Senate Committee on Australia as a Technology and Financial Centre

Third Issue Paper

By Elas Digital Pty Ltd

Bitcoin vs Cryptocurrency

It is important to understand is that Bitcoin is a system that operates as defined in the Bitcoin whitepaper (www.bitcoinsv.io/bitcoin.pdf). The cryptocurrency sold under the name of Bitcoin is not Bitcoin and no longer operates under the rules specified in this system. The operators of the BTC network (Bitcoin Core developers) duplicated the Bitcoin database and created a network separate from Bitcoin in 2017 but kept the name and trading ticker on cryptocurrency exchanges leading to the public perception that BTC is Bitcoin. However, it is simple to show using the text of Satoshi's original document that the BTC system no longer operates as defined.

Dr Craig Steven Wright an Australian born inventor authored the academic White Paper "Bitcoin: A Peer-to-Peer Electronic Cash System" under the moniker 'Satoshi Nakamoto'. Dr Wright also owns the copyright to the whitepaper. In an unprecedented case, "London's High Court has granted ONTIER LLP client and Bitcoin creator, Dr Craig Wright, default judgment in his copyright infringement action against 'Cobra' the pseudonymous operator and publisher of the bitcoin.org website (Ontier UK, 2021 June 29). A Senior Associate at ONTIER LLP, Simon Cohen, commented:

> Dr Wright does not wish to restrict access to his White Paper. However, he does not agree that it should be used by supporters and developers of alternative assets, such as Bitcoin Core, to promote or otherwise misrepresent those assets as being Bitcoin given that they do not support or align with the vision for Bitcoin as he set out in his White Paper. (Ontier, 2021, June 29)

The network that operates in the market as Bitcoin SV (BSV) is the only network that retains the Bitcoin protocol as its primary mechanism of operation and maintaining the original Bitcoin transaction ledger and protocol. Over the last 3 years, a team co-ordinated by the Bitcoin Association have worked to undo damage caused by years of mismanagement by Bitcoin Core developers. It is for this reason that the Bitcoin SV network is capable of thousands of transactions per second (and scaling towards millions) whilst BTC is stuck at just 5 (five) transactions per second globally. It is envisaged that the network operators will transition towards their own proprietary implementations of software to operate bitcoin nodes, respecting the protocol and maintaining its 'set in stone' status. This is an important aspect for network growth as it ensures that governments and enterprises seeking to build their own systems using the network can be sure their work will remain valid for years or decades into the future.

Wherever Bitcoin is referred to herein this document, we are referring to Bitcoin as it is operated by nodes on the Bitcoin SV network, which uses the token sold as BSV in the market.

Importantly, Bitcoin does not seek to be recognised as a 'cryptocurrency' nor does it seek to represent itself as a tool for anonymity or crime. It is a utility ledger providing a traceable and utile cash system which is applicable to a vast number of business cases and opportunities. Importantly, the design of the system is compatible with existing laws and regulations and as we will explain throughout this document, was built to wrap around existing systems and services, providing an efficient and low cost means to improve service delivery. This means that while regulations may be changed, this should be done to affect a better environment for businesses and consumers and not because Bitcoin is being used as a substrate technology.

Shortly, MNP a leading national accounting, tax and business consulting firm in Canada will be releasing a report on which Bitcoin implementation best fits Nakamoto's original vision. Their report will detail their findings that "BSV is most representative of Nakamoto's original intention and design for Bitcoin" (Qureshi, 2021).

Introduction and Credentials

Elas Digital Pty Ltd was created to commercialise key technologies invented by founder Brendan Lee in early 2019. Elas have 5 patents in the UK outlining methods for the creation and use of tokens that operate with a high degree of efficiency and make effective use of Bitcoin's native functionality. Elas' customers include Australian gold tokenisation start up Amleh Gold (www.amleh.com), and the Government of Tuvalu (www.gov.tv).

The Tuvalu National Digital Ledger project is being conducted as part of an industry consortium including London based nChain, an intellectual property and development services firm, and Faia, a Singapore based consultancy. The project is ambitious in scope and seeks to conduct an overhaul of the Government of Tuvalu's services over the next 4 years, starting with a digital citizenship application process and followed by a trial of digital cash services in late 2021.

Key employees of Elas include Brendan Lee (CEO and Co-Founder), Mohammad Jaber (Director of Business and Co-Founder) and Darren Kellenschwiler (CTO).

Brendan Lee is the Founder and CEO of Elas, and sole inventor of our core technology which allows the simple and low-cost creation of administrative ledgers for the recording of immutable attributed data and the issuance of the most versatile tokens in Bitcoin.

Since entering the industry in 2017, Brendan has been part of multiple ventures, firstly founding Coinstorage, selling products and education services for secure storage of Bitcoin. Brendan then went on to be a part of the Tokenized protocol team that won the 5-million-pound CoingGeek tokenization prize. Since May 2019, he has worked as the Training and Development manager for the Bitcoin Association, and has delivered key technical resources including the Bitcoin SV wiki (www.wiki.bitcoinsv.io) and courses for the Bitcoin SV academy (www.bitcoinsv.academy) including 'Introduction to Bitcoin Theory' and the upcoming 'Introduction to Bitcoin Infrastructure'.

Mohammad Jaber has over a decade of experience working in the banking and finance industry within Australia at the big four banks, having worked on a range on high profile

projects across different sectors from Superannuation to Financial Crime, becoming the trusted link between the business, technology and regulators. Since discovering Bitcoin in 2017, he has been fascinated with what the underlying technology can do at scale and what it can do from an efficiency standpoint for large enterprises and government services. Mohammad took on an active role as content creator for media company CoinGeek covering the landscape of the current financial world and the emerging digital currency industry. He was excited to join Elas as the proprietary technology can fill the much-needed gap for enterprise, governments and regulatory bodies to become more efficient, transparent and compliant at a fraction of the costs they are faced with legacy systems that rely on cumbersome processes.

Darren Kellenschwiler spearheads the implementation of Elas' core technology, operating with a team of design and development talent to bring our patented technology from concepts to solutions. Starting research into the technology in 2013, he sold his first business to make the strategic move to London, the epicentre of Bitcoin at the time. There he quickly became lead organiser of the London Bitcoin Meetup, developing a strong network of thinkers, and learning deeply about the technical possibilities yet to be unlocked. This led to Darren starting a research and development firm, which brought a handful of web application to market within its first year, including the encrypted communication tool, Baemail. Darren was selected for the CambrianSV Developers Conference as one of the most prolific entrepreneurs in the space and went on to win Cambridge University's Pheonix Challenge. His flagship apps were presented on stage at the largest conference in the industry, the 2019 Coingeek conference in London. Shortly thereafter those assets were acquired by Elas and Darren was brought on as CTO.

Opportunities in the digital asset and cryptocurrency sector

Bitcoin presents us with a once in a millennia opportunity to completely re-imagine how data, identity and records of ownership and exchange are managed within local, state and federal government jurisdictions on a global scale. The system, as designed, incentivises private industry to build infrastructure capable of receiving, validating and timestamping all economic activity taking place in the world in real time. This includes small cash microtransactions that are as small as 1/100th of a cent, right up to complex multi-party contracts with multiple discrete payments and long timeframes, providing ways for entirely different business and engagement models to be devised and implemented, outside of any dependency on the third party payment providers whose services keep the price of remittance high.

The Bitcoin Protocol and the parameters that govern its issuance and performance were set by Satoshi Nakamoto in 2009 and are fixed in stone. This is important as it means that transaction scripts created today will continue to be valid on the network at any time in the future (whether it is 1, 10 or 100 years-time). Almost all other blockchain projects (BTC, Ethereum etc) are in a constant state of technology flux, rendering efforts to build long-lasting products and services impossible due to the constantly changing protocols.

The system's proof-of-work validation process is highly scalable, in that the amount of energy expended performing proof-of-work is unrelated to the number of transactions being validated. This means that the same proof-of-work that validates 5,000,000 transactions per day today, could equally secure 1,000,000,000,000 transactions per day in future, as would be required for a global system. Importantly, at this scale each transaction must cost just 1/1000th of a cent for the global revenue for bitcoin miners to be $10,000,000 per day, driving a massive innovation opportunity allowing business models that are based on huge numbers of tiny payments to come to life. This makes Bitcoin able to compete with payment processors such as Visa, MasterCard and Payal (Hearn, 2013, March). Importantly, Bitcoin was always designed to act as a plumbing system for a more efficient and secure way of doing trade and payments over the internet (Fortson, 2021, February 14).

This gives the system the capacity to scale to meet the needs of governments and industries the world over, each using it for their own needs and in their own way but making use of the common infrastructure the network represents. Through this scaling effect, we reach a system paradigm where the same proof-of-work system that secures every transaction in the AUD, Euro, USD, JPY and any other currency issued on the network would secure the data of individuals, corporations and more providing immutability and unbeatable security for all applications.

It is important to also understand that Bitcoin is not just a money system. In fact, the 'Bit' in Bitcoin represents its capacity to carry data. In Australia, several companies are already making use of this capacity, with the most notable example being WeatherSV (www.weathersv.app) who by using Bitcoin's low cost payment rails have crowdsourced the money to write over 120,000,000 weather readings to the Bitcoin public ledger since 2018. This weather data is secured on the public ledger and made immutable through proof-of-work timestamping, resulting in a database of weather information that is undisputable in its provenance. We see tremendous potential for Australia to lead the way in understanding and making use of this data capture and validation capacity.

Important also to understand is that the opportunity presented by Bitcoin is not speculative. While Bitcoin is an asset that can be bought and sold, the true opportunity comes from being free to build atop the set-in-stone protocol without risk of work being compromised by unwanted protocol changes made by 'open source developers' trying to make the system more 'decentralised'. It is built for businesses and governments to create new business opportunities and efficient services without having to re-write laws or create new regulations. Elas and our founders in no way endorse the purchase of Bitcoin as an investment for the purpose of speculation.

Triple Entry Accounting

As a further example of Bitcoin's potential, where countries issue their own currency as tokens running on Bitcoin, the opportunity to implement Triple Entry Accounting across the board is presented.

Triple entry accounting is an evolution of today's double-entry accounting systems where each transaction in the system is recorded and stored by a third party. Furthermore, even with IFRS Standards for transparency and harsher laws to hold accountants and auditors accountable, the double-entry accounting system and verifying the integrity of its financial records is costly and time-consuming (Cai, 2021). Ibanez, (2021, May 12) states that "A triple-entry accounting system requires a signed receipt to be held by three parties in three places. If the transaction pattern requires this, all of the parties must have signed the receipt. Bitcoin does this and, in this sense, it is triple-entry". When a cash system exists on Bitcoin, the transaction itself becomes the single source of truth for double entry books on both sides of the exchange. This represents a whole of industry evolution for the accounting profession and can lower the auditing costs for businesses. Wright (2019, February 24) when discussing accounting, states that, "Our system [Bitcoin] allows not only for the integration of the general ledger and accounting functions of a business but the complete integrations of business applications including project charts that can be displayed through linked Bitcoin smart contracts".

Bitcoin is a general-purpose transactional ledger suitable for the exchange of money, data, property and more. It represents an economy wide opportunity to deliver systems and services that far outstrip their ancestors in terms of their speed and efficiency, and with the right support, an economy wide effect can be generated in just a few years. While the internet took around 20 years to be integrated into business and the economy, this was through lack of infrastructure and connectivity. These barriers do not factor into the capacity of the economy to leverage Bitcoin, as the same infrastructure that connects us to the internet today connects us to the Bitcoin network.

This opens up a plethora of new opportunities in this new economy that otherwise would not have existed today. The velocity and high throughput of usage, the ability to conduct commerce in new ways opens up new services and business models which results in a better experience for consumers. These new business services and efficiencies will be attractive to participants being able to start a business with lower upfront costs by leveraging off the infrastructure of the Bitcoin SV network. The same applies to large enterprises or government services looking to conduct a digital transformation for the benefit of being more efficient, transparent and at a fraction of the costs. The incentives of this new technology creates new opportunities that encourages all participants to upskill their knowledge for their niche.

Barriers to the uptake of new technology

The vision of Bitcoin was of a single network forming a single record for global industry and finance. The design intent was for a highly scalable system that could accommodate an unbounded demand for access to the network using economic incentives to allow the network to form without the need for a centralised leadership or decision-making process.

These incentives only come fully to life once the network is at scale, creating a do-or-die situation for the network. Either it will become a global network, or it will fail.

Unfortunately, until now it has been held back by the emergence of competing blockchains which vie for the eye of the public in a speculative marketplace. This costs the industry tremendously in terms of the amount of development work being done to repeat the process of creating a blockchain, each trying to slightly bend the original idea to suit some specific purpose. It is important to know that Bitcoin was built to be general purpose and can accommodate all the same use cases.

Through this window, we can now show that there has actually been very little innovation in the cryptocurrency industry, with most ICO's serving as fronts for crypto-scammers to sell meaningless and worthless tokens to hapless investors via bucket-shop exchanges. Most ICO companies do not generate any actual intellectual property and most 'fail' when the original development team cash out their tokens and move on. The tokens, however, persist forever, being 'mined' by validators and giving the impression that work in ongoing when in fact it has stopped completely.

Case-in-point, the infamous meme coin 'Dogecoin' recently regained popularity through some level of celebrity endorsement, with the value of the network skyrocketing to the billions of dollars. This despite the fact that all of the original developers had left after publicly stating on record that it was created as a joke with no active development on the coin since 2016. (Asarch, 2021 April 15)

While much of the 'crypto' industry is appealing for less regulation, we believe that the regulators must step in and begin applying existing rules that protect consumers much faster than they are currently doing so to prevent any further loss of money. Since the ICO craze started, hundreds of trillions of new tokens have been created, mostly representing illegal securities, and almost all of which have fled from value highs to trade for just fractions of a cent, taking peoples funds and placing them into the pockets of the scam runners. This needs to stop.

Since 2016, the current blockchain landscape of the technology focus has centred around Ethereum smart contracts and private 'blockchain' consortiums. This current focus has proven to fall short of the promise to revolutionize financial operations and technological advancements in Australia as various proof-of-concept attempts continue to run into scaling issues, increasing cost issues and a lack of similar security mechanisms provided by proof-of-work systems like Bitcoin. As the Australian Computer Society (ACS) outlined in their report on blockchain challenges for Australia (2019),

> The identified challenges are scalability, security, regulation, education and employment. These challenges are of strategic importance, as blockchain promises not only to reshape the Australian economy but also to rethink business interactions within the Australian society.

We can show that these challenges can be met and are actively being met by Bitcoin, and through the efforts of industry bodies such as Bitcoin Association (www.bitcoinassociation.net).

Unfortunately, there is some contentious issues surrounding the concept of blockchain and DLT. There is certainly a need for a much broader brush if one is to truly understand revolutionary technology. For example, in an ACS (2019) report, it is unclear to us, how their interpretation of 'scalability challenges' apply to our understanding of Bitcoin:

> ...the growth in the number of computational devices and the geographical dispersion of their data poses a new challenge to maintaining integrity at unprecedented scale. Australia's connection to the rest of the internet is sometimes impaired by natural disasters or human misconfigurations, but reliable connectivity is necessary for blockchain systems to benefit Australia at a large scale. In addition, traditional blockchain systems, whose performance is capped regardless of the amount of participating resources, consume an amount of storage and energy that grows dramatically with the number of participants. This lack of scalability poses a threat to the sustainability of these blockchain systems.

Again, Bitcoin has viable solutions for all of these problems, some technological, some administrative, and all driven by the economic incentives that make Bitcoin so efficient at scale. Private transactions in offline environments are not a challenge for this system, thanks to its use of digital signatures as an evidentiary trail.

ASC (2019) also defines security challenges as:

> Blockchain aims at providing security guarantees, both through cryptography and consensus among participants, to alleviate the need for a central trusted authority. Blockchain systems are frequently attacked through various means. These attacks clearly threaten the privacy and assets of users. Implementing standards that deal with these vulnerabilities is needed for the protection of blockchain users. Australia has an important role to play through its organisations that are already actively engaged in blockchain standardisation.

Bitcoin's security model is almost entirely economic. While there are cryptographic techniques such as digital signatures used when transacting on the network, these are only used by the network's operators, or miners, to judge whether the transacting party is the owner of the coins or not. Without the capacity to scale, these cryptographic security functions are meaningless as it is the system itself that is rendered insecure and likely to collapse.

In the last 4 years, competing networks calling themselves Bitcoin have emerged, including BTC, BCH, BTG and others. Each claim to represent the original vision of Bitcoin, yet none actually operate according to the economic incentives outlined in the Bitcoin whitepaper of 2008. This is important as it is only through the nodes following these incentives that the network can truly scale and become a global network. There have already been multiple

instances of blockchains failing, and this will happen more and more as regulators begin to catch up with the cybercriminals who use them.

In reality, a massively scaled system becomes immune to even the most sophisticated attacks. Thanks to its distributed peer-to-peer nature, unlike the internet services of today Bitcoin has no central system to target. By using Bitcoin to deploy services, companies and individuals can receive that same distributed attack surface, vastly improving the security of our digital commerce systems, while saving cost at the same time.

Lastly, we will look at the opportunities for law enforcement and address the regulatory issues identified by the National Blockchain Roadmap.

Bitcoin is an immutable evidence trail. The immutability of a blockchain is similar to a Write once read many (WORM) data storage device. Organisations in Australia and in other countries must maintain secure backups of data stored offline or online. The Australian Cyber Security Centre suggests that "Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Bitcoin affects this transformation for all information related to data and money exchange but does so in a way such that it is not the responsibility of each company to pay a contracting service to build their own system, but where all companies and individuals use the same system, creating a massive cost saving and simplifying the entire process. This only works if the blockchain is public, as with consortium or private blockchains, this immutability can always be questioned, and the efficiency benefit of global scale is lost.

The National Blockchain Roadmap discusses identity as a key area for clarification, here we would like to discuss current laws surrounding electronic signatures within Australia and the EU and reasons why existing legislation can be applied for a plurality of use cases.

Bitcoin was always designed to work within the law. As such any activity that requires a signature must also apply to Bitcoin. Australia is a technology-neutral environment, since 1999 the Electronic Transactions Act (ETA) recognises Electronic Signatures as legally binding as long as certain requirements are met and that relevant exceptions do not apply. Digital signatures are different to eSignatures as they are a type of electronic signature that uses a specific technical implementation, for example DocuSign provides digital signatures that follow the Public Key Infrastructure Protocol (PKI) (DocuSign, n.d.). The eIDAS Public Key Infrastructure in the EU, is one of the regulation frameworks for electronic identification, which is based on a system of trusted third parties (Konashevych, 2020, April 28). Perhaps Australia can learn from the EU in this regard, as under the eIDAS regulatory framework there are clearer guidelines for verifying identity online. For example, an Advanced Electronic signature, which is based on an advanced certificate uniquely identifying the signer and must meet certain requirements under the eIDAS. Further, a Qualified Electronic Signature, is an Advanced Electronic signature but is created on a Qualified Electronic Signature Creation Device (QSCD) and the certificate issuer must be a Trust Service Provider. In Australia, the Trusted Digital Identity Framework is the

Government's standard for the verification of digital identity. We agree with the National Blockchain Roadmap that there should be a set of Standards for digital signatures. We see a future whereby Trusted Digital Identity Providers can act as a certified registry to validate root keys or public keys and a digital certificate, which would be similar the eIDAS regulation on Qualified Electronic Signature (Wright, 2019). Furthermore, Wright (2019) explains that,

> In this case the pseudonymous identity associated with the bitcoin transaction address can be privately associated with a registered identity certificate. When linked in this manner this could form an "advanced electronic signature" which is linked to the signatory and which is capable of identifying the signatory. The immutable nature of bitcoin also satisfies the requirements that the signature is linked to the data in any alterations made to the document be detected.

Advanced electronic signatures using Bitcoin would also satisfy the National Blockchain Roadmap's concerns about the immutability of blockchain ledgers and the need for data integrity. In any business organisation the integrity of data can usually be kept in check by having adequate tracing of identity and ensuring that signed contracts govern organisational policies in place surrounding data integrity. If data is found to be incorrect, the ledger can be updated with another transaction to record the change, like making an adjusting entry in an accounting system, the immutability of the system does not prevent this.

The policy environment facing neo-banks, through the window of the National Blockchain roadmap

With the correct technical implementation, it should be possible for neo-banks to implement banking services that use Bitcoin as a back-end service for tracking balances and deposits. This would then allow them to interface with public ledger-based PKI identity solutions allowing for the creation of a new type of KYC service where the person can identify themselves to the bank within seconds using documents signed and approved by the issuing government institution (e.g., dept of main roads signed digital driver's license). This can be taken one step further, allowing the banks to minimise their own access to private data, and reduce what they know about their customer to the bare minimum required by law. E.g., the applicant is over 18, and a citizen of Australia. This type of application is one of the very few situations where we would see that existing regulations could be modified to accommodate an innovative technology, as it creates a much more inclusive environment where any person with the legal right to banking services can access it with a minimum amount of stress.

This can be achieved through a clear understanding of the application of distributed identity (DID) tokens and digital signatures.

The use of Bitcoin for contracts with an evidentiary chain

Contracts can be executed on the Bitcoin blockchain as long as both parties to the contract are following governing laws within their jurisdiction. The Bitcoin SV blockchain is capable of storing data that can only be seen by the parties involved in the exchange using cryptographic methods to restrict and allow only authorized access. Wright (2019, p.3.)

explains that, “The parties to an exchange considered over a bitcoin based system is able to embed EDI and other standard electronic documentation methods or even to link a series of external contracts and terms to a transaction”. Master agreements can be linked and displayed on a screen, which satisfies the existence that a relationship existed between parties (Craig, 2019).

Through this framework, it is possible to see that all manner of inter-party contracts, from user terms and conditions to employment contracts and confidentiality agreements, up to international treaties, free trade agreements and more can be captured and stored on the Bitcoin ledger, giving all stakeholders the knowledge that their agreement was agreed to and signed as it is recorded on the ledger, and making it impossible for that moment to be compromised. It is important to understand that while records made are ‘immutable’, documents can be superseded using version control systems such as we have today. This is part of the design of the system and in no-way impacts the existant rules and regulations surrounding contract law.

Privacy and Bitcoin

One concern identified by the National Blockchain Roadmap (2019), is that pseudonymity does not necessarily protect blockchain users privacy and that blockchain systems will need to comply with the privacy Act 1988. While there are clear concerns here for blockchain users, privacy breaches are an ongoing concern in our current digitalized world. Customer data and personal information is often obtained by hacking into computer networks. A 2019 survey of 10 000 people found that 25% of respondents had experienced misuse of their personal information at some time during their life. (Franks and Smith, 2020). These data breaches lead to identity crime that costs Australian citizens time and money. In 2018 the Australian Parliament enacted the Privacy Amendment (Notifiable Data Breaches) Act 2017. This act requires organizations to notify any individuals likely to be at risk of harm due to a data breach so that individuals can take action and be more aware of possible attacks. Franks and Smith (2020, p.14) in their 2019 online survey into identity crime found that the most predominant data breach resulted from a computer hack, the second most common breach was through emails and the third through phishing emails. It is evident that, data has value, and that current systems are far from private and that privacy provisions outlined by the Privacy Act 1988 need to be followed to maintain and increase privacy online. A similar principle can be applied to the pseudonymous nature of a public blockchain. While transactions are public they are not connected to the user’s identity and public keys should remain anonymous. If public keys are not re-used privacy is increased (Nakamoto aka Wright, 2008). Other provisions can be included to increase privacy such as the use of in-private shared key generation techniques such as Diffie Hellman key sharing (Wright, April 2021) which allows two users to establish shared keychains in an off-line manner, suitable

for encrypted communication, data exchange and the facilitation of transactions on the Bitcoin blockchain.

If privacy is breached there is often no responsible party to seek remedy from, so employing techniques where users are able to autonomously set the parameters under which their communications take place, make it much harder for that information to be compromised due to the lack of any central server or location to attack.

While it is true that all data is recorded immutably on the blockchain, this does not mean that it must be stored forever. Section 7 of the Bitcoin Whitepaper 'Reclaiming Disk Space' outlines techniques by which blockchain miners are able to purge particular transactions either because it doesn't make economic sense to keep them, or through instructions by law enforcement. This aspect of Bitcoin can be used to perform purge operations within service provider data warehouses, and the use of 'Crypto-shredding' whereby service provider keys which can access user data are provably destroyed can be employed to meet any and all requirements of global privacy legislation such as are outlined in the European GDPR regulations.

Risks in the digital asset and cryptocurrency sector

In the current environment of multiple incompatible and ever evolving blockchain projects that each present their own version of a digital asset and blockchain, the main issue is that there really is no such thing as an asset that is purely digital. Even the native satoshi tokens that are exchanged on the Bitcoin network confer the owner a real world right to purchase access to the Bitcoin ledger, through services operated by miners. Many so-called digital assets represent no such right, existing solely as a token tradeable via bucket-shop exchanges in a speculative market. This speculation market does represent a risk to financial markets and Australian consumers, as due to the ephemeral nature of the 'value' being exchanged, large parts of the market crash very rapidly, collapsing investor holdings to tiny fractions of the original without rhyme or reason.

Further to this, we have seen since 2016 the rise of so-called stable-coins which are typically used by crypto bucket-shops as a stopgap holding token, allowing users to trade one cryptocurrency for a token that is ostensibly valued at 1USD, and allowing them then to purchase another cryptocurrency for the same value. The main issue with these tokens is that they are unregulated, and there is considerable evidence that despite there being issuances now totalling several tens of billions of dollars of US pegged tokens, there are not even single billions of dollars backing the tokens. The most prevalent examples are USDT, a.k.a. USD Tether, and USDC, a.k.a. USD Circle. These currencies are actively used in crypto markets here in Australia including BTC Markets (www.btcmarkets.com), CoinSpot

(www.coinspot.com.au) and Independent Reserve (www.independentreserve.com) which together represent a sizeable proportion of all crypto market speculation taking place in Australia and facilitated by Australian companies.

Significantly, USDT (Tether) has been under active investigation by the New York Attorney General and have consistently failed to meet audit and reporting requirements asking to provide proof that the 60Bn tether coins in circulation are in fact backed by USD. The lack of evidence of this backing will lead to the closure of the scheme, which will have an immediate impact on Australian investors holding the coins at the time. There won't be a gradual collapse of USDT (Tether) prices. They will go to zero instantly and as such represent an existential threat to the wealth of Australian individuals being exposed to these 'assets'.

To conclude, the main risk to this industry is the industry itself. Despite trying to exude the appearance of appealing to governments and regulators, there has been a consistent and ongoing denial of legal requirements, and total lack of regard for regulations and the normal checks and balances required to operate in a similar space. When choosing to regulate this industry, Elas recommends that the balance tip in favour of community protection rather than allowing these flimsy scams to proliferate further.

References

Asarch, S. (2021, April 15). *Dogecoin's cocreator explains how the 'parody' currency turned into a billion-dollar movement*. Business Insider Australia. https://www.businessinsider.com.au/dogecoin-go-back-down-right-now-price-livee-billy-markus-2021-4?r=US&IR=T

Australian Computer Society, (2019, May). *Blockchain Challenges for Australia.*

Australian Cyber Security Centre, (2020, June). *Essential Eight Maturity Model.* https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

Cai, C.W. (2021). *Triple-entry accounting with blockchain: How far have we come?* Accounting and Finance 61. https://onlinelibrary.wiley.com/doi/epdf/10.1111/acfi.12556

Department of Industry, Science, Energy and Resources. (2020, February). *National Blockchain Roadmap*. https://www.industry.gov.au/data-and-publications/national-blockchain-roadmap

DocuSign. (n.d.). *FAQ*. Retrieved June 23re, 2021, from https://www.docusign.com.au/products/electronic-signature

Fortson, D. (2021, February 14). *Craig Wright: 'I invented bitcoin – now it's a Ponzi scheme'.* The Sunday Times. https://www.thetimes.co.uk/article/craig-wright-i-invented-bitcoin-now-its-a-ponzi-scheme-hkrv75clr

Franks, C. & Smith R.G. (2020). Australian Institute of Criminology. *Identity crime and misuse in Australia: Results of the 2019 online survey.* *https://www.aic.gov.au/sites/default/files/2020-08/sr27_identity_crime_and_misuse_in_Australia_results_2019_survey.pdf*

Hearn, M. (2013, March 07). Ian, *Satoshi did plan for Bitcoin to compete with PayPal/Visa* [Online Forum Post]. Retrieved from https://bitcointalk.org/index.php?topic=149668.msg1596879#msg1596879

Ibanez, J. et al. (2021, January 20). *The Efficiency of Single Truth: Triple-Entry Accounting.*

Konashevych, O. (2020, April 28th). *Is Europe's Experience in E-Signatures and Digital IDs Valuable for Australia?* Cointelegraph. Retrieved from https://cointelegraph.com/news/is-europes-experience-in-e-signatures-and-digital-ids-valuable-for-australia

Nakamoto, S. (a.k.a., Wright, C.). (n.d). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://craigwright.net/bitcoin-white-paper.pdf

Ontier. (2021, June 29). *UK Court awards Bitcoin creator default judgement in Bitcoin copyright infringement claim*. https://www.ontier.digital/post/uk-court-awards-bitcoin-creator-default-judgment-in-bitcoin-copyright-infringement-claim

Qureshi, H. (2021). *The Original Bitcoin Protocol: What is it and Why Does It Matter?* MNP. Retrieved from https://www.mnp.ca/en/insights/directory/the-original-bitcoin-protocol-what-is-it-and-why-does-it-matter#

Wright, C. (2019). *An evidentiary framework using bitcoin and smart contracts in a manner that constitutes a signed written agreement in commercial transactions*. Academic International Conference on Interdisciplinary Legal Studies, Oxford, UK.