RMIT Blockchain Innovation Hub
RMIT University
440 Elizabeth St, Melbourne 3000

26 October 2018

Review of National Arrangements for the Protection and Management of Identity Information
C/o Home Affairs
4-6 Chan St
BELCONNEN ACT 2613

Submission to Review of National Arrangements for the Protection and Management of Identity Information.

Authors: Dr Darcy Allen, Alastair Berg, Dr Chris Berg, Professor Sinclair Davidson, Aaron Lane, Dr Mikayla Novak, and Professor Jason Potts

Contact Author: Alastair Berg, Researcher, RMIT Blockchain Innovation Hub, Email: alastair.berg@rmit.edu.au Mobile: +61417 156 259

Dear Mr Roger Wilkins AO,

We are writing to you regarding the Review of National Arrangements for the Protection and Management of Identity Information commissioned by the Department of Home Affairs. Please find below a submission from members of the RMIT Blockchain Innovation Hub. Our submission focuses on how blockchain technology relates to the terms of reference on achieving "these objectives in ways that respect and promote peoples' privacy".

We have extensive academic and policy experience in blockchain technology, and are currently working on applications which allow individuals to securely store and share identity data. This includes through a Victorian Government grant to examine the opportunities and

challenges in applying blockchain within the health records space.[1] The central contention of our submission is that the Review should recommend further analysis of the potential of blockchain technology as a mechanism to ameliorate the problem of privacy over the governance of identity information, by giving individuals the opportunity to minimise the amount of identity information they disclose as part of government and commercial interactions. Blockchain-based identity solutions allow an individual to prove with probabilistic certainty that they are owner of some identity attribute while significantly decreasing the chance of a data breach. Such a combination of certainty and security is rapidly becoming technically feasible. As a technology for providing secure decentralised governance of ledgers of data—including identity information—blockchain holds great potential to overcome privacy challenges while improving security. We would welcome any opportunity to provide additional information relating to blockchain and the protection and management of identity information.

About the RMIT Blockchain Innovation Hub

The RMIT Blockchain Innovation Hub (BIH) is the world's first social science research centre into blockchain technology. Founded in 2017 at RMIT University, we are an interdisciplinary team of researchers in economics, political economy, organisational theory, law, sociology, politics and communications. The RMIT BIH is developing the foundational theory of institutional cryptoeconomics, business strategy and adaptation to blockchain technologies, mapping the blockchain economy, and identifying the public policy challenges that will hold back or accelerate this economic revolution.[2] We are working across a range of blockchain applications including supply chains, civil society and digital identity.

Blockchain and the protection and management of identity information

The timing of this Review is appropriate, given that individuals are becoming increasingly aware of the dangers of government and commercial entities holding significant amounts of their personal information. Neither government nor commercial entities can completely

[1] See RMIT University, "Blockchain to Transform Healthcare Models," *RMIT University* 2018.
[2] For a brief overview of institutional cryptoeconomics please see Chris Berg, Sinclair Davidson, and Jason Potts to Cryptoeconomics Australia, 27 September, 2017, https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4.

protect an individual's identity information from unauthorised access using traditional centralised databases. The recent instances of Medicare numbers being available from 'dark net' marketplaces for as little as $30, unauthorised access of tax records by ATO employees, and the recent data breaches of companies like Facebook, all illuminate the need for new models of data protection. There is a real and urgent need to look to alternative technologies to better protect Australians from identity crime, allow individuals to access targeted government services, all the while ensuring privacy of personal information.

One way in which government can tailor services to the individual is through *data centralisation*. Digitisation of identity information, as well as comprehensive records of government and commercial interactions, permits almost total surveillance of individuals for the assessment of taxation and entitlements. While a centralised system might appear to have efficiency benefits, the trade-off is that the system is vulnerable to unauthorised access and abuse. Any centralised repository of identity information of this nature stores more identity attributes than is necessary, while presenting a fundamental security weakness. This situation can be referred to as a 'honey pot' of identity information, and is inherently vulnerable to malicious actors.

The alternative to centralised databases sees individuals having greater control over their own identity information. A decentralised model of identity is commonly known as *self-sovereign identity*, and is one where the individual is central to the administration of their personal information.[3] Self-sovereign identity satisfies key principles including individual control, access, portability, and disclosure minimisation. Individuals have sovereignty over the way in which their data is used, and reveal only the information they want, depending on the context of the interaction. Put simply, individuals have property rights over their own data.[4] Such a model sees individuals disclose "just enough" identity information to a counterparty for the

[3] See for instance: Allen, Christopher. 2016. The Path to Self-Sovereign Identity. Accessed 12 February 2018; Der, Uwe, Stefan Jähnichen, and Jan Sürmeli. 2017. "Self-sovereign Identity - Opportunities and Challenges for the Digital Revolution." *arXiv preprint arXiv:1712.01767*; Othman, Asem, and John Callahan. 2017. "The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity." *arXiv preprint arXiv:1711.07127*.

[4] Indeed, academics have recently been examining the ways in which individuals might be able to derive an income from their data – their identity information – rather than its value being realised only by companies like Facebook, Apple, Amazon and Google. See for instance Posner, E.A., and E.G. Weyl. 2018. *Radical Markets: Uprooting Capitalism and Democracy for a Just Society*: Princeton University Press.

purposes of a transaction with a government or commercial entity. For instance, age contingent transactions require only that the counterparty verify that an individual is over a certain age, without the revelation of other identity information like name, address, date of birth and so on.

Many blockchain enabled identity solutions under development adopt the principles of self-sovereign identity. For most of these protocols, blockchain databases are not used to store identity information, rather the blockchain is used to selectively disclose identity information to counterparties, often using allied technology such as zero-knowledge proofs. Zero-knowledge proofs are a technology which allow one to prove the proof or existence of something, without disclosing the exact nature of that claim. Returning to the example of an age contingent transaction, zero-knowledge proofs might allow an individual to prove they are over 18 years of age, without revealing their exact age. It is important to note at the outset that, due to the publically auditable nature of many blockchains, storing identity information directly on the ledger would create serious privacy issues.

Implementation of decentralised approaches to identity governance and management is restricted by available technologies. Blockchain technology has recently emerged as one such technology which has potential to allow individuals the ability to securely store, and selectively share identity information using robust cryptography. Blockchain based identity solutions allow an individual to prove with probabilistic certainty that they are owner of some identity attribute, while significantly decreasing the chance of a data breach; such a combination of certainty and security has never been technically feasible.

Blockchain technology emerged almost ten years ago as a way in which individuals could store and share value using the internet via the cryptocurrency Bitcoin. Blockchains more generally use asymmetric (public-key) cryptography, peer-to-peer networks and economic incentives to create distributed and immutable databases which do not rely on a central entity to maintain data integrity. Aside from their most well-known use in decentralised currencies,

blockchain technology is currently being applied to applications including voting, supply chains, civil society, property registries and identity.[5]

Blockchain may provide for greater privacy protections for the individual, while ensuring instances of identity crime are more readily discovered due to the immutable nature of distributed databases. Unauthorised access to personal information by government employees or other malicious actors would be logged, leaving an immutable record by which those responsible might be traced, allowing steps to be taken to quickly minimise damage.

Blockchain technology is currently being examined and experimented with by entrepreneurs, private organisations, government and NGOs as a way in which identity can be securely managed by the individual to ameliorate some of the drawbacks associated with centrally storing identity information. In addition, there is significant investment being put into the development of standards around the use of blockchain technology in identity governance, including by the World Wide Web Consortium (W3C).

Given the multifaceted and complex questions on the intersection of blockchain and the governance of identity information, we propose that one recommendation be further inquiry into how blockchain technology may provide more decentralised and robust solutions to digital identity in the context of government services.

We trust that this submission has been of interest. We would be pleased to answer any questions that you may have. We look forward to any opportunity you may have to investigate the use of blockchain in enabling the safe storage and sharing of the identity information of Australians.

[5] See for instance our research in these areas: Alastair Berg et al., "Identity as Input to Exchange," (2018); Alastair Berg et al., "The Institutional Economics of Identity," *Available at SSRN 3072823* (2017); Darcy W E Allen et al., "Cryptodemocracy and Its Institutional Possibilities," *The Review of Austrian Economics* (2018); "The Economics of Crypto-Democracy" (paper presented at the Linked Democracy: AI for Democratic Innovation, 26th International Joint Conference on Artificial Intelligence, Melbourne, Australia, 19 August 2017 2017); Darcy W E Allen et al., "Blockchain Tradetech," in *APEC Study Centres Consortium Conference (ASCCC)* (Port Moresby, Papua New Guinea 2018).

References

Allen, Christopher. 2016. The Path to Self-Sovereign Identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Allen, Darcy W E, Chris Berg, Sinclair Davidson, Mikayla Novak, and Jason Potts. "Blockchain Tradetech." In *APEC Study Centres Consortium Conference (ASCCC)*. Port Moresby, Papua New Guinea, 2018.

Allen, Darcy W E, Chris Berg, Aaron M Lane, and Jason Potts. "Cryptodemocracy and Its Institutional Possibilities." *The Review of Austrian Economics* (2018): 1-12.

———. "The Economics of Crypto-Democracy." Paper presented at the Linked Democracy: AI for Democratic Innovation, 26th International Joint Conference on Artificial Intelligence, Melbourne, Australia, 19 August 2017 2017.

Berg, Alastair, Chris Berg, Sinclair Richard Davidson, and Jason Potts. "The Institutional Economics of Identity." *Available at SSRN 3072823* (2017).

Berg, Alastair, Chris Berg, Sinclair Davidson, and Jason Potts. "Identity as Input to Exchange." *Available at SSRN 3171960* (2018).

Berg, Chris, Sinclair Davidson, and Jason Potts. "The Blockchain Economy: A Beginner's Guide to Institutional Cryptoeconomics." In *Cryptoeconomics Australia*, 2017, https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4.

Der, Uwe, Stefan Jähnichen, and Jan Sürmeli. 2017. "Self-sovereign Identity - Opportunities and Challenges for the Digital Revolution." *arXiv preprint arXiv:1712.01767*

Othman, Asem, and John Callahan. 2017. "The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity." *arXiv preprint arXiv:1711.07127*.

Posner, E.A., and E.G. Weyl. 2018. *Radical Markets: Uprooting Capitalism and Democracy for a Just Society*: Princeton University Press.

RMIT University. "Blockchain to Transform Healthcare Models." *RMIT University* 2018, https://www.rmit.edu.au/news/all-news/2018/jul/rmit-dbresults-blockchain.