May 2019

Blockchain Challenges for Australia

An ACS Technical White Paper

Contributors

Nick Addison	ConsenSys
Samuel Brooks	Block8, Standards Australia
Katrina Donaghy	Civic Ledger
Mark Ebeling	IBM
Scott Farrell	King & Wood Mallesons, Standards Australia
Vincent Gramoli	ACS, University of Sydney, CSIRO's Data 61
Adrian Lawrence	Baker & McKenzie
Marc Portlock	ACS
Mick Motion-Wise	ITG
Bridie Ohlsson	AgriDigital
Beth Patterson	Allens Linklaters, Standards Australia
Philippa Ryan	ACS, University of Technology Sydney, Standards Australia
Mark Staples	CSIRO's Data 61
Ingo Weber	CSIRO's Data 61
Tom Worthington	Australian National University, ACS

Workshop note-takers

Anna Chen Fang	University of Technology Sydney
Tyler Crain	University of Sydney
Ethan Huang	University of Technology Sydney
Simonna Malki	University of Technology Sydney
Chris Natoli	University of Sydney
Charlotte Reed	University of Technology Sydney

Workshop conveners

Vincent Gramoli	ACS, University of Sydney, CSIRO's Data 61
Marc Portlock	Australian Computer Society
Philippa Ryan	ACS, University of Technology Sydney, Standards Australia

Foreword

Yohan Ramasundara
President, ACS

Andrew Johnson
Chief Executive
Officer, ACS

Few technologies of the last decade have sparked as much interest as blockchain. Its revolutionary potential has excited ICT professionals and business leaders alike.

Unfortunately for its evangelists, however, it still hasn't crossed the line into broad acceptance. It has yet to cross that threshold of trust that will let it live up to its vaunted potential. Up until now, blockchain implementations beyond cryptocurrency have been small, scattered and experimental, with game changing applications still elusive.

That, however, has not dimmed the enthusiasm of the world's businesses or developers. The upside potential of blockchain is so incredible, so transformative that there's still a tremendous amount of effort going into making it work. Cumulative venture capital funding in blockchain has increased dramatically, up from AUD$1.9 million in 2012 to AUD$7.6 billion as of November 2018. There are 14 job openings for every blockchain developer, and a 28-fold increase in the number of people citing cryptocurrency skills on their resume since 2013. The global market for blockchain products is predicted to exceed $21 billion by 2024.

The good news for Australia is that we're already a world leader in the technology. In November, ACS released Blockchain Innovation, a report that revealed Australia ranks a notable sixth in the world when it comes to ownership of blockchain patents. Australia is managing the International Organization for Standardization's blockchain standards committee and we're home to projects like the Red Belly Blockchain, one of the most advanced blockchain projects in the world.

ACS has a vision for Australia to be a world leader in technology talent, fostering innovation and creating new forms of value. To support achieving this vision, we have a focus on the innovative creation and adoption of best of breed technology in Australia.

What we wanted to find out when it came to blockchain is what would be needed to cross the barrier of acceptance? What challenges are holding the technology back, and how do we, as ICT professionals, solve them in order to realise the tremendous potential of the technology?

To answer those questions, we turned to the Blockchain Committee of ACS' Technical Advisory Board, which includes some of Australia's leading blockchain experts. The committee is led by Vincent Gramoli, one of the creators of the Red Belly Blockchain, and it produced the whitepaper you're reading right now. We'd like to thank the committee for its time and effort, and we hope that it can serve as a first step in solving the blockchain dilemma for Australia.

Please enjoy.

Contents

Executive summary

Bitcoin gave birth to the blockchain technology ten years ago. Blockchain promises to disintermediate interactions between individuals by offering security of exchanges without relying on a central authority of trust. As a result, blockchain has been trialled in various sectors ranging from finance and insurance to energy.

A decade later, Australia is at the forefront of blockchain technology in terms of regulation, research and industry applications. Among many achievements, its standards organisation has been chosen to lead the secretariat of blockchain standards for the ISO[1]; ARC-funded research has produced one of the most scalable blockchain systems[2]; and the World Bank chose an Australian bank to implement the first blockchain-based bond.[3]

Yet, blockchain poses significant challenges that prevent Australia from fully exploiting its promised benefits for our economy and society. This technical white paper identifies some of the predominant challenges for applying blockchain technology in different contexts in Australia and proposes technical directions to overcome these.

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.

The directions that this technical white paper explores for solving these challenges include the analysis of use cases; the education of key actors; the exploration of blockchain development, especially surrounding consensus; and further understanding of regulations. They specifically include assessing the requirements for each use case in terms of speed, volume, scalability and security, in order to identify the most appropriate blockchain proposal for a given application. They also include a roadmap to help technical and legal professionals interact on specific topics.

Introduction

Blockchain has the potential to disrupt our economy and society in a radical way by simplifying the transfer of digital assets between individuals.

Blockchain emerged only a decade ago with the release of the Bitcoin system, but it builds upon much older research areas, including cryptography and distributed systems. Despite being in its infancy, blockchain already allows individuals to transact between one another through a distributed system of computers, bypassing traditional intermediaries, automating processes, and reducing time as well as financial costs.

Half a century ago, nobody predicted that networking individuals through a distributed system of computers would allow dissidents to bypass censorship in expressing themselves, or producers to bypass distributors to reach their consumers directly. Yet, the US military funded project ARPANET, which became the internet, has facilitated these types of disruptions. One could thus reasonably expect that blockchain will experience the same network effect as the internet in the near future.

As blockchain technology matures, its security strengthens, its performance improves, and standardisation efforts multiply. Yet, there remain key challenges that every country has to address in order to embrace the promises that blockchain offers to the economy and society. The goal of this technical white paper is to identify some of the predominant challenges that blockchain poses to Australia and to propose technical directions to overcome these challenges and facilitate the adoption of the blockchain technology by the Australian economy and society.

A. WHAT IS A BLOCKCHAIN?

Blockchain has been used as a keyword to denote two different things: *a data structure*, a specific format for organising and storing digital information; and *a computer system*, the result of the collaborative execution of a specific program on a distributed set of computers. The blockchain data structure, on the one hand, is a chain of blocks similar to the linked list that is usually taught to undergraduate computer science students. The blockchain system, on the other hand, is the distributed execution of a common program by a set of computers at typically different locations and connected by a communication network, instead of a central and trusted computer.

The system implements the data structure, in that during its execution, computers generate new data, exchange this data through the network and try to reach a consensus on the block that they append to the linked list. The data consists of transactions or smart contracts, each indicating how digital assets are being transferred between accounts. The accounts are owned by individuals or users, and transactions are typically generated as a result of an order from one of these users to transfer some of her own assets. Due to its distributed nature and the transactions it stores, the blockchain system is also commonly referred to as a *distributed ledger*.

2008

B. A DECADE OF EVOLUTION

The blockchain system has already evolved through major stages or generations, offering different and more complex functionalities at each new generation. The different generations of the blockchain evolution can be summarised as follows:

BLOCKCHAIN
1.0

The first generation of blockchain systems was proposed in 2008 in the seminal bitcoin white paper.[4] These blockchain systems allow users to issue transactions written in a restricted scripting language to transfer digital assets between participants. New transactions are encapsulated into blocks appended to the chain by miners. The blockchain forks when miners append different blocks at the same index, requiring the miners to reach a consensus later on.

BLOCKCHAIN
2.0

A second generation of blockchain supporting 'smart contracts' was proposed with Ethereum in 2014. Smart contracts are general programs that offer more expressiveness to users than transactions, and users can upload smart contracts to the blockchain and invoke them. The development of smart contracts led to the generic notion of *decentralised applications (DApps)* interacting with the blockchain data structure and whose interface can typically run within a browser.

BLOCKCHAIN
3.0

Newer blockchain systems that aim at improving scalability, interoperability, governance, privacy or sustainability are often considered part of this third generation of blockchains. This generation includes blockchains that better integrate with an interactive version of the web.

References have also been made to newer generations of blockchain, sometimes to indicate that there is a better integration of blockchain in production.

C. A BROAD INTEREST

The growing interest in blockchain led to a very large number of blockchain system proposals and an increase in the complexity of the potential industrial use cases. In a recent survey run by ACS, we observed that more than 83% of the respondents were aware of the applications of blockchain outside cryptocurrencies. More surprisingly, we noticed that more than 20% of the respondents were considering the use of blockchain technology in their organisation or had already deployed blockchains. Although the survey questioned tens of thousands of individuals, we counted around a hundred responses, which limits the statistical relevance of this number, but the response still reflects a broad interest in blockchains. In particular, the respondents represented various sectors as indicated below.
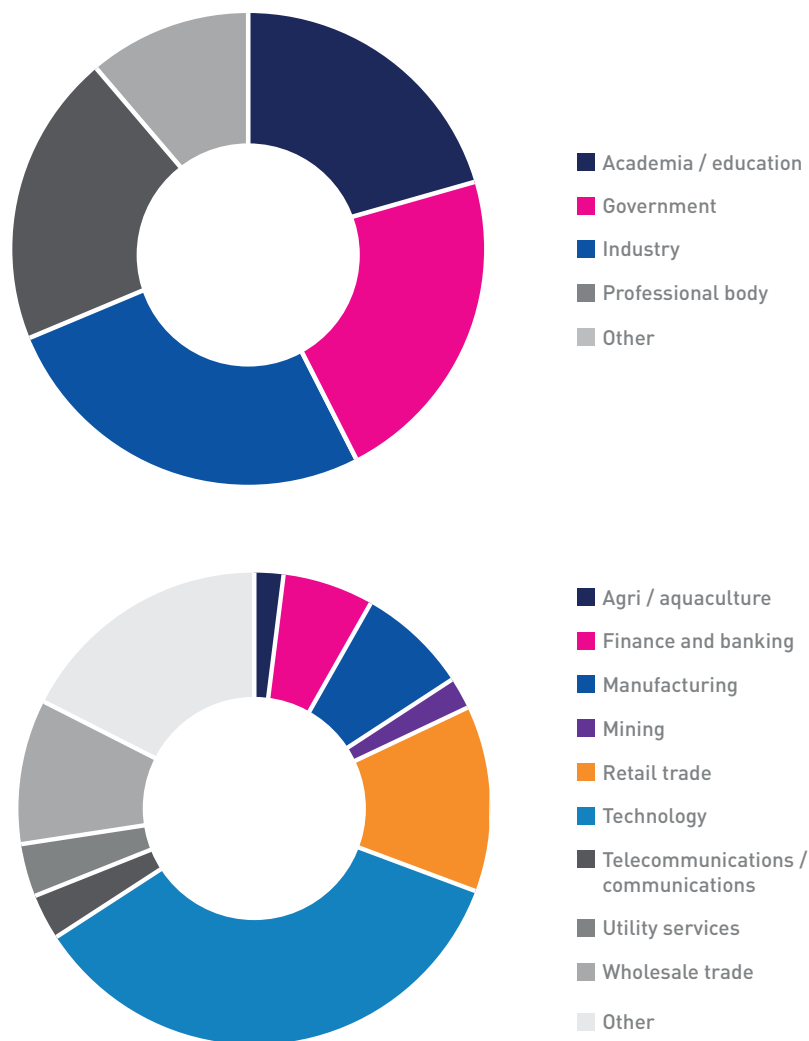

Figure 1 – Among diverse industries and sectors, more than 20% of respondents are considering or have already deployed blockchain technology in their organisation

As blockchain is being tested for more and more critical use cases around the world, it has become important to assess the challenges that blockchain raises for Australia and provide clear directions to rapidly and effectively address these challenges. This will allow Australians to benefit from its promise for the economy and society.

D. THE CHALLENGES

This technical white paper focuses on five key challenges that Australia faces in relation to blockchain: scalability, employment, education, security, and regulation.

Scalability

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.

Security

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.

Regulation

There is a serious lack of clear governance, not only in terms of rules for compliance with legislation and regulation processes, but also to provide clear guarantees to users, regarding issues such as privacy and ownership. This is especially true in Australia where privacy is governed by the *Privacy Act 1988* (Cth)[5] rather than being a general right. Finally, measuring the extent to which 'code' can be considered a legal agreement between parties remains unclear and untested in court.

Education and employment

As one of the largest exporters of education, Australia would benefit from more education in blockchain. The growing demand for engineering and technical skills includes the blockchain sector.
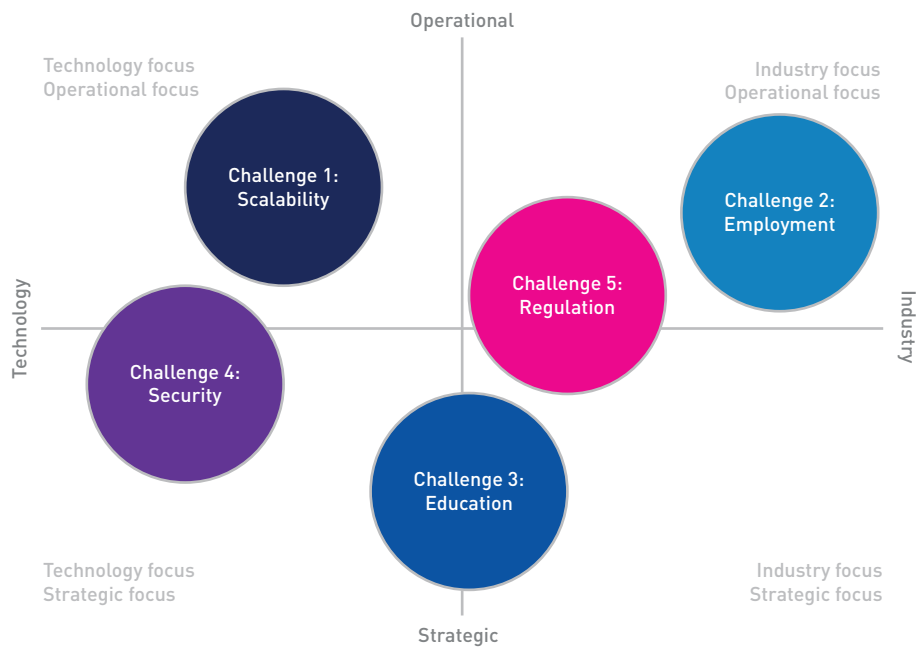
Figure 2 – Five challenges that Australia faces in relation to blockchain

As depicted in Figure 2, the challenges are diverse in nature and typically span different regions of the operation–strategy spectrum. As an example, an education challenge is more strategic than a scalability challenge, as it typically focuses on the long-term goal of adequately preparing new generations to become experts in blockchain technology; whereas the scalability challenge aims at optimising blockchain software to perform well when the number of the blockchain users increases.

Finally, some challenges are very industry focused while others are mainly technology focused. For example, the regulation of blockchains has implications for the way businesses will make use of blockchain technology and offer blockchain services; whereas the security challenge will likely be met with solutions that are technical, for example a software update to the latest encryption scheme that does not yet have any known vulnerabilities.

In the following sections, we explain why each challenge matters to Australia, identify sub-problems of each challenge and offer a set of suggestions for how to address these problems. We conclude this technical white paper with a glossary of key terms.

01
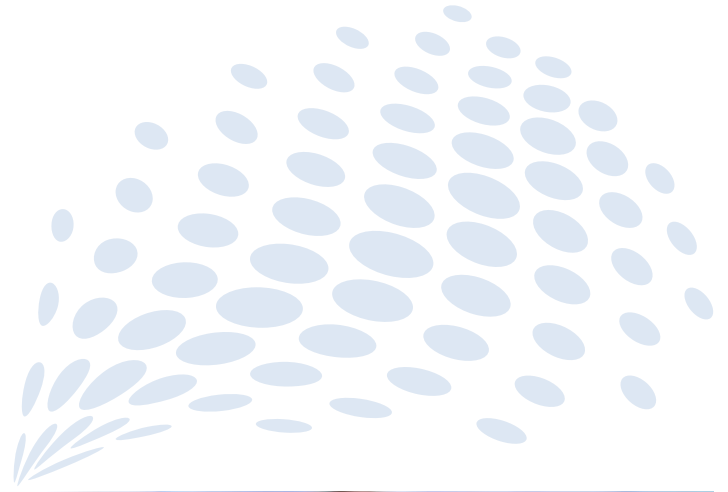
Scalability

The scalability challenge is to ensure that blockchains and distributed ledger technologies are capable of interconnecting individuals at unprecedented scale.

The use of blockchain and the benefits of a decentralised system are currently limited by the challenge of scalability; the predominant blockchain systems are confined by the costs of energy as well as by the trade-off between performance, security and trust.

A. WHY IT IS A CHALLENGE FOR AUSTRALIA

The growth in the number of computational devices and the externalisation of data poses a new challenge: to maintain integrity at unprecedented scale.

What problems do we face in trying to address this challenge?

Booming sectors, like IoT, need infrastructures to maintain performance and auditability of data, as the number of devices grows to unprecedented scale. The challenge lies in providing guidelines about the development of scalable blockchains which can face the challenge of performing worldwide.

- As a recent report observed, the capital costs associated with purchasing specialised mining hardware may be substantial.[6] The advent of proof-of-work blockchain technologies has incentivised a large number of users to specialise their hardware; by maximising the mining performance of their computers, users can obtain an increase in the reward from the corresponding blockchain systems. This trend will likely intensify as long as similar mining strategies remain profitable.

- The operational performance and ability to scale the ledger will rely on the choice of consensus mechanism.[7] Various consensus protocols have been explored since the 1980s, when the problem was first formalised by the distributed computing research community.[8] Several solutions, applicable to distinct environmental models, have different measures of communication and time complexities. A better understanding of the complexities of these consensus proposals is necessary before integrating them in blockchain systems.

- There is a lack of agreed performance criteria.[9] Performance of a blockchain system can be expressed as the number of requests it can handle per unit of time; the time it takes on average to treat one request; or as the guarantees offered by the system when the request has been successfully executed. The notion of scalability itself has several meanings; for example, stating that performance should not degrade, either as the geographical scale increases, or as the number of participants increases. A unified terminology is thus necessary to effectively combine efforts towards improving blockchain solutions.

Why are these problems related to Australia?

Blockchain technology aims to connect machines and users around the world. It promises potentially critical, scalable services that are globally accessible across the internet. The geographical isolation of Australia from other countries is in contrast with this inherent openness, and can affect the quality of its internet communications with major hubs.[10] Such quality degradations at large scale typically impacts the security of blockchain applications running in the regions partitioned from the rest of the network.[11]
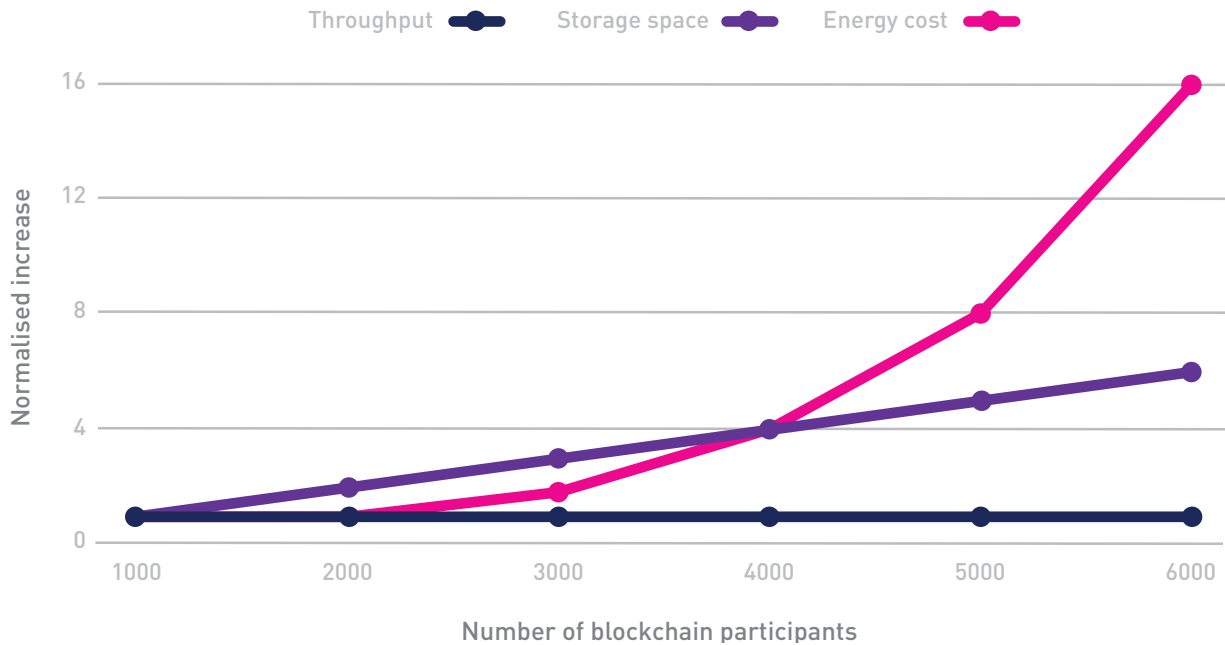
Figure 3 – The performance (e.g., throughput in transactions committed per second) of proof-of-work blockchains does not necessarily increase but consumption of resources (e.g., storage and energy) can increase as the number of participants grows
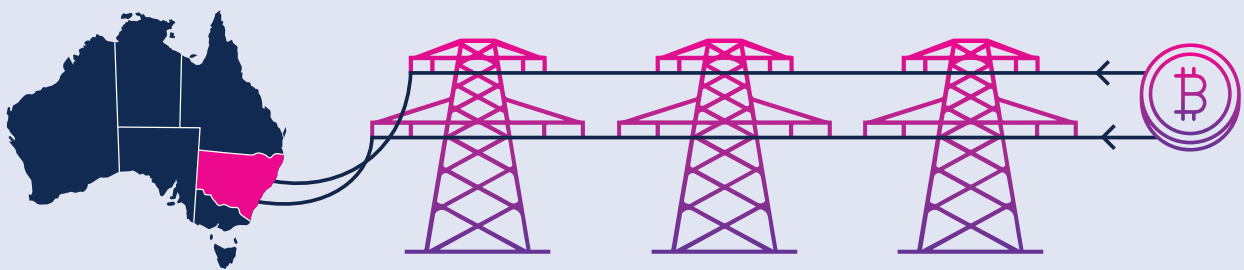
SCALABILITY

At its peak in late 2018, it's estimated that the Bitcoin network had an annualised energy consumption rate of 73 TWh. For comparison, that's more than all the electricity needs of NSW.

B DEFINING SCALABILITY

Scalability is a desirable aspect of a distributed system and can be defined depending on another property as follows:

Def 1. *(Scalability): the ability for a service to maintain or improve a property as its size grows.*

The desired properties of blockchain scalability depend on the considered use case. The property can be low latency, expressed as the average time required to commit a transaction; high throughput, expressed as the number of transactions that the system can commit per second; or security, expressed as the risk that digital assets are lost or stolen.

Figure 3 illustrates the scalability problem that classic blockchains face, where an increase in participants does not necessarily translate into improved performance (e.g. throughput as the number of transactions committed per second) but does translate into increased consumption of resources, such as storage and energy.
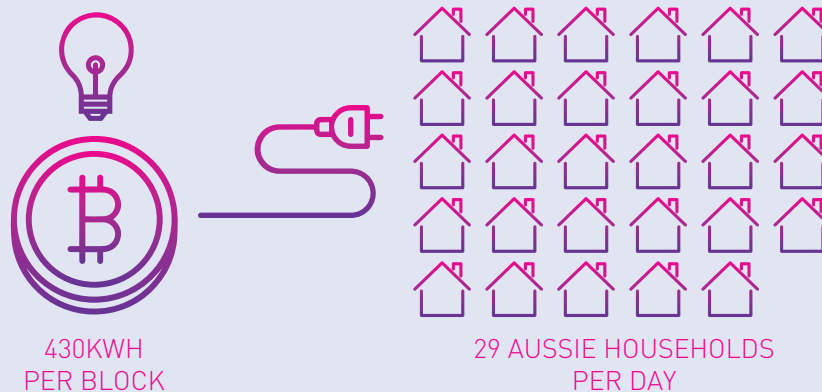
Energy consumption

Typically, some blockchain systems rely on proof-of-work to limit the rate at which blocks are appended to the blockchain. For example, Bitcoin creates a block every ~10 minutes in expectation of the completion of a proof-of-work. The action of mining consists of solving a crypto-puzzle, whose difficulty is dynamic, in order to provide this proof-of-work. As these blockchain systems tend to incentivise the participants to mine by offering them rewards, the resulting growth in number of participants often translates into a growing amount of computational resources dedicated to solving the crypto-puzzle.

To keep the period between blocks close to 10 minutes, the difficulty of the crypto-puzzle has to increase linearly with the available computational resources; this translates into an increase in energy consumption.

The competitive nature of the proof-of-work, which rewards only the winner of the crypto-puzzle, leads participants to outmatch the computational capabilities of one another by acquiring specialised hardware or by building mining farms. This increases energy consumption even further than originally needed. This race towards computational power typically leads to a superlinear ratio between the energy consumption and the system size growth.

ENERGY CONSUMPTION

At present, the largest blockchain network – Bitcoin – consumes 430KWh per block committed. This same energy could power 29 average Aussie households for a full day.


430KWH
PER BLOCK

29 AUSSIE HOUSEHOLDS
PER DAY

Sources: energy.gov.au & digiconomist.net

In a proof-of-work blockchain, the difficulty of the problem – and the energy required to solve it – will increase or decrease with the number of miners.

In turn, power consumption will affect mining profitability, and encourage or discourage miner participation.

NUMBER OF MINERS

PROOF-OF-WORK DIFFICULTY

POWER CONSUMPTION

MINING PROFITABILITY
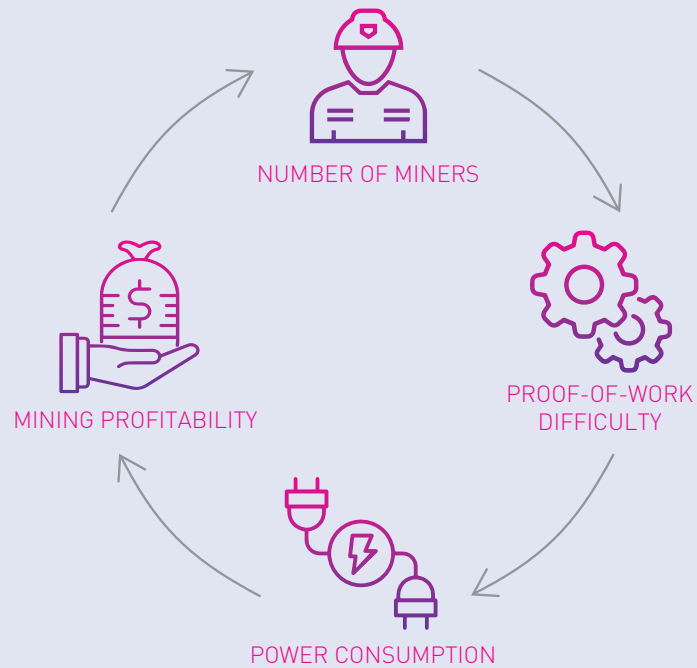
Storage needs

These blockchain systems also require a participant to download the full blockchain in order to be aware of the latest state of the blockchain. The inherent permissionless nature of the blockchain prevents participants from trusting one another when requesting the latest state; each participant has to make sure that the blockchain integrity is preserved down to the genesis block. It follows that cumulative storage dedicated to the blockchain service grows linearly with the number of participants.

Some devices do not meet the requirements of blockchains and cannot fully synchronise, due to the length of time it takes to replay the transactions. This was the case in Ethereum, which experienced denial-of-service attacks through the repetition of the EXTCODESIZE opcode to execute multiple slow reads to the disk. Lack of synchronisation can also occur because the storage space available is not sufficient to store the blockchain.

The Ethereum protocol offers the possibility of avoiding the need to replay the entire set of transactions, and to download a smaller subset of the blockchain. The drawback is that the device that cannot download the full blockchain and replay all transactions may obtain an inconsistent view of the current state of the blockchains, introducing security vulnerabilities.
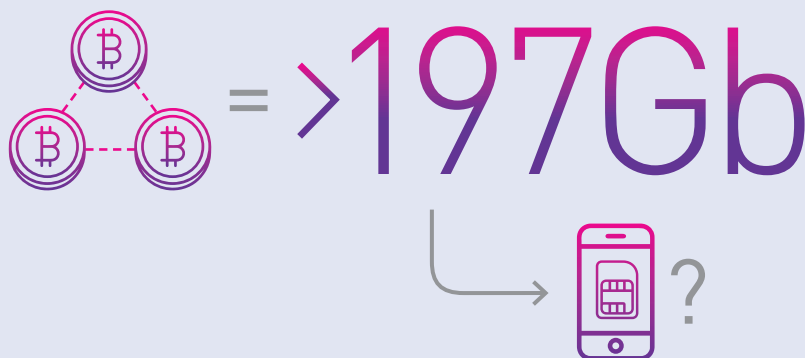
= >197Gb

STORAGE NEEDS

In January 2019 the size of the Bitcoin blockchain exceeded 197Gb (and it can only get larger). This exceeds the storage capacity of most mobile devices and means that not every device can fully participate in the blockchain.

The scalability limitations of performance

Paradoxically, increases in storage size and in computational needs do not necessarily translate into performance (e.g. throughput) improvement. For example, Bitcoin has a period between two blocks that is generally higher than D = 9min15sec.[12] As it keeps the size of its blocks to a maximum of B = 4 MB[13] and its transactions are generally larger than T = 400 bytes[14], it is limited by a maximum capacity throughput of B/(TD), or 18 transactions per second.

As scalability relates to a particular property, it is important to understand the property requirements of various use cases.

C. UNDERSTANDING USE CASES

Whether or not a particular technology is appropriately scalable depends on the use case; different applications will require different technical properties, depending on the application. Hence, a practical discussion on scalability must start with an analysis of the requirements specific to the application. Once the requirements are known, we can engage in a process of trade-offs with the technical properties, in order to develop a solution that is technically feasible. To this end, in the remainder of this document, we distinguish 'scalability properties' and 'system requirement properties'. All properties defined below have scalability dimensions that are purely technical in nature (and so are easily defined and measured).

Client and user count: While user count may be influenced by trust requirements (for example, in a highly critical system, all participants may require all transactions are locally verified), the number of users for a given system can be treated as a raw system requirement. An IoT application, for example, may have a requirement for many network clients (more than human users).

Storage: The amount of storage space required by a single network node increases with the number of participants replicating the blockchain. A blockchain like Bitcoin, that reached 173 GB in June 2018[15], would need close to a petabyte of storage space to be replicated on 5000 machines.

Compute: Ensuring that the computational power needed by the blockchain system does not grow unreasonably large as the number of participants increases is important to applications. Rather than incentivising all machines to be miners, validating transactions, one could potentially segregate machines into distinct roles, with some miners validating transactions and some clients issuing transactions.

Latency: The time taken between the issuance of a transaction and its commit. It increases as the system grows geographically and with the number of participants, so limiting the growth of latency is a key technical challenge.

Throughput: The number of transactions committed per second, or data items stored per second, should not drop as the system grows. Maintaining a minimal throughput as the system grows typically requires efficiently leveraging the existing network bandwidth, which is a limited resource.

Use case requirements	Priority					
	Computational power	Low latency	Volume of data storage	Data throughput	Number of users	Number of clients
Provenance – high-value items (e.g. diamonds)	L	H	M	L	M	L
Provenance – low-value items (e.g. pork)	L	H	H	M	H	M
Micropayments	H	H	H	H	H	H
Large-value payments	L	M	L	L	L	L
Uber	M	M	H	M	M	M
Clinical trials	M	L	M	L	L	L
Prescriptions	M	M	H	M	H	M
Software audit (monitoring of software processes)	L	H	M	L	L	L
Education/ micro-credential	L	M	H	L	H	M

H: High   M: Medium   L: Low

Figure 4 – Example of scalability requirements of blockchains depending on the targeted use case (H: High, M: Medium, L: Low)

As indicated in Figure 4, the scalability requirements of blockchains depend on the targeting use case. Various use cases require different properties from a blockchain system. For example, a high-value item whose provenance is recorded or tracked by a blockchain would involve only a low number of clients and users, due to the nature of its niche market.

By contrast, the provenance of lower value items will typically need to cope with more clients and users. The latency is typically of high importance for these two use cases as provenance tracking requires a constant monitoring, in quasi real time, of the location of the item being tracked. This latency will not be as important in the educational context (where users obtain micro-credentials) due to the long duration of the process leading to graduation. Other use cases, like micropayment, will differ due to the high frequency of requests, requiring that a large volume of transactions can be handled per unit of time (or volume of data storage).

D. ACHIEVING SCALABILITY

One interesting solution to cope with the aforementioned scalability issues is getting rid of proof-of-work. Proof-of-work consists of selecting nodes that are legitimately proposing a block to be appended to the chain; however, this limits the throughput and latency of blockchains.

Several consortium blockchains already cope with this waste of resources by assigning the roles of creating block to a predetermined set of nodes, instead of requiring nodes to provide a proof-of-work to append a block. However, these consortium blockchains do not offer the same level of openness as public blockchains, because they do not allow nodes outside the predetermined set to create blocks.

Other blockchains recommend the use of sharding, which allows participants to create blocks faster (in parallel), while a new class of Byzantine fault-tolerant blockchains aim at relying on fundamental results of distributed computing to cope with potential malicious behaviours. The drawback is that classic Byzantine fault-tolerant solutions were typically not designed to scale to large systems.[28]

Australian Research Council funded research recently led to the Red Belly Blockchain, that has already demonstrated high performance by scaling to 1000 machines distributed across four continents.[16] It is neither a consortium blockchain nor a public blockchain. Rather than incentivising all nodes to mine the same block, it allows any node to mine selected blocks.
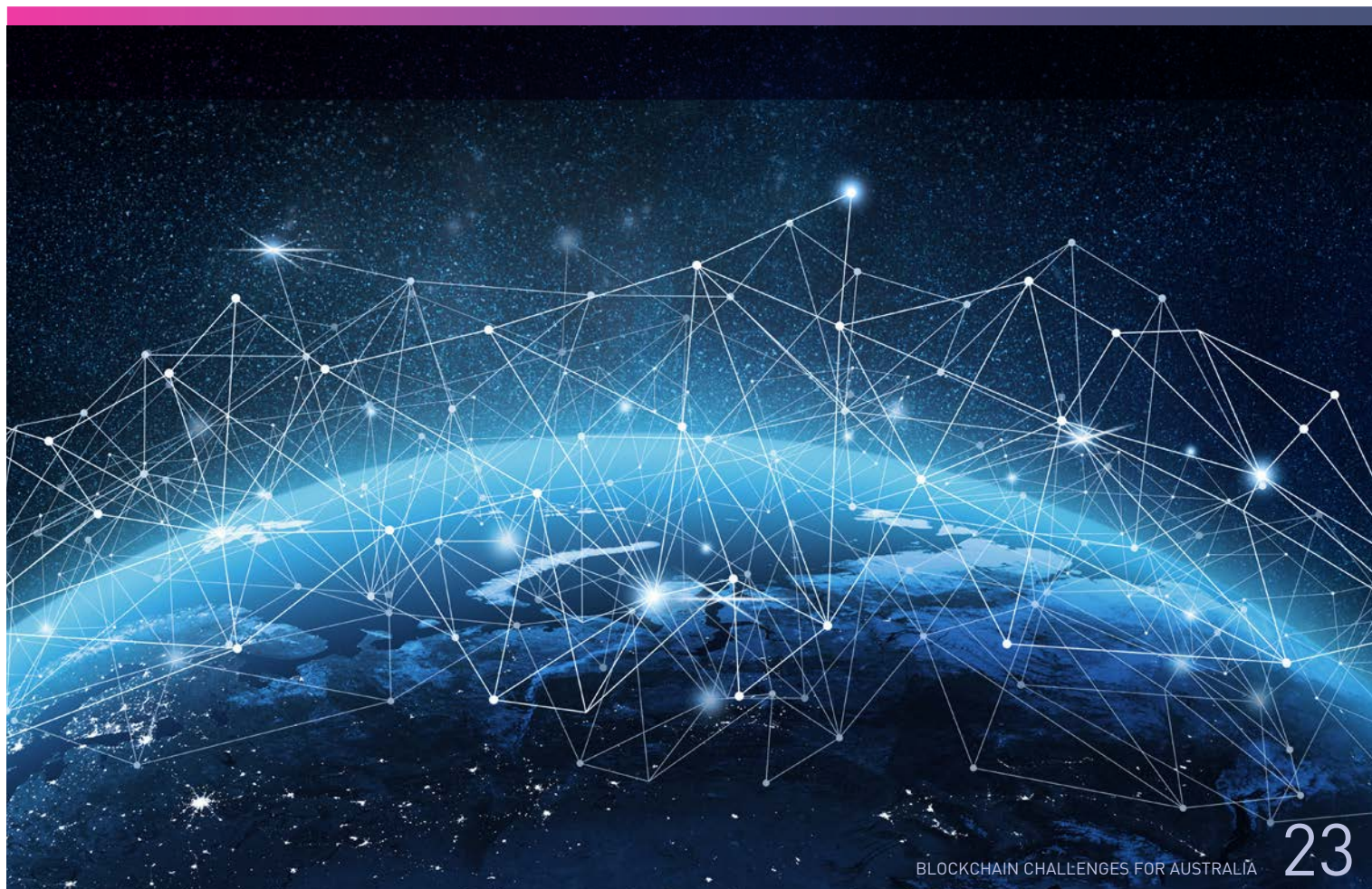
02
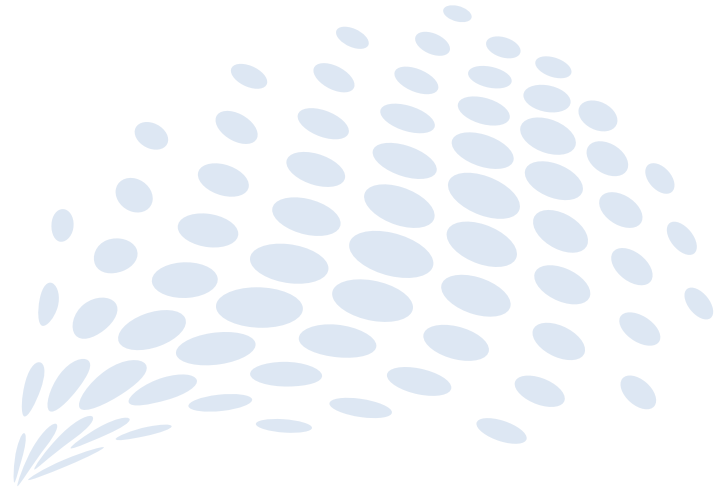
Security

Instead of using a trusted central authority, blockchain uses security mechanisms guaranteeing, on the one hand, that users get permissions granted through the use of cryptographic keys, and on the other hand, that the state of the blockchain is consistent among all participants of the system.

As with any other sharing platform, a distributed ledger raises concerns over the privacy of the data it stores – it is typical for a user to want to retain an access to their personal information even after interacting with other users.

A. WHY IT IS A CHALLENGE FOR AUSTRALIA

Security is a key component of blockchain systems. It is what alleviates the need for a trusted central authority. Defining the appropriate prerequisites for a blockchain system to be secure depending on its context (public, consortium, private) is important to protect the users. Unfortunately, most existing blockchains do not offer *accountability*, as they do not allow users to identify responsible actors and initiate recovery processes in case of losses. Accountability is required to provide blockchain users with some guarantee as to the security of their transactions.

What problems do we face in trying to address this challenge?

- It is important to select a blockchain system that is well suited for the needs of the considered applications and use cases, especially in terms of immutability and consistency. Depending on the selected blockchain components, in particular its consensus and selection mechanisms, the system may offer different properties.[17]

- Financial institutions may have to rethink their strategies with regard to 'workforce optimisation, data centre requirements, storage, networking and security'.[18] In an interconnected environment, it is important not to assume that communications are reliable, private and secure.

- The management of identity is not resolved. In particular, key management remains problematic[19] as users exploit blockchains to avoid trusting a central authority, yet they sometimes trust additional services, like exchange platforms, or insecure wallet software, to maintain their credentials.

STANDARDISATION

Standardisation the best defence against attacks on blockchain networks. Blockchain systems are not invulnerable and are still susceptible to attack.

Australia is playing an important role in the development of standards to help protect privacy and assets on blockchain networks.

Why are these problems related to Australia?

Australia now manages the secretariat of the international technical committee for the development of blockchain standards, after the International Organization for Standardization (ISO) approved Standards Australia's proposal for new international standards on blockchain. These standards are the foundations that define the security requirements to protect blockchain users. Previous efforts by the ISO led to the specification of cryptographic libraries that define guidelines regarding the parameters on such libraries that are relevant to blockchains.[20]

There may be a need to regulate exportation of blockchain technology from Australia, similarly to security protocols, as part of Defence Export Controls list. At the time of writing, blockchain technologies do not appear on this list, yet they will likely be considered a sensitive class of software that could become subject to the same exportation restrictions as other specific cryptographic software that they embed.

B. THE TRADE-OFF BETWEEN SCALABILITY AND SECURITY

In most blockchain technologies, there exists a trade-off between the scalability of a blockchain and the level of security it offers. This means in order to ensure the performance of the blockchain as the system size grows, one often has to sacrifice some level of security. Despite important progress in research into scalable secure consensus, this trade-off remains, outlining the difficulty of offering a 'one-size-fits-all' blockchain system that could address both scalability and security, as depicted Figure 5.
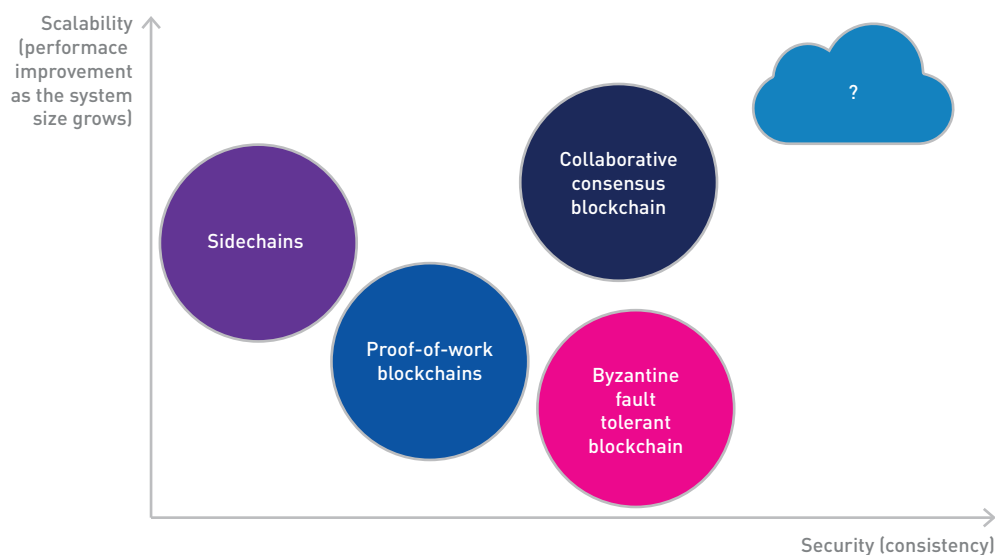
Figure 5 – There is no one-size-fits-all blockchain solution

In particular, blockchain systems based on proof-of-work typically offer a publicly accessible blockchain but assume *synchrony* in that the communication between any pair of nodes takes a maximum amount of time known by the algorithm. Blockchain systems that are Byzantine fault tolerant actually tolerate the misbehaviours of a bounded number of participants but without necessarily assuming synchrony. There exist, however, new ways of bypassing proof-of-work by adopting proof-of-authority alternatives, for example in Ethereum nodes. Proof-of-authority already leverages Byzantine fault tolerance but, unfortunately, still requires synchrony, making it potentially vulnerable to unforeseen delays. Sidechains typically run in parallel to a primary blockchain, sometimes trading security for performance before the results of their execution get resynchronised to the primary blockchain.

A more recent variant of blockchains, employing a collaborative form of consensus, shares similarities with the Byzantine fault-tolerant blockchains in that it offers security by preventing the blockchain from forking, hence preserving the 'chain' structure. It differs, however, from the Byzantine fault-tolerant blockchains because it does not aim at solving the classic Byzantine agreement problem28 for the sake of scalability.

In contrast, the collaborative consensus variant,[21] discovered by a joint collaboration of European and Australian researchers, allows this block to be distinct from any proposed blocks. It allows for higher scalability because the block can result from accumulating the sets of transactions proposed by distinct participants. It is not limited to just the set of transactions proposed by one participant. Continued funding of international research in this discipline is key to the scalability of blockchain systems and to ensuring both security and scalability for the Australian users of blockchains.

C. ILLUSTRATING THE TRADE-OFF IN PROOF-OF-WORK BLOCKCHAINS

To illustrate the trade-off between scalability and security, let us consider proof-of-work blockchains. As discussed in the Scalability section, maintaining the difficulty of the crypto-puzzle in proof-of-work blockchains while increasing the number of participants mining (and thus the computational power in use to solve the crypto-puzzle) improves the rate at which blocks get appended.

This would typically offer better scalability, in terms of throughput and latency, by reducing the period P between consecutive block creations. The reason why this solution cannot be adopted is because it would reduce security. In particular, the aforementioned synchrony assumption of these blockchains states that there is an upper bound U on the time it takes for blocks to be propagated to another node. Maintaining P that is significantly larger than U helps reducing the chances of *forking* (conflicting blocks becoming appended at the same index of the chain) simply by ensuring that blocks get delivered to all nodes before a new crypto-puzzle is solved and a new block is created. As soon as P is closer to U, the chances that conflicting blocks get created at the same index increases, hence increasing the risks that conflicts remain undetected. When P exceeds U, multiple miners are likely to create conflicting blocks to the same index of the chain before they can learn of the other created blocks. These blocks contain transactions that could be used for *double spending* (i.e. spending the exact same assets twice), a problem that can be serious for critical applications.

D. THE CONSENSUS PROBLEM

The consensus problem is central to blockchain as it ensures agreement among the machines (or nodes) as to the next block to append to the blockchain. Originally introduced in 1982, the consensus problem is a difficult problem of distributed computing that requires a subset of machines to act correctly (i.e., not misbehaving) to eventually decide a common value that was initially proposed by one of these machines.[28] Many solutions to this problem were proposed in the literature, like PBFT[22], often relying on a leader and aiming at being used among a small set of participants, running in the same local area network.

To work in an open environment, some blockchain systems combined a protocol to select consensus participants from the environment with a simple consensus protocol working under communication synchrony.[4] The selection typically consists of limiting the power of the adversary by allowing only machines solving the proof-of-work to propose a new block, hence reducing the chance of an attacker imposing its block. The consensus protocols of typical blockchains often rely on a local decision based on the linked structure of blocks received from the network, sometimes choosing the block that is the first of the longest branch of a tree of blocks.

As we mentioned previously, to offer scalability in terms of performance as the system grows, a new form of consensus problem does not require the decided block to be proposed by a single node. By leveraging the validation of transaction signatures inherent to the blockchain system, this blockchain consensus problem[23] allows the blockchain to decide on a superblock that results from all valid blocks proposed by distinct nodes, hence increasing potentially the throughput with the number of consensus participants.

A very large number of blockchain proposals exist, often with different combinations of consensus protocols and selection protocols. As examples of selection protocols, the proof-of-stake selects the nodes with high value at stake, the proof-of-authority selects an authorised node, the proof-of-importance[24] selects a node based on its value at stake and its activity, etc. As examples of consensus protocols, the Raft consensus protocol has been adopted in distributed ledgers to tolerate crash failures but not malicious behaviours;[25] multiple PBFT variants have been explored in different blockchains as well.[26]

How do you get users to agree? What happens when users don't agree?
Solving the consensus problem is a major blockchain challenge.

Centralised Systems	Decentralised Systems	Distrubuted System
SINGLE SOURCE OF TRUTH	MANAGED SOURCE OF TRUTH	TRUTH BY CONSENSUS
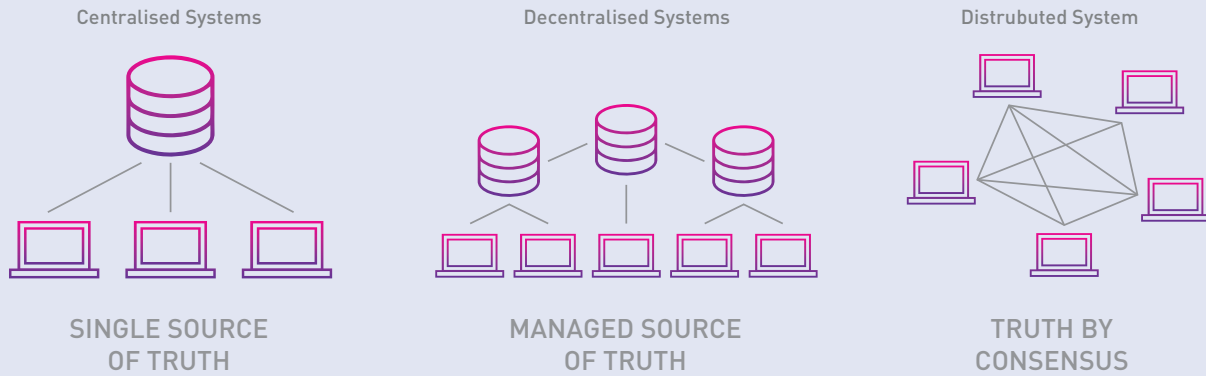
E. THE TRADE-OFF BETWEEN CONSISTENCY AND AVAILABILITY

In 2000, distributed systems, which now include blockchain systems, were conjectured[27] to provide at most two of the three properties called consistency, availability and partition:

Consistency

The system provides *consistency* when there exists a total order on all operations such that each operation looks as if it were completed by a single instance. In the context of blockchain, violating consistency could lead to two unordered transactions that double spend the same coins.

Availability

A system provides *availability* when all requests terminate even during the case of severe network failures. A lack of availability in a blockchain system would translate into a balance or transaction request not being served.

Partition tolerance

During a partition, all messages sent from nodes in one component of the partition to nodes in another component are lost. *Partition tolerance* is provided when the network is allowed to lose an arbitrary number of messages between nodes.

A couple of years later, this conjecture was demonstrated formally and led to an impossibility result called the CAP theorem, where CAP stands for consistency, availability and partition-tolerance:

CAP theorem: *There is no distributed service that ensures availability, consistency and tolerance to partitions.*[28]

This theorem is particularly useful when assessing the security of a blockchain system, as it tells us that, like any other distributed system, a blockchain system cannot ensure security in the form of both consistency and availability when many network messages are lost. The internet is constantly subject to message losses, due to faults, congestion, the limited capacity of switches, the queue size of the server, human misconfiguration or natural disasters. Even connection-oriented protocols, such as TCP/IP, are subjects to disconnections. This is why partitions in blockchains should be thought as the norm rather than the exception.

Consistency, on the one hand, is crucial for security. An inconsistency occurs when a *fork* or multiple blocks are appended at the same index of the chain, making it hard to determine which of their set of transactions came first. For example, consider a blockchain that initially has 300 blocks, and two new blocks B_1 and B_2 being mined for index 301 concurrently in Australia and in Europe. If Alice manages to include in B_1 a transaction that transfers all her coins to Bob and include in B_2 another transaction that transfers all her coins to Carol, then Alice risks double spending, as mentioned above, essentially buying goods from Bob and Carol, whose cumulative value is twice the coins she owned.

Availability, on the other hand, is less critical as it provides the responsiveness of the blockchain service to its users.[29] The availability of a service is often expressed as a percent of the time the service can serve requests; for example, some cloud computing companies aim to be able to serve requests 99.99% of the time. As it seems impossible to guarantee availability 100% of the time, one can consider it sufficient to guarantee availability as long as the network is not partitioned.

Blockchain system	Consistency (with partition)	Availability
Bitcoin / Litecoin / Ethereum	✘	✔
Tendermint / Red Belly Blockchain	✔	✘

Figure 6 – A blockchain can only be either consistent or available when a network gets partitioned

Figure 6 shows whether particular blockchain systems ensure availability or consistency in the case of a network partition. First, one can observe that traditional blockchain systems, like Bitcoin and (proof-of-work based) Ethereum, favour availability over consistency, hence offering responsiveness in case of network partitions, at the risk of being inconsistent. Second, more recent blockchain systems, like Tendermint, Red Belly Blockchain or a 'correct-by-construction' Casper proposal (different from the 'friendly finality gadget' Casper) favour consistency over availability, hence guaranteeing the absence of double spending but potentially delaying responses when network partitions occur.

These differences indicate the blockchain systems that are best suited for particular use cases, whether the use case is critical and can tolerate delays, or whether the use case is non-critical but requires high availability.

F PRIVACY AND TRUST

Whereas traditional blockchains provide ways to hide the relationship between accounts and users, they do not allow anonymity of its users. Hence, the term 'pseudonymity' is often used to describe the possibility for users to act behind account numbers or public keys that serve as pseudonyms.[22] If a user reveals his public key to other users, then these users can retrieve the set of transactions he invoked simply by looking at the history of transactions in the blockchain.

Def. 2 (Privacy): *The degree to which transactions from any one node are sensitive to being observed to any other node on the network.*

Privacy heavily influences system architectures where there is sensitive information; this precludes gossip-style protocols exchanging content in plain text. Privacy is typically important for various use cases related to health, where blockchain is used to store medical records of patients. It may also be enforced in different ways; for example, the European jurisdiction with the General Data Protection Regulation (GDPR) or the Australian jurisdiction. There are various technologies that can be used in a combination with a blockchain protocol to ensure that information being exchanged is encrypted. This includes TLS/SSL for connection-oriented communication.

The degree to which a user can trust the operation of the network depends on the way it is implemented. It is a function of the system architecture, consensus mechanism and transaction criticality. If the application requires that all nodes participate in consensus and locally verify transactions (instead of some portion of network users handing off to a set of special network validators), this increases the technical requirements of the network.

A way to decrease the technical requirement of the network is to require that the client contact as many nodes as required to retrieve the correct information, hence offering a tolerance to a specific number of failures.

These requirements should ideally be regulated to offer protection to users and to hold developers or blockchain participants accountable for any violation of this protection.

03
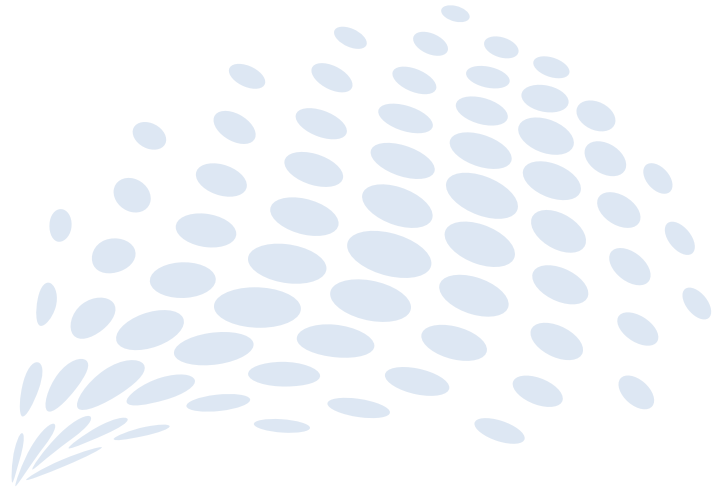
Regulation

Governance and oversight typically progresses at a slower pace than technology. As a result, regulation efforts can become outdated by the time they are in place and may prove ineffectual. As with other technologies, a gap exists between blockchain technology and an adequate regulation framework.

A. WHY IT IS A CHALLENGE FOR AUSTRALIA?

There is a limited regulatory landscape around blockchains. The challenge is to develop a clear statement of the legal, policy and ethical framework that enables the use of blockchain technology, especially cryptocurrency. Some related issues include a lack of clarity on the terminology, and perceived immaturity of the technology. Additionally, a lack of clear governance rules for compliance with legislation and regulation for know-your-customer (KYC), anti-money-laundering (AML) and counter-terrorism-financing (CTF) processes for pseudonymous users is a challenge;[30] and measuring the extent to which 'code' can be considered a legal agreement between parties remains unclear and untested in court.

What problems do we face in trying to address this challenge?

The challenges to privacy and security that blockchain technology poses to Australia involve five main points: key management; identity management; privacy; immutability and governance; and verification and assurance.

1

Key management
This includes the security of private keys for each participant on the network as well as management of servers, cloud infrastructure and possible recovery of keys on disposed hardware.

2

Identity management
Due to the pseudonymity of blockchain users, the challenge of linking identities with those on and off chain must be considered. By matching identities, blockchain systems can help maintain integrity of the transactions conducted on the ledger and help reduce fraud.

3

Privacy
Privacy is a key area of focus. The de-identification of users may not be enough to ensure privacy, since transactions and data can be retraced through a ledger of the blockchain. Privacy should also be looked at with respect to identity, scalability and trust.

4

Immutability and governance
The data on a blockchain is hard to modify. Therefore, in cases where transactions have been fraudulently conducted, it becomes a challenge to recover stolen assets as blockchain does not allow for reversal of transactions due to its immutable characteristic.

5

Verification and assurance
This is important in terms of security; a security audit of the code and implementation of best practices can reduce fraudulent behaviour on the blockchain.

A problem that arises in addressing the above challenges is the standardisation of cryptographic techniques that are the key to the security of the blockchain systems. In particular, more efforts, such as those conducted by the ISO and IETF,[31,40] are necessary to understand the security guarantees of a particular blockchain system.

A further problem is the removal of intermediaries. Understanding how the absence of intermediaries affects liability is a key issue. The removal of intermediaries may open up new areas of unforeseen risks, particularly in the financial sector, by encouraging herding behaviours.[32] Unless these risks are minimised, there will be insufficient trust to enable adoption. This will also jeopardise the necessary insurance schemes that each industry, and some of the professions, require for licensed or prudent practice. These challenges must be addressed in a way that satisfies the whole community of government, business, developers, professionals, and consumers.

Why are these problems related to Australia?

There is no general right to privacy in Australia. Instead, privacy in Australia is governed by the *Privacy Act 1988* (Cth)[33]. This makes the task of upholding privacy and security particularly important, as, when dealing with a decentralised technology such as blockchain, there is no accountability or intermediary from whom to seek remedy, or ways to erase personal information from the blockchain data structure.

B. THE LAW–TECHNOLOGY GAP IN BLOCKCHAIN

The aforementioned gap between the technical and legal communities is also due to disconnected expectations of what can be achieved through blockchain technologies and the legality of these processes.

Encoding relations: For those operating in the technology landscape, blockchain presents an opportunity to formulate certainty through programmable rules dictating what can and cannot be done, such as proof-of-work, and consensus technologies. In the context of social arrangements, technologists could attempt to reflect relationships into computational code, thereby reducing them to pre-programmed, digital codes to be managed without human intervention. This results in the removal of conscience from the coded rules.

For those operating in the legal landscape, conscience is found in the foundations of the law. Combining explicit law, implicit practice, and a culture that implicates ethical, social and economic aspects, legal systems reflect social arrangements and relationships through rules such as contract, and the rules of equity.

Both technology and law are underpinned by social values, but it is crucial for the communities to reach a middle ground in which they can work together to achieve common goals.
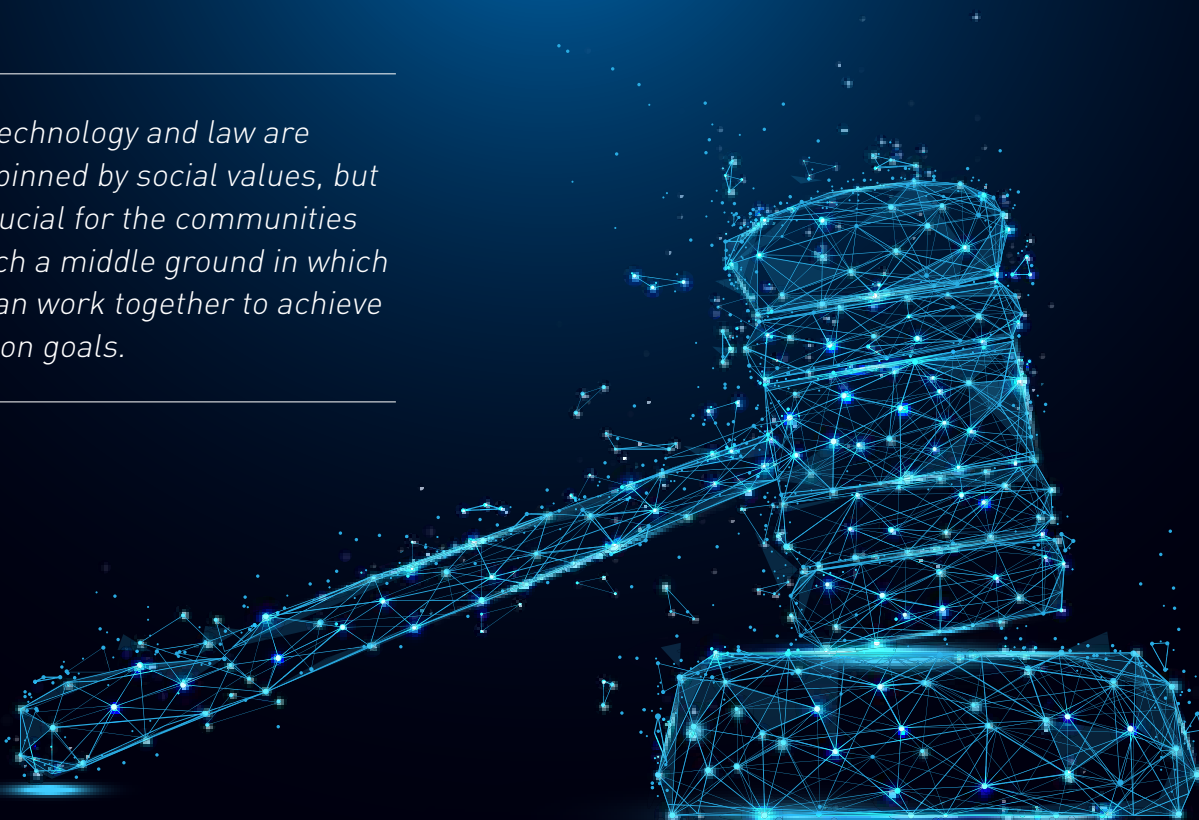
In establishing the extent of the gap in knowledge and expectations it is useful to contemplate hypothetical scenarios which demonstrate how differing legal and technical problems arise in the use of blockchain technologies. These scenarios demonstrate several ways in which laws and regulations cannot currently be coded out of and conversely, scenarios in which coding rules cannot currently be contracted out of. These scenarios present an opportunity for the legal and technology communities to reconcile what is legally and technically possible.

1

Legal problem — open source communities and employment
In the blockchain space, companies often use existing open source code, whilst employing individuals to develop and extend existing code. This raises concerns about incorporating employee rights and obligations in the open source community, especially if employee actions have an effect on the blockchain users. In answering this concern, we must consider that some of the law and contract regulations cannot be coded out of, and likewise, some of the coding cannot be contracted out of.

2

Accountability? Trust aversion and risk allocation
How do we optimise technological and legal structures within an industry (law) that has a low appetite for trust, and is risk averse? On the blockchain, we have to promise that it works. When so many people have a hand in something so foundational, who can be sued becomes unclear. From a legal point of view, we cannot fast-track the allocation of risk because we do not know what the right standard is yet.

3 Smart contracts

A smart contract can be defined as an event-driven computer program that executes on an electronic distributed, decentralised, shared and replicated ledger used to automate transactions.[33] Even where a smart contract is not technically a 'contract at law', it may give rise to obligations and remedies that sound like a contract in law. This means that parties to a non-contractual transaction may be required to fulfil certain obligations or must refrain from certain actions. These can include breaches of common law obligations and legislative provisions (such as economic torts, mistakes, fraud, collusion, anti-competitive behaviour, misleading and deceptive conduct, breach of the *Sale of Goods Act*, breach of fiduciary duty, breach of trust) as well as accessorial liability for either inducing or knowingly participating in breaches of fiduciary duty or breach of trust. Remedies that can arise from breaching non-contractual obligations include damages, compensation, unjust enrichment, equitable compensation, account of profits, or even a constructive trust.

4 Token, cryptocurrency and title

Technologists may perceive the issue of a cryptocurrency token as a way in which corruptible courts and rule makers can be prevented from jeopardising the factual integrity of records of ownership recorded on the blockchain. Technologists could argue that a record of something dematerialised is enough to represent ownership. For example, technologists could assume that having a register of tokens (cryptocurrency) on a blockchain creates title, where legally, it does not. From a legal point of view there are still rules about how ownership is recorded. In accordance with rules surrounding property and title, the legal community views a digital token as distinct from legal title; it cannot be used as evidence to a legal claim. Rules apply to dematerialised rights, including most of the world's securities or patents, which are not subject to ownership necessarily, but encumbrances and rights.

C. FINDING THE MIDDLE GROUND BETWEEN LAW AND TECHNOLOGY

Currently, there is a gap between technologists and the legal professionals, where the technologists do not fully comprehend the legal, and the legal do not fully comprehend the technical. Addressing this mismatch translates into closing this gap and providing a middle ground where technologists meet legal professionals.

TABLE 1 –THE MIDDLE GROUND BETWEEN TECHNOLOGISTS AND LEGAL PROFESSIONALS

FINDING THE MIDDLE GROUND BETWEEN TECH AND LAW		
Technology	**Middle ground**	**Law**
Immutability	*Erasing the key to decipher*	Right to be forgotten
Automated payment on income	Technologists can help	Tax legislation (can be directly coded)
Explaining system and code	Technologists can give input to legal professionals	Dispute resolution in court
Changing TX validity requires hard fork	Law can help tech	Zero-hour rule retrospectively voids TXs
Loss of private key (cannot recover private key)	Law can help tech	Re-prove lost certificate or title
A token is a digital title	Transforming digital title into legal title	A token is not a legal title
Lost keys		Title recovery

For example, Europe's GDPR stipulates that individuals do not have the right to be forgotten, but rather possess the 'right to erasure'. This may not contradict the immutability property of blockchain systems.

An organisation can comply with these rules by showing the existence of a process to perform the erasure. Erasing the key to decrypt the data on a profile may be sufficient, although it is not possible to rule out that someone with photographic memory remembers the key, or that someone may secretly have a copy of the key.

On the one hand, technologists can help legal professionals in their tasks. Tax legislation can be automated using technologists, using a simple program which deducts taxes directly from the outcome based on accurate measure, estimating closely the taxes and compensating error margins based on inputs. Similarly, technologists can help resolve disputes in court, by explaining the intentions behind the semantics of a program used to encode a contract between parties.

On the other hand, legal professionals can help technologists. If a corporation becomes insolvent, corporate law rules state that the zero-hour principle will retrospectively render void any transactions made by the company from midnight of that day. However, from a technical perspective, any transactions made on the blockchain may still be valid, and added as a block on the chain, because the zero-hour rule is not integrated into proof-of-work and integrity requirements, and technologists can advise on this.

As for filling the gap between token and physical titles, technologists should encourage the legal community to support the potential for transforming digital title into legal title, rather than use technology to support the existing limitations put in place by existing rules. If technologists are to affect social change in how title is viewed and transacted within society, they also require the support of the legal community to bridge the gap in knowledge. This is because, in order to affect social change, technology must affect the judicial fabric of society (as the judiciary influence the rules that govern society). However, technologists do not need to know the law to do this; instead, they need to know how they can be interoperable with the law.

There is, however, a mismatch between how laws regulate processes and how blockchain can encode them. If a user obtains title to land on the blockchain through a digital token, and subsequently loses their private key, then given the importance of private keys in blockchain processes, will it become technically impossible to transfer this digital title? Technically, this may not be feasible. In contrast, transferring legal title to land in the form of a certificate which has been lost is still possible, as there are laws which establish procedures to re-prove a lost certificate of title.

D. CLOSING THE GAP

Trust is a crucial issue that must be addressed when closing the gap in knowledge between technologists and lawyers. There needs to be a mutual understanding of what level and standard of trust is required. For example, when considering the enforceability of contractual terms on a blockchain, the ability to accurately and consistently decipher what is an 'essential term' of a contract vs a 'non-essential term' could serve to promote certainty and trust in this area. The legal community could also educate technologists on existing concepts of trust in the law, to support new forms of trust that may arise through technological development.

In order to bridge the gap between knowledge and expectations, certainty must be achieved regarding the rights blockchain technologies can create and enforce. One solution would be to analogise the rights and assets created on a blockchain to rights that are created in a contract. If a contract is conceptualised as a physical, paper representation of rights and obligations that have been agreed upon by two persons, an asset or contract on a blockchain can similarly be viewed as a digital representation of a physical asset or right.

We anticipate a pushback from the legal community (including from the courts) when attempting to integrate technology into legal framework; as creating standards for technologists creates a standard for everyone. For lawyers, their main concern is the requirement to defend their client's commercial or industry practices, as well as the systems they adopt in their own legal practices. This defence takes the form of explaining and justifying these systems in dispute resolution and in court. In order to do this, lawyers must be able to understand those systems, including systems that exist wholly or partly in code. It would, therefore, be useful to have a general framework around technologies such as smart contracts. This framework would provide guidelines on issues such as the ability to write in beneficial payments; how to give recognition to contracts; how to translate code into plain English; the ability to remove transactions that exist; the ability to transfer financial instruments along with assets; and whether or not payment can flow through the contracts.

In order for the use of blockchain to be optimised, technologists and legal regulators do not need to occupy the same space. Instead, both communities should acknowledge the presence of the other, while establishing a point of connection across their fields of expertise in order to educate each other on important principles and concepts. For this to be achieved, the nexus between the two communities should be small, so that regulators do not negatively impact the technologists and impede their technological development. These points of connection should be narrow, so as to enable the exchange of information to be limited to only what is necessary, in order for both landscapes to be interoperable.

So while it is clear that there needs to be a bridge between the two communities, it is not clear at what point it is crucial for there to be a bridge; what needs to be avoided is the separate fields getting in the way of each other.

04
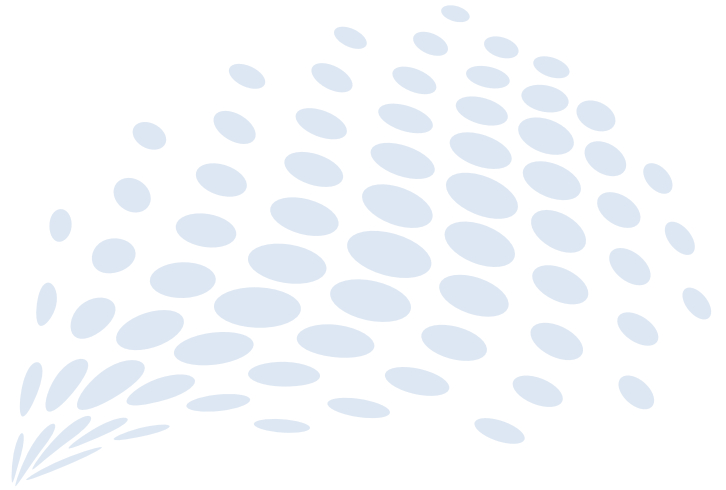
Education and Employment

Education and employment are two linked challenges that may limit the development of blockchain in Australia.

A. WHY IT IS A CHALLENGE FOR AUSTRALIA

What problems do we face in trying to address this challenge?

The challenge blockchain poses to education and employment is one of supply and demand, where education is the supply, and employment is the demand.

- Currently, the industry (recruitment) is experiencing a shortage of supply, and is resorting to non-accredited individuals to fulfil skill-specific jobs.[34] Some recruitment agencies specialised in IT are specialising in blockchain as well. Incubators are also specialising in the fintech economy, including more particularly in the blockchain economy. The employment challenge requires putting VET and tertiary education organisations in contact with recruiters or SMEs.

- A key challenge is to fund research in blockchain for academics in order to educate others. Breaking it down further, education challenges in particular can be thought of as a concentric circle; the research, academia and the technical profession must be the first to be educated on blockchain, and only then can that knowledge be dispersed to related professionals and government, followed by professional users and decision makers and then public end users.

Why are these problems related to Australia?

There is a great opportunity for Australia to develop and improve its current technology as well as fund blockchain-related research and education to become a greater export of technologists and disruptive technology. The number of international students in Australia in November 2018 had grown by 11% in one year to reach 690,468 students.[35]

Australia will have to cope with the impact of blockchain technologies on the job market and the education sector: already in 2015, most interviewed ICT employers in Australia used non-accredited training in the last 12 months.[57] This indicates a need to refine the curricula of accredited educational institutions.

B. EDUCATION AND LAW FIRMS

Education is paramount as the foundation for understanding this technology. The education challenge also includes the tasks of educating the public as well as professionals and service organisations; professional users; organisations that integrate, or interface with, the blockchains; and also legal professionals.

From a legal point of view, there is currently no precedent in law dealing with blockchain. As a result, the law is likely to struggle with the implications of blockchain. Increasingly, knowledge and teaching of ethics will be extremely important. Technologists must operate, innovate and create in a way that is sustainable and does not infringe upon any principles of ethics or the law.

The main problem is understanding what education is needed, by whom, and at what level. Addressing this problem requires defining the skills that need to be taught at tertiary (higher level) education as well as vocational education and training (VET): software engineering, distributed systems, cryptography, economics, trust and ethics.

In particular, fundamental knowledge should be prioritised along with technology-specific knowledge in order to guarantee that users understand the blockchain system they use. For example, users should not expect to be protected by the distributed nature of a blockchain if they rely on a central exchange platform to use the blockchain system.[36]

C. RETRAINING EMPLOYEES

With regards to employment, the specific challenges include blockchain's disruption to traditional administrative roles. It presents the potential to make jobs by automating the processes previously conducted by intermediaries while creating entirely new jobs where opportunities will be in future for new industries.[37] The problem lies in understanding how best to tackle retraining and relearning, with constantly developing technology.

Conclusion

In this paper we have identified a number of challenges that need to be overcome to enable a widespread use of, and benefit from, blockchain in Australia. These challenges often require joint expertise from academia, regulators, industry and government. In this technical white paper, we have identified that the fabric to address some of these challenges exists already. Such fabric consists of the underlying principles behind the research, law and technology. Putting these principles to work requires close collaboration between different sectors.

The scalability challenge will require a complete rethinking of the design of blockchain systems, where proof-of-work is not likely to have a place. As we alleviate the slowness and energy-greediness inherent to the crypto-puzzle functionality of classic blockchain systems, other overheads will become more apparent, in terms of storage space, program execution and communication bandwidth. Research on how to mitigate these overheads will probably lead to a bottom-up redesign of the blockchain systems. This will be crucial to obtaining radically new blockchain systems that can scale worldwide while leveraging the resources of their participants.

The security challenge will be key to full adoption of blockchain systems by industry. The frequent vulnerabilities formalised theoretically, experienced empirically and sometimes relayed in the news prevent the application of these blockchain systems to critical use cases and relegate their use to test cases or toy applications. Researching, understanding and limiting these vulnerabilities, by – for example – reaching consensus on the block at each index, alleviating the need for communication synchrony, or by holding participants accountable for their actions, will reinforce trust in blockchain systems. This trust will facilitate the application of blockchain systems often tested in labs, to automate industry processes in production.

The regulation challenge lies in the dramatic lack of clear governance rules for compliance with legislation and regulation processes. This challenge can be addressed in part by having technologists and legal professionals help each other to bridge the gap between blockchain technology and law. This will require them to communicate and create a landscape in which technologists are able to clearly and easily identify whether they are liable, what their responsibilities are, and whether they are 'swimming in between the red and yellow flags' – by reference to the already existing policies and principles of the law.

The education challenge will require academics and professionals to determine the best way forward to educate the industry on the features of blockchains that match adequately the technology to the production use cases, and to educate users on the guarantees of blockchain systems. One specific way that this can be achieved is through the creation of a common taxonomy in regard to blockchain, and this taxonomy can help align the languages of different professions and industries for effective communication.

Glossary

Availability: A property of a system where all requests issued by clients terminate, even in the presence of failures.

Client: A machine that requests the blockchain service by storing data, sending transaction, requesting data or requesting a balance.

Consistency: A property of a system where once its state is stored, it will report the same state in every subsequent operation until the state is explicitly changed. It is equivalent to having a single up-to-date copy of the data.

Community blockchain: A blockchain where potentially different subsets of participants help decide upon each block but not all participants decide upon all blocks, so as to reduce resource usage.

Consensus:

> **Consensus problem:** The challenge of finding a mechanism by which participants of a blockchain system can collectively decide upon a unique block for a given index of the blockchain.

> **Proof-of-*:** A set of mechanisms that allow a subset of participants, who provide a proof, to participate in solving the consensus problem.

Consortium blockchain: A blockchain where only one preselected subset of participants help decide upon each block.64

Fork: A fork occurs when distinct blocks are appended at the same index of the chain, hence creating distinct branches of blocks.

Full node: A full node is a machine that both offers the blockchain service by creating blocks and requests the blockchain service by storing data, sending a transaction, requesting data or requesting a balance.

Light node: A light node is a machine that does not download the entire blockchain and offers a lightweight service.

Latency: The average time taken for a request to be treated by the system (e.g., a transaction being committed, a data item being stored).

Participant: A participant is a machine participating in some way in the blockchain; it can either be a client, a light node or a full node.

Partition tolerance: A property of a system that continues to operate despite arbitrary message loss or failure of part of the system.

Sidechain: A type of blockchain that operates independently from a main blockchain and uses an alternate storage representation of events, some of which may me mapped to corresponding events in the main blockchain.

Privacy: The degree to which transactions from any one node are sensitive to being observed to any other node on the network.

Private blockchain: A type of blockchain system where only one central organisation can decide upon a new block.

Proof-of-work blockchain: A type of blockchain system that requires users to solve a crypto-puzzle and include the proof-of-work solution into a block for the block to be considered by the system.

Pseudonymity: The property of a system where users are identified only through their pseudonym. This pseudonym can refer to a public key or an account number, without necessarily identifying a user through their personal information.

Public blockchain64: a blockchain where any participant can help deciding upon each unique block at a given index of the chain.

Scalability: The ability for a service to maintain or improve a property as its size grows.

Smart contract: An event-driven computer program that executes on an electronic, distributed, decentralised, shared and replicated ledger that is used to automate transactions.

Synchrony: In blockchain terms, this refers to the placement of a universally accepted upper bound on the amount of time in which a message must be delivered.

Throughput: The volume of data or transactions that can be processed by the system per unit of time.

Byzantine fault-tolerant blockchain: A type of blockchain system that allows participants to decide upon a unique block at a given index of the chain as long as a sufficiently number of these participants behave correctly.

Trust: Acceptance of exposure to risks.

User: The person behind the client machine who makes use of the service.

References

1   *Australia in driving seat as global blockchain standards take shape.* James Eyers, AFR, 2018. https://www.afr.com/technology/australia-in-driving-seat-as-global-blockchain-standards-take-shape-20180906-h151w7

2   *CSIRO and the University of Sydney's Red Belly Blockchain breaks new ground for speed.* Yolanda Redrup, AFR, 2018. https://www.afr.com/technology/csiro-and-the-university-of-sydneys-red-belly-blockchain-breaks-new-ground-for-speed-20180913-h15byh

3   *World Bank appoints CBA for first bond deal on blockchain.* James Eyers, AFR, 2018. https://www.afr.com/business/banking-and-finance/financial-services/world-bank-appoints-cba-for-first-bond-deal-on-blockchain-20180809-h13qji

4   *Bitcoin: A Peer-to-Peer Electronic Cash System.* Satoshi Nakamoto, 2008. https://bitcoin.org/bitcoin.pdf

5   *Privacy Act.* https://www.oaic.gov.au/privacy-law/privacy-act/

6   *Blockchain: Enigma. Paradox. Opportunity.* Deloitte, 2016. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf

7   *The Distributed Ledger Technology Applied to Securities Markets.* European Securities and Markets Authority, 2016. https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf

8   *The Byzantine Generals Problem.* Leslie Lamport, Robert Shostak and Marshall Pease. ACM Transactions on Programming Languages and Systems, 4(3), 382-401, 1982. https://doi.org/10.1145/357172.357176

9   *The Missing Links in the Chains? Mutual Distributed Ledger (aka Blockchain) Standards.* Michael Mainelli and Simon Mills, 2016. https://www.longfinance.net/media/documents/The_Missing_Links_In_The_Chain_Mutual_Distributed_Ledger_aka_blockchain_Standa_DMN9ulM.pdf

10 *Australian internet connections slowed down by submarine cable fault.* Ben Grubb, Sydney Morning Herald, 2014. https://www.smh.com.au/technology/australian-internet-connections-slowed-down-by-submarine-cable-fault-20141202-11yc8m.html

11 *The Balance Attack or Why Forkable Blockchains are Ill-Suited for Consortium.* In proceedings of the 47th Annual IEEE/IFIP International Conference on Dependable Systems and Network, 2017. http://doi.ieeecomputersociety.org/10.1109/DSN.2017.44

12 See https://data.bitcoinity.org/bitcoin/block_time/5y?f=m10&t=

13 See https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki#Block_size

14 See https://tradeblock.com/blog/analysis-of-bitcoin-transaction-size-trends

15 See https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

16 *Evaluating the Red Belly Blockchain.* Tyler Crain, Christopher Natoli and Vincent Gramoli, arXiv 2018. h ttps://arxiv.org/abs/1812.11747

17 *The 74th Meeting of the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance - Technological and Societal Challenges to Blockchain Dependability and Security,* Luxembourg, 2018.

18 *Blockchain-Enabled Distributed Ledgers: Are Investment Banks Ready?* Accenture Consulting, 2017. https://www.accenture.com/t20160203T200922Zw/us-en/acnmedia/PDF-6/Accenture-Blockchain-Enabled-Distributed-Ledgers.pdf

19 *Distributed Ledger Technology in Payments, Clearing, and Settlement.* Mills et al., 2016. https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf

20 ISO/IEC 14888-3:2016. *Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms.*

21 *DBFT: Efficient Leaderless Byzantine Consensus and its Applications to Blockchains.* Tyler Crain, Vincent Gramoli, Mikel Larrea and Michel Raynal. Proceedings of the 17th IEEE International Symposium on Network Computing and Applications, 2018.

22 *Practical Byzantine Fault Tolerance.* Miguel Castro and Barbara Liskov. OSDI 1999.

23 *Blockchain Consensus.* Tyler Crain, Vincent Gramoli, Mikel Larrea and Michel Raynal. AlgoTel, 2017.

24 See https://gravity.io/.

25 *In Search of an Understandable Consensus Algorithm.* Diego Ongaro and John Ousterhout. USENIX ATC, 305-320, 2014.

26 https://www.jpmorgan.com/global/Quorum.

27 *Towards Robust Distributed Systems. Keynote talk.* Eric Brewer. PODC 2000.

28 *Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services.* Seth Gilbert and Nancy Lynch (2002) 33(3) ACM SIGACT News 51.

29 *On Availability for Blockchain-Based Systems.* Weber et.al., SRDS, 2017. https://doi.org/10.1109/SRDS.2017.15

30 *Discussion Paper: The Distributed Ledger Technology Applied to Securities Markets.* European Securities and Markets Authority, 2016. https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt_0.pdf

31 Curve25519 - RFC7748 Elliptic Curves for Security, Section 4.1, 2016.

32 *Why Is the Insurance Sector Considered a Low-Risk Investment?* Investopedia, 2015.

33 Senate Bill No. 1662 – State of Tennessee. 22 March 2018.

34 *Draft Industry Skills Forecast and Proposed Schedule of Work.* PWC, 2018.

35 *International Student Data.* Australian Government, Department of Education and Training, 2018.

36 *Distributed Ledger Technology in Payments, Clearing, and Settlement.* Mills et al., 2016.

37 *How Blockchains Could Change the World.* McKinsey & Company, 2016.

38 *ComChain: Bridging the Gap Between Public and Consortium Blockchains.* Guillaume Vizier and Vincent Gramoli IEEE Blockchain, 1469-1474, Jul 2018. https://doi.org/10.1109/Cybermatics_2018.2018.00249

39 See https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

ABOUT THE ACS

ACS is the professional association for Australia's Information and Communication Technology (ICT) sector. More than 40,000 ACS members work in business, education, government and the community.

ACS has a vision for Australia to be a world leader in technology talent, fostering innovation and creating new forms of value. We are firmly vested in the innovative creation and adoption of best of breed technology in Australia, and we strive to create the environment and provide the opportunities for members and partners to succeed.

ACS works to ensure ICT professionals are recognised as drivers of innovation in our society, relevant across all sectors, and to promote the formulation of effective policies on ICT and related matters.

Visit www.acs.org.au for more information.