Australian
Banking & Finance
Law Bulletin

Taking and enforcing security over cryptocurrency

David Kreltszheim CORNWALL STODART

Increasing numbers of individuals and corporations in Australia have significant entitlements to cryptocurrency. To this extent, discussions about the blockchain and cryptocurrency are not theoretical or abstract or matters for the future. There are real questions in the here and the now about how lenders can take effective security over cryptocurrency and how insolvency practitioners might identify, secure and sell entitlements to cryptocurrency. The legal nature of cryptocurrency is not clear. Nonetheless, there are several things that lenders and insolvency practitioners can do to achieve the best possible result.

What is cryptocurrency?

A cryptocurrency is a particular type of digital currency that has been defined as having the following characteristics:

> [It] has an equivalent value in real (fiat) currency and can be exchanged back-and-forth for real currency [and is decentralised] …
> …
> [It is a] distributed, open-source, math-based, peer-to-peer [currency] that [has] no central administrating authority and no central monitoring or oversight.[1]

The first — and pre-eminent — example of a cryptocurrency is bitcoin,[2] which has operated for nearly a decade as a reliable and tamper-resistant method for transferring value online without using a financial intermediary like a bank or a credit card company.[3] In addition, there are now literally hundreds of other cryptocurrencies[4] including Ethereum,[5] Dash,[6] Monero,[7] Ripple[8] and Litecoin.[9]

How does a cryptocurrency work?

The key characteristics of bitcoin (and any comparable cryptocurrency) are as follows.

Cryptography is used to secure users' cryptocurrency entitlements in wallets

The Bitcoin protocol includes a mechanism for a "wallet" and bitcoin addresses to be created for a user (let us call her Alice). That involves the generation of a private and public key pair for Alice based on asymmetric public key cryptography.[10] "Asymmetric" means that different keys are used for encryption and for decryption. Broadly, the process can be thought of like this:

> … anybody can close a padlock simply by clicking it shut [analogous to applying a public key], but only the person who has the [private] key can open it. Locking (encryption) is easy, something everybody can do, but unlocking (decryption) can be done only by the owner of the key. The trivial knowledge of knowing how to click the padlock shut does not tell you how to unlock it.[11]

More technically, asymmetric key cryptography is based on practically irreversible mathematical functions that are easy to calculate in one direction but are presently not feasible to "reverse engineer".

Alice's bitcoin address associated with her wallet is derived from Alice's public key. If another user (Bob) wants to "transfer"[12] an entitlement to an amount of cryptocurrency to Alice, Bob uses the software protocol to apply his private key[13] and Alice's bitcoin address in a process to implement that transfer.

Assuming that Bob has kept his private key private, the application of that key demonstrates that the transfer of the relevant amount of cryptocurrency was initiated by Bob and not by some other user. This permits Bob to access the amount of cryptocurrency to be transferred (Bob has in effect used his private key to "unlock the padlock" represented by the cryptocurrency associated with his public key/bitcoin address).

Bob's application of Alice's public key-derived wallet address in the process (by in effect clicking shut the padlock that can only be opened by Alice) ensures that that amount is available to be used by Alice and not some other user. This is because Alice needs to apply her private key to use the amount of cryptocurrency transferred to her (by in effect opening her padlock). As a result, if Alice keeps her private key private, only Alice will be able to use the amount of cryptocurrency transferred to her by Bob.

There is more than one way to participate in the system

A user may choose to participate in a cryptocurrency system in various ways. In the case of bitcoin, for example, a user may:

- Download the "full bitcoin client" or "full node" that stores the entire history of bitcoin transactions and is capable of initiating transactions directly on the Bitcoin blockchain.[14] This full node would also manage the user's wallets.

- Download a "lightweight client" which only stores a user's wallets but relies on third-party servers for access to the Bitcoin blockchain.[15]
- Rely on a "web client" accessed through the user's browser, where the user's wallet is stored on a third party's server which provides access to the Bitcoin blockchain.[16] Web clients can either:
  - — use client-side encryption so that the user has full control of the private keys and transaction records, which are created and maintained on the client side, ie on the user's desktop or mobile device or
  - — store the user's private keys and transaction information on the third party's server
- Purchase and manage a bitcoin entitlement through a cryptocurrency exchange.[17]

A tech-savvy user may choose to hold their private keys in "cold storage". This is where keys are generated on an offline system (never connected to the internet) and stored offline either on paper or on a digital medium like a USB memory stick.[18]

Users are not explicitly linked with their "real-world" identity

Typically, the software protocol of a cryptocurrency would not limit Alice or Bob or any other user to a single bitcoin address (ie private/public key pair) linked to their "real-world" identity. In the case of bitcoin, for example, it is usual for a single user to have multiple bitcoin addresses associated with their wallet. Each address is a string of numbers and letters that is publicly visible on the Bitcoin blockchain. That address is effectively a pseudonym for the relevant individual. Since an individual may have multiple bitcoin addresses, they may have multiple pseudonyms.[19]

The fact that Alice and Bob need not be explicitly identified by their real names in bitcoin transactions does not necessarily mean that they are anonymous in those transactions. In particular, because the payer and payee bitcoin addresses are publicly visible on the Bitcoin blockchain, it may be possible to identify the real identities of Alice and Bob by data analysis of the Bitcoin blockchain.[20]

Users' currency entitlements are recorded on a decentralised "electronic ledger"

For Alice to pay Bob in bitcoin, Alice causes her wallet application to do two things. First, her wallet application needs to find inputs that can pay the amount that she wants to pay Bob. Those inputs are an aggregation of previous amounts paid to her by other users that she has not yet spent. Second, the wallet application "unlocks" those unspent outputs attributed to her public key on the Bitcoin blockchain and creates a new transaction output that can only be unlocked in turn by Bob using his private key.[21] In this way, the Bitcoin blockchain is an "electronic ledger" that contains a complete history of the generation and transfer of bitcoin from user to user over time.

The decentralised electronic ledger must be updated to prevent double spending

A key fraud mitigation issue for any purported payment system or currency is to address the risk of Alice seeking to double spend value attributed to her, first to pay Bob and (before the system is updated) to pay Charles also. In bitcoin, this issue is addressed by the use of a mechanism for the nodes operating the Bitcoin blockchain to achieve a consensus about what the authoritative version of the blockchain is at any given point in time. The transaction by which Alice pays value to Bob is initially propagated through the nodes operating the Bitcoin blockchain. At this stage, the transaction has yet to become part of the authoritative version of the blockchain. That will not happen until the transaction is verified and included in a "block" that is added to the authoritative version of the blockchain by a process called "mining".[22]

The legal nature of cryptocurrency

In my view, there is no single legal characterisation of cryptocurrency that can be formulated in the abstract to apply generally. Context is all-important. For the purposes of this article, the main issue is to identify what property rights a "holder" of cryptocurrency has for the purposes of security and insolvency law.

As noted above, users can participate in a cryptocurrency system in various ways.[23] Many users "hold" bitcoin by having an entitlement recorded in their name on a cryptocurrency exchange or other third-party server (Third-Party Holding). These users do not have direct control of the private keys that unlock their entitlements on the relevant cryptocurrency blockchain. On the other hand, there are other users who take steps to control directly the private keys that are needed to deal with the cryptocurrency that they hold (Direct Holding).

In some respects, a Third-Party Holding places the third party in a position that is similar to a bank, in that the user will merely have a right of action against the third party.[24] In other respects, a Third-Party Holding is more akin to a custodial relationship, on the basis that the third party has custody of some asset belonging to the user.[25] The law is unclear.

What does a user have in the case of a Direct Holding? What they have specifically is knowledge of a long secret number that confers the ability to transfer an amount of value to any public address for that cryptocurrency.[26] Whether that gives rise to a property right and, if so, the way that property right should be conceptualised, is a vexed question.[27]

The above issues will be addressed over time. I expect they will be the subject of much learned legal analysis and contention. For now, despite the uncertainties, I think there are several things that lenders and insolvency practitioners can do to achieve the best possible result.

Taking security in Australia over cryptocurrency

The Personal Property Securities Act 2009 (Cth) (PPSA) regulates the validity and priority of security interests over personal property. In the face of the uncertainties outlined above, I suggest the following starting points:

- A user's Third-Party Holding or Direct Holding of cryptocurrency should be taken to be a form of personal property.
- As a result, a user's Third-Party Holding or Direct Holding of cryptocurrency would be within the scope of any properly drawn definition of secured collateral in a general security agreement.
- Whatever type of personal property is constituted by a user's Third-Party Holding or Direct Holding, it is unlikely to be collateral of the kind that is specified in s 21(2)(c) of the PPSA. That is, a secured party cannot perfect its security interest over the collateral by controlling the collateral in one or other of the ways that are outlined in ss 23–9 of the PPSA.
- As a result, the secured party should perfect its security interest by registration. It is not clear whether a user's Third-Party Holding or Direct Holding is within the collateral class of "financial property"[28] or "intangible property".[29] Given this uncertainty, I suggest a registration in the collateral class of "all present and after-acquired property, except".[30] This will mitigate the risk of selecting the wrong collateral class. The secured party should take care in drafting the exception in the "collateral description" field of the registration, noting that the exception must specify an item or class of personal property that is not covered by the registration.[31]
- As noted above, the secured party's security interest is unlikely to be able to be perfected by control. As a result, the security interest cannot have priority over other security interests over the same property on the basis that the secured party has perfected its interest by control.[32] Further, given the uncertainty of the classification of Third-Party Holdings and Direct Holdings of cryptocurrency for PPSA purposes, a secured party who finances a user's acquisition of cryptocurrency should be wary about relying on having a purchase money security interest to give the secured party priority.[33] As a result, the secured party should ensure that its security interest is registered first, or it enters into appropriate priority agreements with the holders of prior-registered interests.[34]
- If a secured party is relying on a user's Direct Holding (or Third-Party Holding[35]) as a significant component of its security, the secured party should take practical steps to control those rights. This means that the cryptocurrency should be "transferred" to the secured party, that is, transferred to a public address on the relevant cryptocurrency blockchain for which the secured party holds the corresponding private keys. The secured party should store those private keys offline either on paper or on a digital medium like a USB memory stick. This approach means that the user will not have the day-to-day benefit of the cryptocurrency as a circulating asset in the nature of currency or funds in a bank account. However, this approach is functionally similar to how a secured party would take control of (and effectively immobilise) a grantor's interests in investment instruments.
- If there is policy or other reasons why a secured party does not wish to have a Direct Holding of cryptocurrency itself, the secured party may nominate a custodian to hold the Direct Holding for the secured party for as long as the PPSA security interest is on foot. The secured party would need to satisfy itself as to the solvency of the custodian and the security measures adopted by it.

Taking control over cryptocurrency in insolvency in Australia

Again, despite the uncertainties outlined above, I suggest the following starting points in the external administration of a company or in a personal bankruptcy:

- A user's Third-Party Holding or Direct Holding of cryptocurrency should be taken to be "property" for the purposes of the Bankruptcy Act 1966 (Cth).[36] As a result, those holdings are capable of being "the property of the bankrupt" that will vest in the Official Trustee or the registered trustee of the bankrupt's estate[37] in a personal bankruptcy.

Similarly, a company's Third-Party Holding or Direct Holding should be taken to be property for the purposes of the Corporations Act 2001 (Cth).[38] Again, this would subject those holdings to the legal control of the external administrator (receiver, voluntary administrator or liquidator).

- Legal control is all very well. A significant practical issue for an insolvency practitioner (or for a secured party contemplating enforcement) is to even identify that a user has a Third-Party Holding or a Direct Holding.
- A secured party considering enforcement should assess the possibility of the grantor having a Third-Party Holding or a Direct Holding and, if so, the best means of securing those assets immediately upon enforcement.[39] The questions that should be asked include these:
  - — Is the grantor likely to have received payment for their services in a cryptocurrency?
  - — Is the user likely to have taken an investment position in a cryptocurrency? In either case, is the grantor more likely to have a Third-Party Holding or a Direct Holding?
  - — If the secured party knows or suspects that the grantor has a significant Direct Holding, can the secured party rely on an "assets in jeopardy" event of default to take possession or make an appointment under its general security agreement without issuing a prior demand? Or should the secured party rely on the power that it would most likely have under its general security agreement to inspect secured property without prior notice in order to ascertain more about the Direct Holding prior to enforcement, eg by identifying the physical medium on which the private keys are stored? (That may constrain a grantor who might otherwise be inclined to misappropriate a Direct Holding as soon as enforcement occurs.)
- If an insolvency practitioner knows or suspects that a bankrupt or an insolvent company has significant Direct Holdings, the insolvency practitioner may use the legal powers available to them to identify the Direct Holdings and take control of them (see below).
- If an insolvency practitioner knows or suspects that a bankrupt or an insolvent company has significant Third-Party Holdings, the insolvency practitioner should notify the applicable cryptocurrency exchanges of their appointment as soon as possible.[40]
- An insolvency practitioner should immediately take control over all Direct Holdings that are identified by them.[41] Those Direct Holdings should be transferred into the exclusive control of the insolvency practitioner, that is, transferred to a public address on the relevant cryptocurrency blockchain for which the insolvency practitioner holds the corresponding private keys. Ideally, the insolvency practitioner should store those private keys offline either on paper or on a digital medium like a USB memory stick.
- Given the numerous highly publicised hacks of cryptocurrency exchanges, an insolvency practitioner who identifies Third-Party Holdings would be well advised to transfer those holdings into a Direct Holding under the exclusive control of the insolvency practitioner as outlined above.

These are starting points only. The commercial practice and legal analysis in relation to cryptocurrency in security and insolvency will evolve over time.

David Kreltszheim
Special Counsel
Cornwall Stodart
d.kreltszheim@cornwalls.com.au
www.cornwalls.com.au

About the author
David is a banking, payments and regulatory lawyer. He publishes and presents widely on these topics. The views expressed are the author's and do not necessarily reflect those of Cornwall Stodart.

Footnotes

[1] Senate Economics References Committee (Cth) *Digital currency — game changer or bit player* (August 2015) 3–4 paras 2.3–2.4 www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/Report/. This is a paraphrase of a comparable definition in Financial Action Task Force *Virtual Currencies: Key Definitions and Potential AML/CTF Risks* (June 2014) 4 www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

[2] Bitcoin has now "forked" into Bitcoin Core and Bitcoin Cash, but that is not relevant for present purposes. See Bitcoin.com, accessed 31 July 2018, available at www.bitcoin.com. The term "bitcoin" here refers to the digital currency bearing that name. The term is also used to describe the underlying blockchain technology platform (the Bitcoin blockchain) and the protocol (ie software programs) that runs over the underlying blockchain technology (the Bitcoin protocol): See M Swan, *Blockchain: Blueprint for a New Economy*, 1st edn, O'Reilly Media, 2015, pp 1–2. Following convention, in this article, the lowercase

"bitcoin" is used to denote the cryptocurrency, in contrast with the other two usages of the term.

3. Cryptocurrency exchanges managing bitcoin entitlements have been hacked, repeatedly. But those hacks did not result from a compromise of the security of the Bitcoin blockchain or the Bitcoin protocol.

4. There are over 1400 cryptocurrencies listed in order of market capitalisation in CoinMarketCap, Top 100 Cryptocurrencies By Market Capitalization, accessed 31 July 2018, https://coinmarketcap.com.

5. See Ethereum: Blockchain App Platform, accessed 31 July 2018, available at www.ethereum.org.

6. See Dash, accessed 31 July 2018, available at www.dash.org.

7. See Monero: Private Digital Currency, accessed 31 July 2018, available at https://getmonero.org/home.

8. See Ripple, accessed 31 July 2018, available at https://ripple.com.

9. See Litecoin, accessed 31 July 2018, available at https://litecoin.com.

10. The same technology underlies the operation of e-conveyancing in Australia (through Electronic Lodgment Network Operators like Property Exchange Australia (PEXA)) and the "Gatekeeper" Digital Signature Certificates that are allocated to users for various dealings with the Commonwealth Government and Australian state governments.

11. See S Singh, *The Code Book: The Secret History of Codes and Code-Breaking*, 1999, p 270.

12. The use of the term "transfer" makes certain assumptions about the legal nature of bitcoin and other cryptocurrencies, hence the use of quotation marks for this term and various other terms in this article. If one uses value-laden terms and analogies when analysing the legal nature of a new electronic payment system, one should be self-conscious about it: see D Kreltszheim "The legal nature of 'electronic money': Part 1" (2003) 14(3) *Journal of Banking and Finance Law and Practice* 161 at 162 and 172–4 and D Kreltszheim "The legal nature of 'electronic money': Part 2" (2003) 14 *Journal of Banking and Finance Law and Practice* 261 at 276–8.

13. A private key is not a physical thing. It is simply information, that is, a string of numbers and letters, like this: 5J76sF8L5jTtzE96r66Sf8cka9y44wdpJjMwCxR3tzLh3ibVPxh.

14. See A Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 2015, pp 6–7. The term "client" refers here to a requesting program or user in a client–server relationship: see TechTarget, Client, accessed 31 July 2018, available at http://searchenterprisedesktop.techtarget.com/definition/client.

15. Antonopoulos, above n 14, at pp 6–7.

16. Antonopoulos, above n 14, at pp 6–7.

17. There are numerous cryptocurrency exchanges in business. For an extensive list, see Finder "Cryptocurrency Exchange Finder" (15 August 2018) www.finder.com.au/cryptocurrency/exchanges.

18. Antonopoulos, above n 14, at p 237. As noted in above n 13, a private key is simply information, not a physical thing. As a result, it can be recorded on paper.

19. The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) regulates digital currency exchange businesses which have a relevant geographical link with Australia when those businesses provide the service of (see s 6(1) table 1 item 50A):

- exchanging digital currency (which is defined in a manner that includes cryptocurrencies) for money, whether the money is Australian or not or
- exchanging money, whether Australian or not, for digital currency

As a result, these businesses need to verify the identity of their customers. But this requires Alice and Bob to be identified by their real-world identities in limited circumstances only, that is, where they use a cryptocurrency exchange business to exchange cryptocurrency for money or vice versa.

20. See S Meiklejohn, M Pomarole, G Jordan, K Levchenko, D McCoy, G M Voelker and S Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names" Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Spain (23–25 October 2013) pp 127–140 https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf. This article refers to a study in which the publicly visible Bitcoin blockchain was analysed in a simulated experiment to construct a pattern of behaviour, in which approximately 40% of the bitcoin users' identities were revealed.

21. See Antonopoulos, above n 14, pp 21–4.

22. This is the "secret sauce" of a cryptocurrency: the combination of mathematics with game theory to give participants an economic incentive to assist in achieving consensus about the authoritative version of the decentralised ledger at a given time.

23. See the text associated with above nn 14–17.

24. S Bayern "Dynamic Common Law and Technological Change: The Classification of Bitcoin" (2014) 71(2) *Washington and Lee Law Review Online* 22 at 25–9.

25. K FK Low and E GS Teo "Bitcoins and other cryptocurrencies as property?" (2017) 9(2) *Law, Innovation and Technology* 235 at 265–6 https://doi.org/10.1080/17579961.2017.1377915; D Fox, "Cyber-Currencies in Private Law" in *The Search for Certainty: Essays in Honour of John Smillie*, S E Griffiths, M Henaghan and MB R Ferrere (Eds), 2016, pp 129 and 132.

26. Above n 24, at 31–2.

27. Above n 24, at 29–33; Low and Teo, above n 25, at 245–54; Fox, above n 25, at pp 137–40.

28. PPSA, s 10 — this is defined as any of chattel paper, currency, a document of title, an investment instrument and a negotiable instrument.

29. This is relevantly defined as personal property (including a licence) that is not financial property, goods or an intermediated security (above n 28, s 10). A cryptocurrency entitlement would fall into this definition if it is clear that the entitlement is not financial property. In my view, that is not clear.

30. Personal Property Securities Regulations 2010 (Cth), Sch 1 para 2.3(1)(d).
31. See above n 30, reg 1.6 — definition of “all present and after-acquired property, except”.
32. Above n 28, s 57(1).
33. Priority is available for a security interest of the type specified in above n 28, s 14(1)(b) which is perfected by registration in accordance with s 62(3).
34. Above n 28, s 61.
35. Given the inherent hacking and insolvency risks of a Third-Party Holding, I suggest that the best course is to convert a user’s Third-Party Holding into the secured party’s Direct Holding as outlined here.
36. Bankruptcy Act 1966 (Cth), s 5 provides that “property” means:

    > … real or personal property of every description, whether situate in Australia or elsewhere, and includes any estate, interest or profit, whether present or future, vested or contingent, arising out of or incident to any such real or personal property.

37. Above n 36, s 5 — definition of “the property of the bankrupt” read together with s 58 (vesting of property upon bankruptcy — general rule).
38. Corporations Act 2001 (Cth), s 9 relevantly provides that “property” means “any legal or equitable estate or interest (whether present or future and whether vested or contingent) in real or personal property of any description and includes a thing in action”.
39. These issues are not unique to cryptocurrencies. They would arise in any instance where the secured property includes valuable assets that are difficult to identify and easy for delinquent grantors to misappropriate upon enforcement, such as in a diamond wholesaling business, for example.
40. See above n 17.
41. This is easier said than done. A good example of success (in a law enforcement context) was Victoria Police’s seizure of three electronic wallets containing private keys in relation to 24,518 bitcoins from a drug dealer in Warrandyte in December 2012. That bitcoin was eventually sold by Ernst & Young on behalf of the Victorian Government in a 48-hour sealed bid auction in June 2016, yielding many millions of dollars more than what would have been realised if the bitcoin had been sold earlier on: see C Griffith “Cops, red tape and a $25m bitcoin windfall” *The Australian* 20 June 2016 www.theaustralian.com.au/business/technology/cops-red-tape-and-a-25m-bitcoin-windfall/news-story/6de90658f976c3d1164fe8012241e55b.