-vulnerable algorithms to be deprecated under NIST's standards by 2035. These standards are already being adopted internationally and integrated into core internet protocols. Multiple governments have issued directives requiring transitions to quantum-resistant encryption by 2030.

While migration to post-quantum cryptography may be a multi-year endeavour for most organizations, the existence of published post-quantum cryptography standards today is already changing the calculus in respect of what regulators and courts could consider to be reasonable security arrangements. While the adoption of these standards may potentially be hamstrung by the increased computational requirements for post-quantum cryptography, organizations handling sensitive data with long shelf lives should assess whether to adopt these standards or take other preparatory steps now.

CRACKING THE BLOCKCHAIN

The blockchains underlying Bitcoin and Ethereum rely on a type of cryptography that a smaller quantum computer can break, and unlike traditional finance, they offer little to no recourse if a transfer is forged. Ethereum has set a 2029 target for post-quantum migration; and Bitcoin has no central authority to mandate a cryptographic upgrade (it must instead rely on decentralised consensus for changes to be made to the network which can be slow).

In March 2026, Google Quantum AI published a whitepaper demonstrating that breaking the cryptography protecting Bitcoin and Ethereum could require fewer than 500,000 physical qubits, which is a roughly 20-fold reduction from prior estimates. Google estimates a quantum machine could crack a Bitcoin private key in roughly nine minutes. This is significant because when someone sends Bitcoin, their public key is visible to the network for roughly 10 minutes before the transaction is confirmed, and an attacker who can derive the private key within that window could broadcast a fraudulent replacement transaction before the original settles. Even slower attacks could affect the roughly 6.9 million BTC which sits in wallets at heightened risk due to exposed or exposable public keys.

The DrewTech Series explored blockchain disputes in Chapter 9, "Of Blockchains and Stumbling Blocks." Those questions take on a new dimension here: if a quantum-forged signature drains a wallet, who is liable? The attacker is anonymous. The protocol developers built a system secure against classical computers. The wallet provider may not have offered quantum-resistant options. The network itself has no legal personality.

QUANTUM-PROOFING YOUR CONTRACTS

The situation is far from hopeless, and there are practical steps to help prevent your organisation from becoming a sitting duck in the post-classical computing world. First, organizations should conduct a cryptographic inventory to identify where encryption is used across their environment, using tools like the CSA's Quantum Readiness Index. Priority should go to data where long-term confidentiality is critical. Second, existing contracts that typically require "state-of-the-art" or "reasonable" security should be reviewed, as the emergence of post-quantum standards may already be shifting what those terms mean. Third, hybrid encryption combining classical and post-quantum algorithms should be tested early, since a new technology stack may be necessary to support future post-quantum encryption standards.

CONCLUSION

The message is not one of alarm, but of preparation. Organizations that begin assessing their exposure and reviewing their contracts now will be in a materially better position than those that wait for the first quantum-enabled breach to make headlines. As the DrewTech Series has observed across many chapters: the best time to plan for difficult eventualities is before they arrive, at a time when clear-headed parties are at peace. The quantum clock is ticking.

UPDATES IN DREWTECH SERIES

1. [Chapter 1: The Importance of an Exit Strategy in Technology Contracts <6 March 2019>](#)
2. [Chapter 2: Employees, Technology and A Legal Hangover – Bring Your Own Problems? <4 June 2019>](#)
3. [Chapter 3: I host, you post, I get sued? <24 September 2019>](#)
4. [Chapter 4: Diabolus ex machina <18 February 2020>](#)
5. [Chapter 5: Bringing hygiene online – the MAS notice on cyber hygiene <28 April 2020>](#)

6. Chapter 6: Signing without signing – contactless contracts <16 July 2020>
7. Chapter 7: My Kingdom for a Horse – When your Systems are Held to Ransom <22 January 2021>
8. Chapter 8: New risks in new skins – Updates to the Guidelines on Risk Management Practices – Technology Risk <3 March 2021>
9. Chapter 9: Of blockchains and stumbling blocks <21 July 2021>
10. Chapter 10: Service by airdrop – no parachutes required <7 July 2022>
11. Chapter 11: Large Language Models and Larger Legal Minefields <4 April 2023>
12. Chapter 12: Beset on all sides – liability for data breaches <19 July 2023>
13. Chapter 13: Pitfalls of user-generated content <18 October 2023>
14. Chapter 14: Red queen races – vulnerability disclosure programs <1 August 2024>
15. Chapter 15: Looking at the man in the middle (in a cyber breach) – allocation of risk <5 March 2025>
16. Chapter 16: Speak, Friend, and Enter - Access Controls and Authorised Users <28 May 2025>
17. Chapter 17: I love the smell of AI in the morning – a review of an AI-generated letter of demand <12 November 2025>
18. Chapter 18: Schrodinger's Safe – Quantum Computing and the Law <22 April 2026>

The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances. Copyright in this publication is owned by Drew & Napier LLC. This publication may not be reproduced or transmitted in any form or by any means, in whole or in part, without prior written approval

If you have any questions or comments on this article, please contact:



Rakesh Kirpalani

Director, Dispute Resolution &
Information Technology
Chief Technology Officer

T: +65 6531 2521

E: rakesh.kirpalani@drewnapier.com



Drew & Napier LLC

10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T: +65 6535 0733

T: +65 9726 0573 (After Hours)

F: +65 6535 4906