Submission to the Parliamentary Joint Committee on Law Enforcement

Inquiry into Combatting Crime as a Service

Title: Australian Crypto Crime as Entrepreneurship

Authors: Assoc. Prof. Darcy W. E. Allen
Dr Aaron M. Lane

Contact author: Assoc. Prof. Darcy W. E. Allen, [redacted]

Date: 13 October 2025

Dear Committee,

We thank you for the opportunity to contribute to this *Inquiry into Combating Crime as a Service*. From 2017 to 2019, this same Committee inquired into the *Impact of New and Emerging Information and Communication Technology* for law enforcement, with the final report directly referencing the rise of cryptocurrencies and the challenges that they create.[1] The impact of frontier technologies on how criminals operate is even more salient today. Indeed, the findings of your current Inquiry will be timely in the context of the rapid evolution of not just cryptocurrencies, but more broadly including advanced cryptography and artificial intelligence.

We make our submission as academics, practitioners and policy experts. We have spent over a decade researching, lecturing and engaging with technology, including the institutional, legal and regulatory implications of innovation.[2] Our submission draws on two key pieces of research:

- Allen, D.W.E. and Lane, A.M. (forthcoming) "Crypto Crime as Criminal Entrepreneurship", In L. Robb and J. Floor (Eds.) *Handbook on Blockchain in Society, De Gruyter*. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4915881.
- Lane, A.M. and Adam, L. (2022). "Crime and cryptocurrency in Australian courts". *Monash University Law Review*, 48(3), 146-190. Available online: https://search.informit.org/doi/abs/10.3316/informit.373188427576671

[1] See Parliamentary Joint Committee on Law Enforcement, Inquiry into the Impact of New and Emerging Information and Communications Technology https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/NewandemergingICT

[2] Associate Professor Darcy W. E. Allen is an academic economist, Director of the Digital Economy Council of Australia, and has written extensively on the economics of emerging technologies and regulation.
Dr Aaron M. Lane is a Senior Lecturer in Law and Barrister. Aaron is an academic specialising in law, technology and regulation, with practical legal experience as a member of the Victorian Bar.

Together, our research shows that criminals behave like entrepreneurs, and this insight can help the Committee anticipate and combat crime as a service:

- Crime as a service is entrepreneurial because criminals behave like entrepreneurs, shifting their methods as technologies lower the costs of anonymity, coordination, and payments.
- Understanding criminals as entrepreneurs matters for policymakers and law enforcement because, if crime is adaptive, then policy must be adaptive too. Enforcement strategies need to anticipate change, not just respond to it.
- Direct evidence from Australia's prosecutions shows that cryptocurrency-enabled crime is not hypothetical. Crimes involving cryptocurrency are already in our courts, and the number of cases is growing.

If the opportunity arises, we would be pleased to elaborate on our submission, including appearing before the Committee at a public hearing.

Crime as a service and technological entrepreneurship

The Committee has been tasked with examining how crime as a service is changing the work of Australian law enforcement, including "the nature and impact of these and other technology-driven advancements on criminal methodologies and activities, including the use of cryptocurrencies".

Our research shows that criminals are entrepreneurial. That is, criminals spot opportunities, allocate resources and make choices based on the perceived opportunities and costs of their actions. In this context, the Committee should consider crime as a service not as a new category of crime, but a new business model for crime. Criminals adapt to technological and regulatory change, just as legitimate entrepreneurs do. Our framework draws on the economics of crime (Becker 1998) and entrepreneurship (Baumol 1996).[3] This perspective explains why crime is not static. It shifts when new technologies alter the transaction costs of anonymity, coordination, and payment.

Cryptocurrency features matter for criminals because they change the costs of their various courses of action. Global reach, interoperability, censorship resistance, and transparency shift the economics of crime. They change the opportunity space for criminal activities. For instance, cryptocurrencies make global payments cheaper and more difficult to reverse, lowering barriers to transnational service-based crime. They can also both lower or increase the likelihood of detection by law enforcement.

---

[3] See Becker, G. (1998). "The Economics of Crime: Prevention, Enforcement and Punishment" *Cross Sections*, 8-15; Baumol, W. J. (1996). "Entrepreneurship: Productive, Unproductive, and Destructive". *Journal of Business Venturing*, 11(1), 3-22.

Often crypto-based crime is thought of as a single category. We propose that crypto-crime is better understood as a taxonomy. Our chapter sets out a classification system based on *method* (theft vs. fraud) and *context* (conventional, intermediary-enabled, decentralised). These dimensions explain how different technologies enable different kinds of crime. We have reproduced the Table from our chapter below, which illustrates how different service-based models of crime fit into a framework.

	Conventional	**Intermediary-Enabled**	**Decentralised**
Theft	Stealing a Hardware Wallet Stealing/Copying Private Keys (or recovery phrases)	Stealing from a Digital Currency Exchange Misappropriation of assets under custody	Hacking of Decentralised Exchange Smart Contract Exploits
Fraud	Malware with Crypto as Payment Method Investment or Romance Scam with Crypto as Payment Method	Fake Initial Coin Offerings Pump and Dump Schemes	Rug Pulls in Decentralised Finance Flash Loan Attacks in Decentralised Finance

Source: Allen, DWE and Lane, AM (forthcoming), "Crypto Crime as Criminal Entrepreneurship" In L. Robb and J. Floor (Eds.) Handbook on Blockchain in Society, De Gruyter.

It is also critical to understand that crimes, including those committed using new technologies, are the outcome of the adaptiveness of criminal entrepreneurs. Subsequently, interventions that raise costs in one domain often push activity elsewhere. For example, tightening regulation of centralised cryptocurrency exchanges may drive activity toward decentralised platforms, or incentivise criminals to adopt privacy-enhancing technologies such as mixers and zero-knowledge proofs.

While the present inquiry focuses on public solutions to suppressing crime, decisions about this must also be made in the context of private and public co-evolution. Suppressing crime is not only a government task. There are strong economic incentives for private actors (e.g. exchanges and wallet providers) to invest in crime-prevention technologies (e.g. scam detection toolkits, hacker bounty programs, dispute resolution mechanisms). Crime as a service thus evolves within a tug-of-war between criminals, regulators, and private innovators.

Crime as a service is not fixed, but a moving frontier as entrepreneurs adapt to their circumstances. Understanding crime as entrepreneurial allows law enforcement and policymakers to anticipate where criminal business models may go next, rather than only reacting to past harms.

Below we directly respond to the Committee's Terms of Reference, regarding this entrepreneurial crime theory.

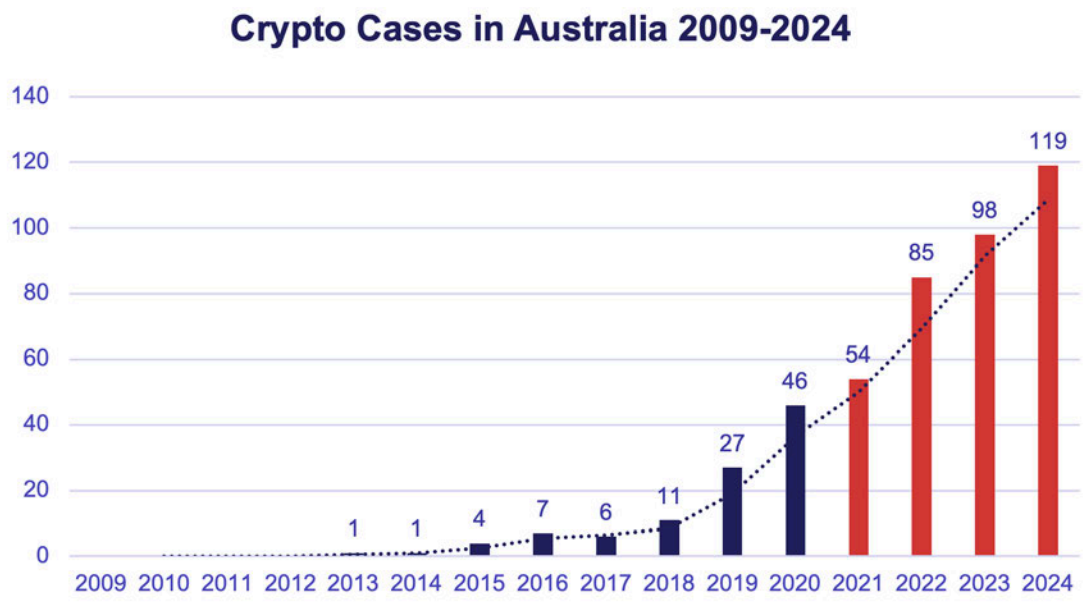
Term of Reference	**Relevance of our entrepreneurial crime theory**
"the nature and impact of these and other technology-driven advancements on criminal methodologies and activities, including the use of cryptocurrencies"	Our research shows criminals adopt cryptocurrencies when they lower payment costs, and when regulation in one area pushes them elsewhere. Cryptocurrencies reduce the costs of payments and anonymity, enabling scalable service-based criminal models.
"challenges and opportunities for Australian law enforcement in combatting these and other evolving criminal methodologies"	Because crime adapts, enforcement must be proactive. Technologies like blockchain analysis create new opportunities, but criminals will continually seek new advantages.
"whether the existing legislative, regulatory, and policy frameworks to address these and other evolving criminal methodologies are fit for purpose"	Static frameworks lag behind dynamic entrepreneurial crime. Our research shows the need for adaptive, technology-neutral regulation that avoids locking in outdated assumptions.

Evidence from Australian prosecutions

Theory must be matched with evidence. Our second contribution is to provide an empirical analysis of how crime as a service has appeared in Australian courts. Lane and Adam's study in the *Monash University Law Review* was the first systematic analysis of cryptocurrency-related prosecutions in Australia. We outline the key findings from that paper below, including that:

- Australian courts are already handling a range of crypto-enabled crimes, including fraud, theft, and money laundering.
- The analysis shows the relative frequency of these offences and provides insight into how courts are approaching them.

This confirms that crime as a service is not abstract. It is part of the day-to-day work of Australian law enforcement. Indeed, the number of Australian criminal cases involving cryptocurrency is growing each year. The Figure below, with updated figures for 2021-2024, shows the growing number of cryptocurrency cases per year.



Source: Lane talk to the ASLA Conference 2025, "Crime and Cryptocurrency in Australian Courts: Cases from 2021-2024"

Criminal entrepreneurs were early adopters of cryptocurrency. Unsurprisingly, law enforcement has had to adapt quickly. Agencies such as the AFP Cybercrime Operations Unit and AUSTRAC have built capacity, but cases continue to rise.

A wide range of crimes have been prosecuted. Australian courts have already considered cryptocurrency in the context of fraud, theft, drug trafficking, money laundering, and related offences. Yet in most cases, policing remains traditional. Offenders were caught using standard investigative methods such as intercepting packages, physical surveillance, admissions during questioning. Only a minority of cases involved sophisticated crypto analysis or undercover operations on dark web markets. This evidence supports the entrepreneurial theory outlined above: offenders are adopting crypto when it reduces costs or when it is required, not necessarily because they are highly sophisticated. Indeed, many offenders used cryptocurrency not because they were sophisticated criminals but because it was the required or most convenient form of payment on illicit markets. That is, it is not necessarily the case that cryptocurrency was used out of convenience, but because it was necessary in that particular context.

This research shows that crypto-enabled crime is not speculative but is rather already part of the Australian justice system.

Policy implications

While our focus here has both theoretical implications (in how we should understand crypto crimes as a choice) and also empirical implications (in the cases that have been prosecuted), we can also draw some general high-level implications for Australian policy, including the need to:

- Shift enforcement framing to see criminals as adaptive entrepreneurs, not static actors.
- Design adaptive, technology-neutral regulation that anticipates change rather than target specific tools or platforms.
- Build capability to continually track prosecutions and measure the evolving criminal landscape.
- Support law enforcement to anticipate new cost structures (e.g. anonymity services, AI-driven criminal tools) rather than react only after harm has occurred.

Conclusion

Our research demonstrates that crime as a service is best understood as entrepreneurial. Criminals, like entrepreneurs, adapt their behaviour in response to the costs and opportunities created by technology. This perspective helps explain why particular forms of criminal activity emerge and decline over time, and it provides a framework for anticipating how crime will continue to evolve in Australia.

Importantly, this is not just a theoretical observation. Empirical prosecution data from Australian courts shows that these challenges are already present. Offenders are making use of cryptocurrencies in practice because these technologies reduce barriers to entry, lower costs, or are simply the easiest available option. These realities must shape how law enforcement and policymakers think about the challenges of crime as a service.

We would welcome the opportunity to provide further information, updated data, or to appear before the Committee.

Regards,

Associate Professor Darcy W.E. Allen

Dr Aaron M. Lane