

DISTRIBUTED LEDGERS

Scenarios for the Australian economy
over the coming decades

May 2017

CITATION

Hanson RT, Reeson A, Staples M (2017)
Distributed Ledgers, Scenarios for the Australian
economy over the coming decades, Canberra.

COPYRIGHT

© Commonwealth Scientific and Industrial Research
Organisation 2017. To the extent permitted by law,
all rights are reserved and no part of this publication
covered by copyright may be reproduced or copied
in any form or by any means except with the written
permission of CSIRO.

IMPORTANT DISCLAIMER

CSIRO advises that the information contained in
this publication comprises general statements
based on scientific research. The reader is advised
and needs to be aware that such information may
be incomplete or unable to be used in any specific
situation. No reliance or actions must therefore be
made on that information without seeking prior
expert professional, scientific and technical advice.
To the extent permitted by law, CSIRO (including its
employees and consultants) excludes all liability to
any person for any consequences, including but not
limited to all losses, damages, costs, expenses and
any other compensation, arising directly or indirectly
from using this publication (in part or in whole) and
any information or material contained in it.

CSIRO is committed to providing web accessible
content wherever possible. If you are having
difficulties with accessing this document please
contact csiroenquiries@csiro.au.

ACKNOWLEDGEMENTS

This project is funded by the Australian Government's
National Innovation Science Agenda (NISA), with
assistance from the Treasury. The authors would like
to thank Treasury staff for their leadership and support
during the study.

The authors of this report would also like to express
gratitude to the many individuals and organisations
who kindly shared their time, resources, expertise
and knowledge. Over 100 subject-matter experts were
engaged through a series of consultative workshops,
interviews, and panel discussions. The authors would
like to especially acknowledge the greatly appreciated
contributions of:

Malcolm Crompton AM, former Privacy Commissioner
of Australia, Managing Director Information Integrity
Solutions Pty Ltd

Simon Crowther, Partner, Fraud Investigation and
Dispute Services, Ernst and Young

Scott Farrell, Partner, King & Wood Mallesons

Nick Giurietto, CEO and Managing Director of the
Australian Digital Currency and Commerce Association

The Honourable Theresa Grafenstine, Inspector General
of the U.S. House of Representatives, and Deputy Chair of
the International Board of Directors for the Information
Systems Auditing and Control Association (ISACA)

Adrian McCullagh PhD, Research Fellow at
the Law Futures Centre of Griffith University,
Principal ODMOB Lawyers



FOREWORD

We are living in an era of rapid technology-fuelled change, which is creating complex strategy and policy choices for governments and companies. An explosion in device connectivity, data volumes, digital communication, e-commerce, computing power and overall internet use is reinventing the landscape for governments, companies, societies and individuals.

The all-pervasive digital economy of the future will profoundly impact the majority of companies, governments and societies worldwide. Some jobs will disappear, and new jobs will be created. Some existing markets may be extinguished, and new ones emerge. New roles and capabilities for government will emerge.

Comprehending forthcoming change and being proactive is increasingly important. As a consequence, CSIRO's Data61 is dedicated to helping organisations understand forthcoming change and make better strategic choices.



We are focused on issues relating to digital disruption, the digital economy, knowledge industries and the innovation system.

We are focused on issues relating to digital disruption, the digital economy, knowledge industries and the innovation system. This allows us to understand the context for digital disruption. Typically it is not only the digital technology that matters, the socio-economic drivers that create demand for technology (or change in response to it) may be equally, if not more, important. The digital business models that work best have understood people first and digital technology second.

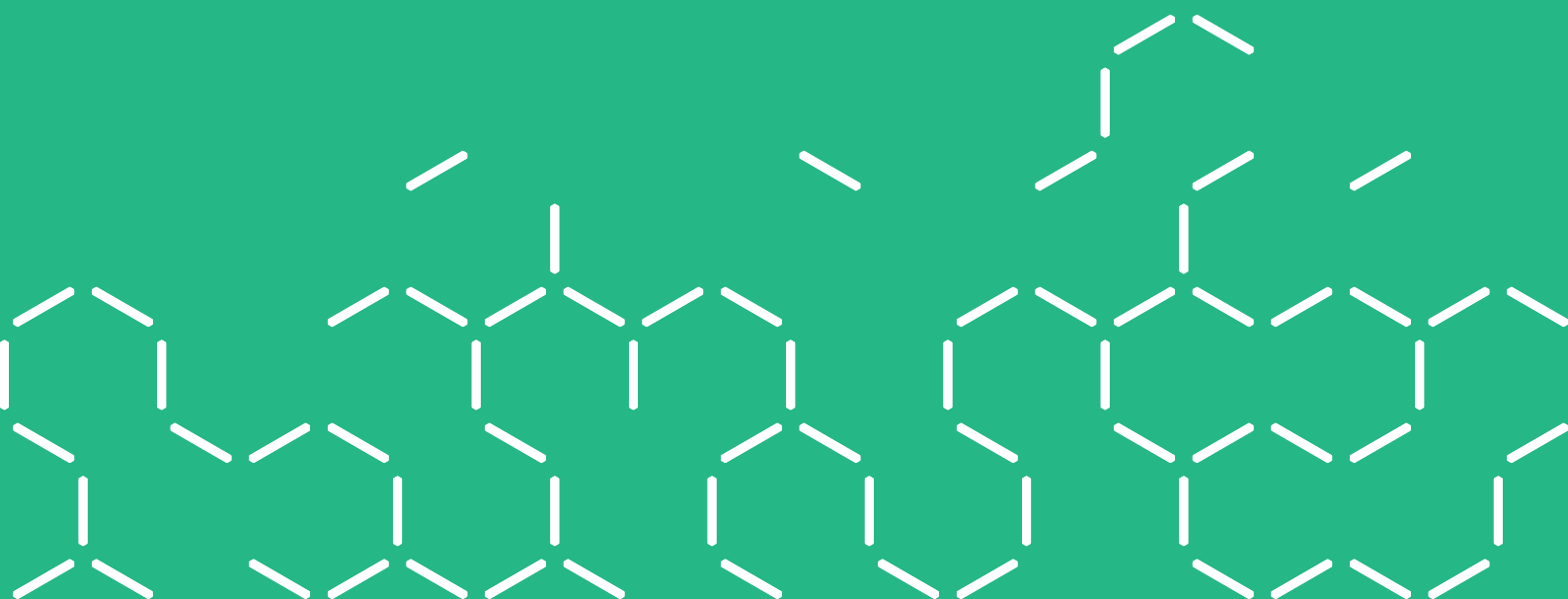
Given that improved performance in innovation will be essential to Australia's future economic growth, where should Australian Governments and companies be directing this effort? In a rapidly changing world and uncertain future, what investments will allow Australia to harness future opportunities across the widest range of possible futures? In this increasingly interconnected and rapidly changing global market, Australia risks being left behind if it fails to innovate and build innovation capacity.

Innovation will be important on two fronts. First, it will be key to driving future productivity growth in both established and emerging industries. This is important because the resources boom masked a decline in Australia's productivity. Over the past decade, Australia's productivity has declined more sharply than in many other Organisation for Economic Co-operation and Development (OECD) economies.¹

Second, innovation will be key to developing new companies and new industries based on emerging science and technologies. With many of these innovations disrupting existing industries, it will be important to use these breakthroughs to generate new sources of productivity and international competitive advantage.

Data61 monitors, and incubates, innovation at all levels within the Australian context, where it is new to the world, where it is new to an industry, and where it is new to Australia. Distributed Ledger Technologies, including Blockchain, have advanced well beyond Bitcoin – presenting new opportunities to both existing organisations and emerging industries.

¹ The Conference Board Total Economy Database™, 2015



CONTENTS



Foreword	i
Executive summary	iv
1 Study objectives	1
2 Distributed Ledger Technology (DLT)	2
2.1 How do blockchains work?	4
2.2 Trust.....	11
2.3 Identity.....	13
3 Implementation considerations	15
3.1 Skill requirements	16
3.2 A conceptual shift.....	16
3.3 Design trade-offs	21
3.4 Next steps	22
4 Our future world	23
5 Scenarios	27
5.1 Scenario summaries	28
5.2 Aspirational scenario: Regulation on rails	30
5.3 Transformational scenario: The sheriff on the digital superhighway.....	36
5.4 New equilibrium scenario: A bumpy ride	41
5.5 Collapse scenario: A slippery slope	45
6 Methodology	51
6.1 Our research	51
6.2 CSIRO strategic foresight methodology	52
6.3 Scenario design	53
References	56
Glossary	61

EXECUTIVE SUMMARY

Distributed ledgers record the transactions supporting modern life. These ledgers are mainly held in databases² that enable the volume and velocity of transactions in the global economy to continue to increase. The challenge with these distributed ledgers has, however, been ensuring their integrity. Electronic information is notoriously easy to modify and falsify. Cyber security threats are also a growing threat to the confidentiality, integrity and availability of online data.

Relatively new ideas on how to ensure the integrity of data have raised a significant amount of interest. The first example (known as a ‘use case’) of a publicly distributed ledger was the digital currency, known as Bitcoin. Bitcoin also provides a high level of availability and a measure of confidentiality to these transactions. There is now significant investment in using these ideas for other use cases (see figure 1).

The term blockchain has been widely adopted in order to refer to technologies that have taken inspiration from Bitcoin, and implement distributed ledgers. Blockchain generally refers to the particular process that Bitcoin uses to create integrity in the transactions and data.

The current state of innovation, however, is analogous to the internet of the 1990s, with significant investments resulting in advances that are constantly being proposed, and proofs-of-concepts being deployed, with distributed ledgers adopting new processes for integrity. These new ledgers may not necessarily be defined as blockchains. The definitions in this emerging field are inconsistent, an issue being addressed by the International Standards Organisation.

The ability to generate integrity in distributed ledgers enables the formation of trust. Trust is a key enabler for economic activity. This may be in situations where trust was formerly not able to be established, or simply better trust than was previously available. In Bitcoin there is trust that this blockchain will perform as described, given that it has been tried and tested in the face of the worst online adversaries. The challenge for new technology platforms, and integrity processes, is to clearly describe what they are going to do, and deliver on this benefit. Distributed ledgers exist in an ecosystem of other technologies that must also deliver on this promise. For example, a crucial component of these systems is the use of private cryptographic keys to identify users, and control access. Losing control of these keys would invalidate trust in the system.

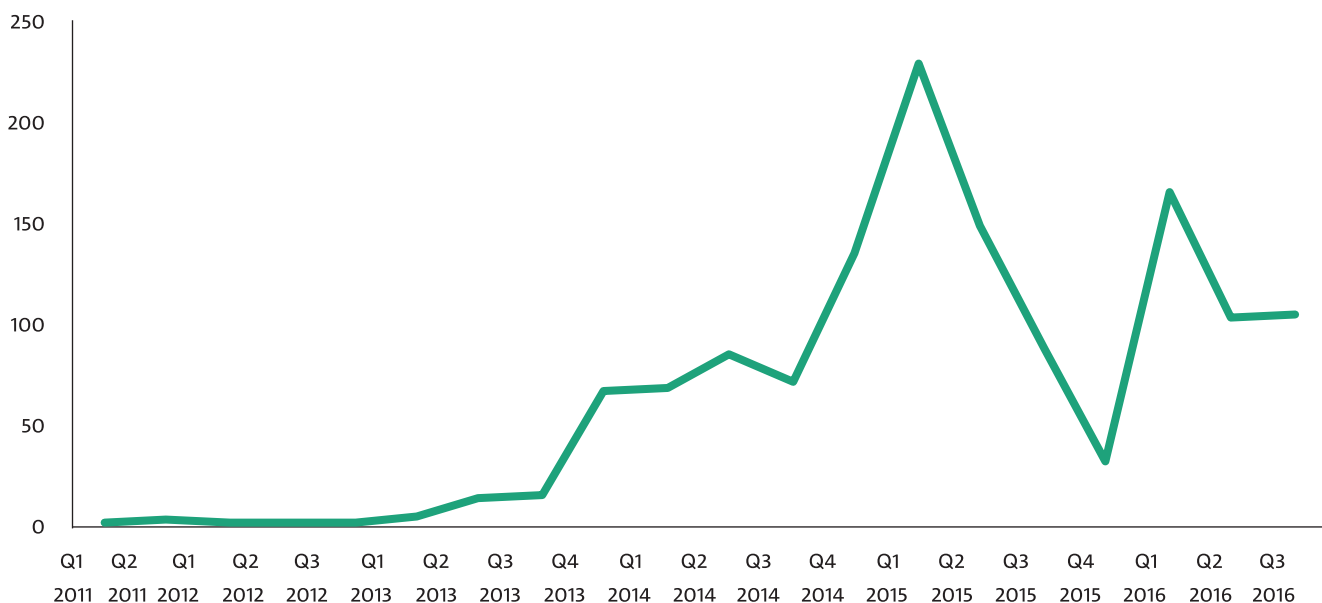
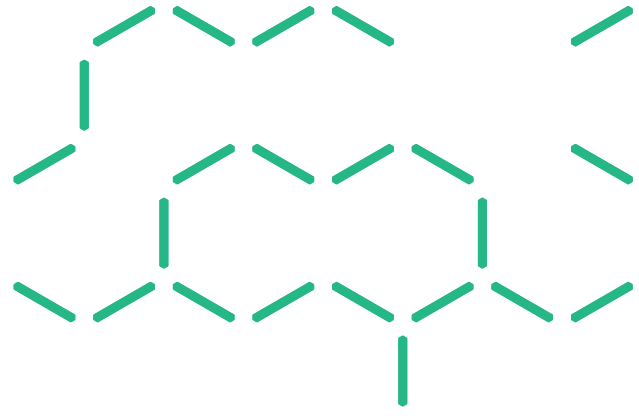


Figure 1: Venture Capital Investment in Blockchain Q1 2011–Q3 2016 in \$USD Millions

Sources: Brave New Coin, 2016.

² Often these are relational databases, such as SQL, which have been around since the 1970s.



Digital identity is verging on a human right. Electricity, telecommunications and banking have incrementally established themselves as essential pillars of our society. Their cyber security has become a facet of a more holistic security approach, as cyber risks to these pillars have transitioned into real world impacts.³ In order to operate in our economy, digitally identifying users has become critical to establishing trust in transactions, and for accessing essential services.

Proof of identity is one of the most fundamental, often challenging, and resource-intensive transactions involved in our heavily digitised world.⁴ Specialised identity ledgers would be a practical approach to managing identity, and associated regulatory compliance, and for facilitating interoperability between distributed ledgers.

In order to generate value for new blockchain use cases, the risks and opportunities of the technology should be considered. This report outlines concepts for this consideration and describes a series of plausible future scenarios that illustrate implications for industry, public policy and the community in terms of productivity and social acceptance.

The blockchain is not a silver bullet, and has certain limitations that should be considered before and during the design and development of new systems. Some of these limitations have not yet been experienced as Bitcoin and other blockchain experiments, are yet to reach these points. For example, ultimately the processing of transactions will transition to a commission-based (user pays) scheme. In the end this loss of the provision of new Bitcoins to miners may reveal the currently hidden transaction costs of the system, increase transaction costs (commissions) and disrupt the market that has formed by removing a competitive advantage and making it less attractive than the regulated market ('mining' break-out box). The potentially uneven introduction of advanced computing processing power, such as quantum computing, is another example of an emerging disruption on the horizon for this technology.

The scalability of blockchain, as it stands, is limited and should be considered as a potential constraint for the future performance of a new system. High transaction demands alone may choke a system on its own popularity. Carefully employing blockchains for specific roles inside larger distributed ledgers may optimise outcomes. Dedicating a blockchain to a sole function such as the management of identity, content, or transactions may balance the technology's strengths and weaknesses, and increase the benefits realised.

Balancing the risks and rewards of this technology requires the integration of relevant domains of expertise. This integration is challenged by the current lack of agreed definitions and is generating confusion as key concepts are becoming lost in translation between domains. For example, 'smart contracts' are arguably neither smart, nor contracts, and the use of the term could imply assurances of functionality it does not have. Integrating cross-domain knowledge for blockchains is complex as they are fraud controls, potentially cyber security controls, are utilised in digitised transactions that represent the performance of legal contracts, can and do operate across multiple jurisdictions, simulate or interact with banking and finance systems, and are increasingly being used to record activities, actions and assets in the real world. The permanence and persistence of new distributed ledgers also present challenges and risks that are novel in information systems. Consequently professionals and practitioners from many disciplines would be required to be engaged in order to balance risk and optimise reward.

IT professionals should consider the broader risks in, and from, their distributed ledgers, in a similar way to cyber security's shift towards a holistic security approach, as the impacts now materialise in the real world.⁵ Blockchain has come a long way from Bitcoin. This means IT professionals should have an awareness and appreciation for the fields of accounting, audit, fraud control, law, banking and finance, and any relevant sector in which a given blockchain will operate. Public and private sector initiatives, such as training, guidelines and standards, would assist technical and non-technical professionals realise benefits, and reduce the risks of adoption. Regulators and enterprises will need to be aware of the typical technical risks and limitations of blockchain technologies, in order to effectively manage them.

³ Center for Long-Term Cybersecurity, University of California Berkeley, 2016

⁴ ADCCA, 2016


⁵ Center for Long-Term Cybersecurity, University of California Berkeley, 2016

Given the novelty, and relative immaturity, of blockchain innovation, there are a series of suggested considerations to be undertaken when assessing the viability of these solutions:

- The volume of transactions on a ledger will increase if the digital asset requires additional record keeping. Significant transaction record keeping changes may require a redesign of the ledger's format.
- A distributed ledger does not need to be a dis-intermediator in order to generate value.
- A distributed ledger does not need to have a crypto-currency.
- Distributed ledgers may provide value as a fraud-resistant and tamper-evident record.
- Persistent ledgers could present problems, such as for privacy and perpetual agreements.

This report has been written in conjunction with another report, 'Risks and Opportunities for Systems Using Blockchain and Smart Contracts', which explores the use cases and technologies for the current point in time. In contrast, this report offers a set of four scenarios to illustrate the plausible adoption, risks and rewards of the technology in the future.

Scenarios were famously utilised by Shell in the 1970s to create a competitive advantage in the face of a disruptive oil shock. Scenarios do not seek to predict the future, but rather they allow the decision maker to imagine 'what if'. Scenarios allow the decision maker to consider: if these, or similar, possibilities were to occur then what should they prepare, rehearse and/or plan for ahead of time. Scenarios assist private and public sector organisations in being proactive. By being better informed of plausible disruptive situations, decision makers are provided with a map with which to navigate pathways to preferred futures.



Scenarios do not seek to predict the future, but rather they allow the decision maker to imagine 'what if'.

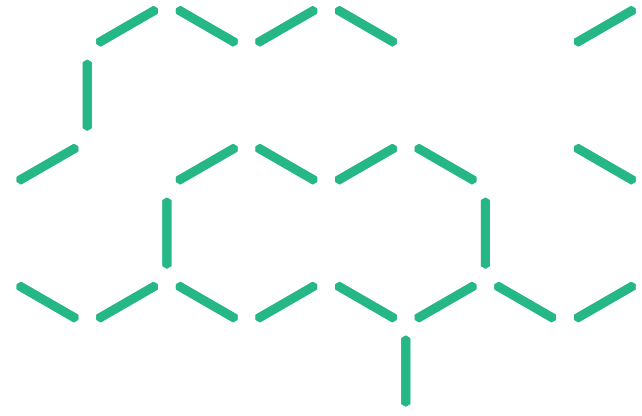
The four scenarios in this report follow the four archetypal categories of aspiration, transformation, new equilibrium and collapse. The scenarios cover the three aspects of critical uncertainty for this situation: people, process and technology, particularly the trends in technological innovation and the human factors of regulatory support and user adoption. None of the scenarios, or the events described within them, are suggested as being more likely than the other, nor are the events from only one scenario likely to materialise; reality is rarely this simple. The time horizon for these scenarios is 2030 for illustrative purposes only and is not a prediction of when actual events may occur.

REGULATION ON RAILS, ASPIRATIONAL SCENARIO

In this scenario we imagine a future where governments and the public sector have recognised the risks and potential of emerging technologies and provided leadership by embracing a cohesive regulatory regime that supports and leverages them. Distributed ledgers are employed to increase trust in government activities through identity management, fraud control, programmable money/ transactions (smart contracts), and regtech. High levels of regulatory support and regulatory automation, private and public sector adoption and technological innovation and development have led to significant improvements in productivity, with the Australian economy riding the Distributed Ledger Express on a track towards emerging and sunrise industries, including additive manufacturing and digital intellectual property.

Key questions:

- How should government deliver services in 2030?
- How should the government and public sector keep itself aware of emerging technologies, such as blockchain, and conduct the research and development to build the skills, policy, and technology required to deliver the services society will demand, and drive growth?



THE SHERIFF ON THE DIGITAL SUPERHIGHWAY, TRANSFORMATIONAL SCENARIO

In this scenario we imagine a future where industry adopts a leadership role in the adoption of the Internet of Things (IoT) and distributed ledger technology. The IoT has continued on its projected exponential growth curve and is in part responsible for a similar growth in the amount of data being generated. Industry standards and distributed ledger technologies are used to manage the cyber security and data provenance problem created by the intersection of these two growth trends. In order to create an internet of trust, which could be harnessed to increase productivity, there needs to be a sheriff on this frontier, and distributed ledgers have been deputised.

Key questions:

- How could Distributed Ledger Technologies help provide safety and security for our data-driven future?
- How should the private sector generate trust for the digital transactions and economic activity of the future?
- How should the private sector maximise the potential of the IoT?

A BUMPY RIDE, NEW EQUILIBRIUM SCENARIO

In this scenario we imagine a future where the actions of the market are unregulated and there is no leadership or industry guidelines or standards. Blockchains and other distributed ledger technologies proliferate, and compete with each other and more traditional financial products that enjoy a renaissance. The lack of standards and regulation leaves the public with a sense of uncertainty in the quality, longevity and credibility of these products. Whilst technological innovation improves, a lack of regulatory support and a lack of trust from users and industry (who are wary of a technology with a trail of pot holes in its recent past) means the pathway to the productivity potential of this technology is not smooth.

Key questions:

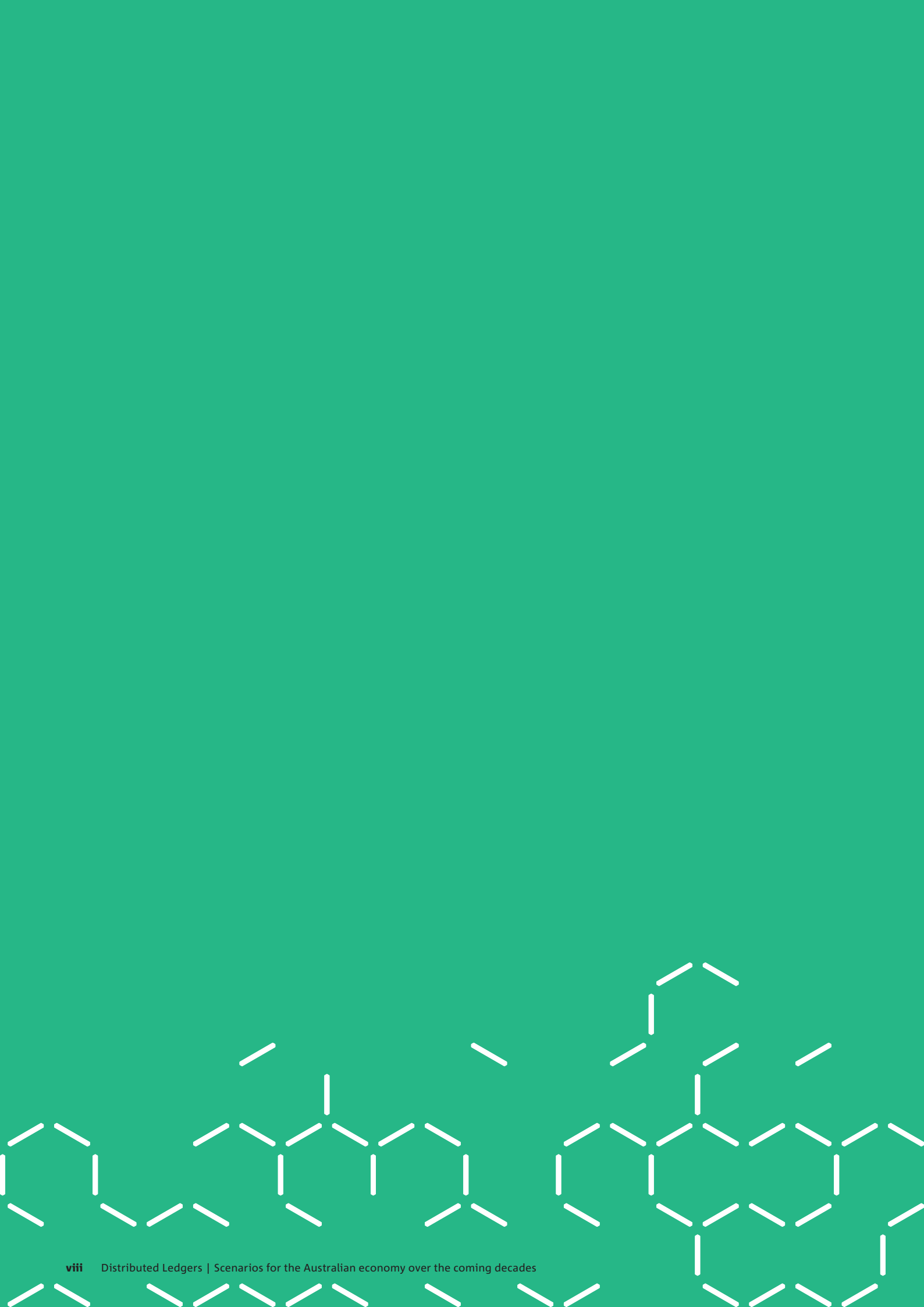
- How may the market behave if left to its own devices?
- How may public and private sector organisations provide leadership and direction to the market in order to minimise risk and optimise rewards? Particularly where innovation occurs offshore and Australia is in a position where it would need to accelerate research and development in order to remain competitive.

A SLIPPERY SLOPE, COLLAPSE SCENARIO

In this scenario we imagine a future where the worst outcomes that could occur, have occurred. The intention is for decision and policy makers, and any other relevant stakeholders to consider why these events may occur and consequently, how to prepare for, prevent, respond to and/or recover from them. This process is known as a pre-mortem. The failures in this scenario stem from the combination of technological and regulatory issues that have led to an abandonment of the blockchain brand.

Key questions:

- Why may institutions and users become averse to the use of Distributed Ledger Technology?
- How should the public and private sector ensure the relevant engagement and interaction of professionals and practitioners, from the various domains involved, in order to avoid the failures outlined in this scenario, and discover the ones that are not?
- How should both sectors provide certainty to investors and innovators operating new technologies and business models?



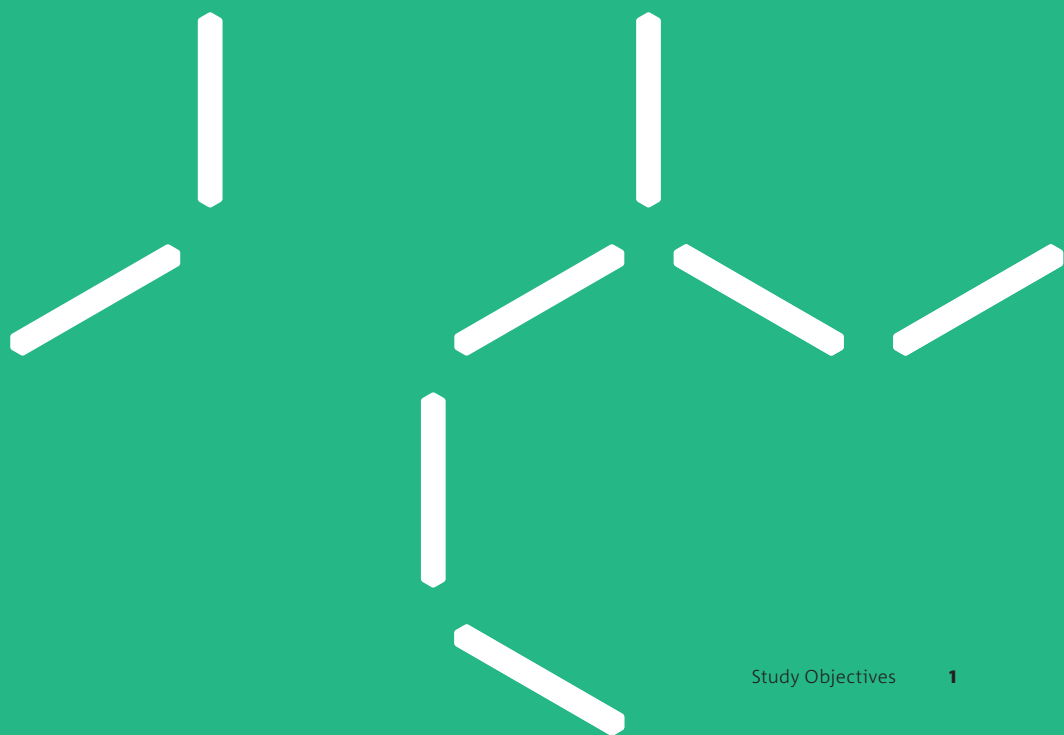
1 STUDY OBJECTIVES



This study contains analysis, interpretation and foresight, created by Data61 in consultation with subject-matter experts, in order to inform government, industry, and the broader Australian community of the plausible implications of Distributed Ledger Technology (DLT). The intended outcome is to provide advance warning of potential challenges, risks and opportunities so that leaders and innovators can make better-informed decisions, including high impact policies, for today, which will impact our future.

This study has developed a set of four plausible scenarios for the adoption of DLT use cases in the context of Australia 2030. These scenarios are based on broad groupings of significantly disruptive and/or high value and impact use cases. These scenarios are designed to:

- Provide policy makers with a greater appreciation and depth of understanding of emerging issues likely to impact on Australian business, industry and the broader economy, including associated policy implications, opportunities and challenges.
- Identify and illustrate potentially significantly disruptive and/or high impact/value use cases, and their implications, to relevant industries, sectors and communities in the Australian context.



2 DISTRIBUTED LEDGER TECHNOLOGY (DLT)

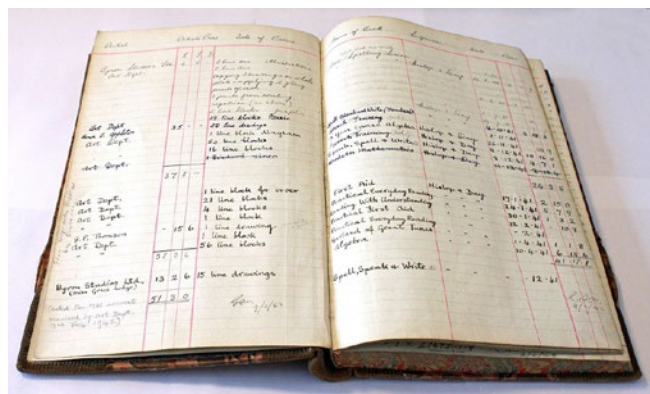
A ledger is a document containing a series of transactions. Traditionally ledgers were physical items (generally bound books) that were accessed and kept by a skilled⁶ and trusted person, who we would consider an intermediary. Entries in the ledger were permanent, usually made in ink, and tampering was generally visible and evident, as it was not possible to erase entries or remove pages in the ledger without leaving some trace. Consequently ledgers could provide both a historical record of transactions and a source of truth as to the current status (e.g. ownership) of the items it covers. Sometimes we refer to these sources of truth as ‘oracles’. The strengths and weaknesses of the trusted third party in charge of such a centralised ledger is that they are responsible for validating and safe-guarding the transactions entered into the ledger and then preserving their history.⁷

Historical examples of ledgers include general ledgers for accounting, land title and patent registers. The strengths of the trusted ledger keeper ensure the viability and sustainability of the overarching business process or system. For example, a patent clerk was trusted to enter patents on the in order to determine if another similar invention had been registered first. The trade-off for this integrity is that the process was necessarily slow.

Computers and networks enable information to be accessed, and transactions processed, by many more people and far more efficiently, but makes maintaining integrity more problematic. This ease of making transactions is the essential difference between the physical and digital environments. Digitally enabled economies require distributed ledgers that can be quickly accessed by multiple people from multiple places. Digital information can be erased, updated or altered without leaving any discernible trace of such activity. Transaction logs are available as auditable trails, but are subject to interception, interruption, modification and fabrication.⁸ In the absence of physical evidence (i.e. ink on paper) trust becomes even more crucial.

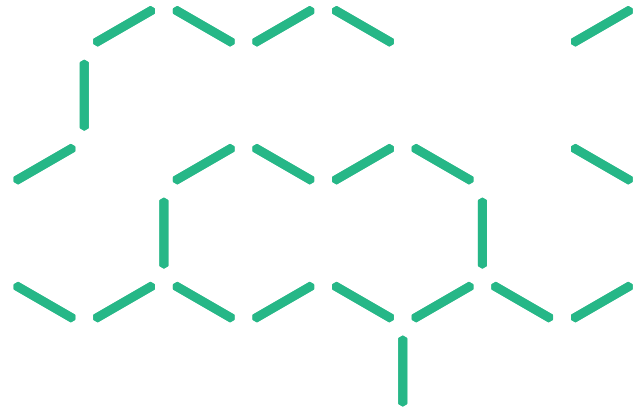
These computerised distributed ledgers remained logically centralised. Consequently, they still suffered the vulnerability of being subject to their trusted system administrators being in charge of the validation, safe guarding and preservation of the transactions, meaning there is the potential to forge, reverse and censor transactions – or otherwise carry out fraud.⁹ Owners and users of systems find themselves asking, ‘who watches the watchers?’

The internet, originally known as ARPANet, was invented as a military communications system designed to provide high-availability messaging resilient to the partial loss of the network, due to nuclear attack.¹⁰ The original users of the network were trusted personnel and the security paradigm focussed on external threats.¹¹ Consequently, even though information security is generally considered to comprise of three elements (confidentiality, integrity and availability), the internet’s design focused on availability. As the scope of uses and users of ARPANet expanded towards today’s internet, the trust model dissolved leaving a network, designed for resilience and high availability, accessed by untrusted individuals and with limited inbuilt functions for ensuring accuracy and secrecy.



Source: Edinburgh City of Print

6 Historically, reading and writing were exclusive skills.
7 Mainelli & Mills, 2016
8 Chakrabarti & Manimaran, 2002
9 Mainelli & Mills, 2016
10 Abbate, 1999
11 Timberg, 2015



Consequently, global trade and ecommerce has been operating on a network architecture that had to have information security controls bolted onto systems that, at their core, were designed to trust everyone.¹² It is clear that many actors currently use the internet with illicit and malicious intentions¹³, it is also clear that the internet has become embedded into the fabric of our economies and societies, from critical infrastructure to corporate, social and family networks.¹⁴ ¹⁵ The health and hygiene of our digital infrastructure is therefore of paramount importance to our data-driven future.¹⁶

The economy has become highly dependent on the ability to conduct digital transactions with high integrity; often at high velocity.¹⁷ Not only are traditional institutions and architectures of our society sensitive to the human frailties and malfeasance that manifest in technology, our emerging industries and social systems are especially sensitive to their influence as well.¹⁸

The relatively recent emergence of affordable consumer internet access and computer processing power has enabled decades-old technologies to provide integrity in distributed ledgers.¹⁹ Consensus mechanisms were then economical enough to enable decentralised distributed ledgers that meant untrusted participants on an untrusted network could trust their transactions. Through the use of special mathematics, known as cryptography, 'Satoshi Nakamoto'²⁰ described²¹ a method, famously used by Bitcoin, to allow participants on an untrusted public network (i.e. the internet) to exchange a digital currency with each other in a trusted fashion. In this method, everyone keeps a copy of the distributed ledger and there is consensus on all new transactions, with a complete history of all transactions kept.²² Trust is gained from the participation of the honest majority of the crowd involved.

Nakamoto's design addressed the fundamental issue in digital currencies, the 'double-spend' problem. (As digital currencies are essentially sets of ones and zeros, the double spend problem is – how do you stop these being copied and re-used when somebody spends them?) This works because by using Nakamoto's method it is evident to everyone when you have already spent your money. In other words, a fully decentralised currency system allows people to reach agreement on who owns what asset without having to trust each other or use a separate third party. The way distributed ledgers will achieve integrity in the future however, may be very different.

The description of how any technology may potentially be used to solve a problem is referred to as the 'use case'. Nakamoto's approach provided integrity for digital currency transactions, and is now being actively investigated for providing integrity in other distributed ledger use cases. The further away a distributed ledger is adapted from Bitcoin's original use case and underlying technological architecture, the less experience and understanding there is about the viability and plausibility for it working and providing actual value. The resulting uncertainty is especially evident when use cases rely on digitised representations²³ (i.e. tokens) of real-world transactions and assets, as compared to Bitcoin's self-contained digital ecosystem. Consequently the perceived, and actual, integrity of the link with the digital representation to the physical asset, or transaction can be weakened.

12 Reis, 2016

13 Australian Cyber Security Centre, 2016

14 Lewis, 2015

15 Manyika & Roxburgh, 2011

16 Australian Computer Society, 2016

17 Department of Broadband, Communications and the Digital Economy, 2013

18 Ferrara, Varol, David, Menczer, & Flammini, 2015

19 Deloitte Centre for the Edge, 2015

20 This is a nom de plume, generally considered to be a collective of individuals.

21 Nakamoto, 2008

22 This type of distributed ledger is sometimes referred to as a 'mutually distributed ledger'. Mainelli & Mills, 2016

23 For example, this could be the unique number that identifies an RFID tag.

2.1 How do blockchains work?

Descriptions and discussions of blockchains often centre on Bitcoin but this can be confusing and counterproductive as Bitcoin is a very specific technology platform. The term blockchain, however, has been widely adopted in order to refer to technologies that have taken inspiration from Bitcoin. At the time of writing there is no universally accepted definition for the term 'blockchain'. In their seminal paper, 'Nakamoto' simply referred to 'a chain of blocks'.²⁴ Standards Australia has been appointed by the International Organisation for Standardisation (ISO) as the Secretariat for the International Blockchain Standards, with the responsibility of establishing globally recognised definitions for the technology.

A simple way to imagine how the 'blockchain' method provides integrity for distributed ledgers is to think of spreadsheets. Spreadsheets are often used for much more than numbers and finances. They are often used for tasks such as risk assessments, corporate planning, and stock takes and inventory. These ledgers are often shared, or distributed, for multiple parties to contribute to the task at hand. Unfortunately this means that copies of these spreadsheets end up on thumb drives, laptops, network shares and smart phones. When the task manager wants to understand the current state of the data, they are often unsure what has been updated, by whom and when, and how accurate these entries are. In other words, the data has no global consistency or integrity.

If we imagine that in our blockchain, all the people involved in the above task are given a worksheet which is formatted in exactly the same way, and every time one of them makes an entry (enters a transaction) a copy of that row enters into the 'cloud' (where everyone can see) and it is checked (by the processing node, in accordance with the blockchain's business rules – see the 'mining' breakout box for further detail) to see if it is valid. After a set amount of time, all valid entries sitting in the 'cloud' are collected into a new worksheet and given a timestamp, which identifies when it was entered into the ledger. These entries are now locked, and cannot be changed, and everyone adds this worksheet to their own copy of the ledger as the next block.

When someone enters their transaction into the 'cloud', they may not want the details of their transaction to be visible, as it may be sensitive or commercial in nature. Instead they use a digital fingerprint that uniquely identifies the transaction, such that the entry cannot be refuted. These fingerprints are known as one-way hashes. Each hash is very easy to make but computationally infeasible to reverse and determine the information they were made from. They may also digitally sign the transaction, which uniquely identifies the author with a pseudonym. These steps provide integrity for the transaction.

As the worksheet in the 'cloud' is locked, a digital fingerprint is made of the whole block. This fingerprint is placed both on this block (locking it), and on the next block that will be made – linking them together (the way a watermark identifies a legitimate bank note). By recording this chain of fingerprints mathematically, and cryptographically, we link together all the blocks in our distributed ledger, all the way back to the original 'genesis' block. This provides integrity to the entire ledger and makes any attempt to alter, or tamper with, the contents visibly evident. The process of creating and locking the blocks, using Nakamoto's method, is referred to as 'mining'.



Descriptions and discussions of blockchains often centre on Bitcoin but this can be confusing and counterproductive

²⁴ Nakamoto, 2008

MINING

In Bitcoin, and similar blockchain technology architectures, where it is desirable for the blocks of transactions to be added to the ledger in a trusted manner, the network employs a consensus approach. The consensus approach here is known as ‘proof-of-work’. Each processing node (or ‘miner’) attempts to solve a mathematical problem – a puzzle that can only be solved by computational ‘brute force’, or in other words through iterative guesses until the solution is found – this is known as ‘mining’.

The winning miner is the one who solves the problem first. The miner is rewarded with a set amount of the digital currency used by the blockchain technology architecture and/or a commission from the transactions involved. The miner’s work, like a Sudoku puzzle, is hard to do but easily checked by the other participants in the network. They all then add the block of transactions, with the correctly guessed answer, to their copy of the ledger. The mathematics works in such a way that each block is cryptographically linked to the previous block, thus ensuring the integrity of the ledger.

The idea is that if an attacker wanted to insert a fraudulent transaction into a block, they would have to solve that particular mining problem, in order to hide the fraud, by doing more work than the entire community of other miners.

This process is trusted because we cannot be sure who will ‘mine’ the next block, and because miners do not typically have a vested interest in the particular transactions on the block they are mining, their interest is just in how fast they can solve the puzzle.

This incentive mechanism is a novel approach; however, the Bitcoin experiment has not yet reached the point where no more Bitcoin will be created. By design of the system, Bitcoin will eventually cease to be generated, in order to create artificial scarcity of the resource, and consequently keep the value high. When miners are no longer rewarded with new Bitcoin, the system will operate solely with a more conventional fee-for-service approach.

What impacts will the loss of new digital currency creation have on these systems?

- Could fraud become an issue as the incentive shifts from mining to commissions?
- Could commission fees force actors (users or miners) out of the market?
- When the Bitcoin gold rush is over, could the miners – and their dedicated and specialised data centres – disappear? What would be the impact of this degradation to the infrastructure that underpins the system?

What about quantum computing?

- If quantum computers can easily solve the mathematical puzzle in current proof-of-work systems, then what would the impact of their introduction be?
- If quantum computing is initially only available to those who can afford expensive equipment, will this create market asymmetries and social inequalities? Quantum haves and have nots?
- At what point should distributed ledgers, using proof-of-work, alter their puzzles to quantum-computer-scale mathematical problems?

2.1.1 BLOCKCHAIN IMPLEMENTATION CHALLENGES

Regulators and enterprises would need to be aware of not only the typical technical risks and limitations of blockchain technologies but of the other information management issues and human factors, such as privacy, in order to effectively manage them.

CONCENTRATION OF POWER

While proof-of-work was designed as a dis-intermediating and democratising platform, the current composition of miners in the Bitcoin network reveals another story. The commercialisation of the task (solving puzzles to receive Bitcoins and commissions) has led to industry competition that means specialised mining computers, or shares in this specialised hardware, are required to hurdle the barrier to entry. Dedicated industrial data centres operate in collaborative networks known as ‘mining pools’. Below is a snapshot of 24 hours of activity by these mining pools.

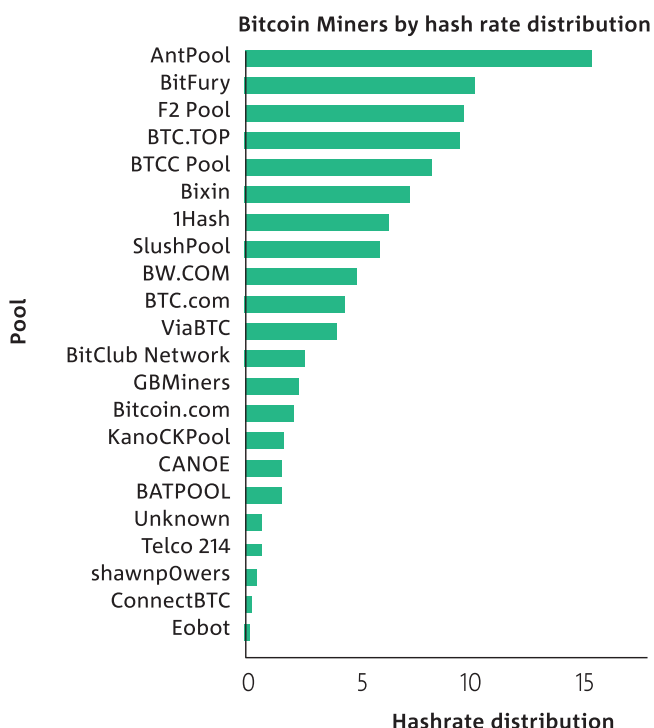


Figure 2: 24 hours of hash rates as seen on April 22 2017

Data source: Bitcoin Mining, 2017.

Mining conducted by regular individuals participating in the Bitcoin network has become negligible. The total mining resources owned by the largest five miners is approximately 84% (Antpool ~30%, F2Pool ~25%, BTCC ~15%, and Slush Pool and BWPool (BW.com) with ~7% each).²⁵ Consequently, the claim that proof-of-work is resistant to ‘bad actors’ due to the randomness of which miner will win any given block is brought into question by this market reality, which at the very least greatly reduces the number of targets that would have to be compromised by a cyber-attack.

For public distributed ledgers, such as Bitcoin, the open participation in the acceptance of code modification, and decision making around dispute arbitration and remediation, equates to a governance system which is novel to many organisations. This governance system may appear anarchic and unpredictable, and the number of individuals involved in the process balloons as the respective public distributed ledger platform becomes more popular. This governance system, while more robust and resilient to malicious influence than others, is still corruptible in the event of a majority of participants colluding, achievable through a co-ordinated, or nation state commissioned, cyber-attack. This risk is concentrated by the market dynamics of Bitcoin’s mining pools, dominated by a small number of, mostly Chinese-based, miners.

CONSUMPTION OF POWER

The proof-of-work competition also has the added cost of the wasted computational power and energy used by all the miners involved in the process. The snapshot below depicts the Bitcoin miners as currently consuming over 11 Terra Watt hours per year. To put this in context, Bitcoin mining currently accounts for 0.05% of the world’s energy consumption, which could power over a million households in the United States of America.²⁶ This is the hidden transaction cost of the system.

²⁵ Bitcoin Mining, 2017

²⁶ Digiconomist, 2017

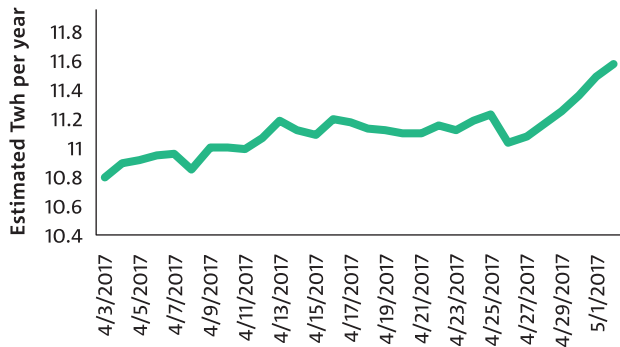
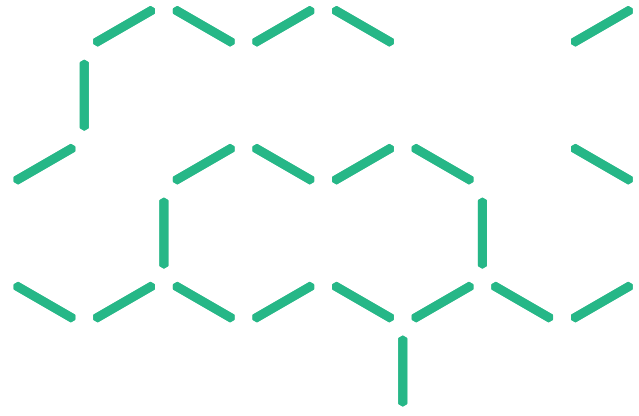


Figure 3: Bitcoin Energy Consumption Index Chart

Source: Digiconomist, 2017. As at 4 May 2017.

TOXIC DATA

The other-side of the coin with having a permanent and persistent ledger is the issue of not being able to delete or alter the data on it. Consequently, there are several significant issues that must be considered in the context of the specific use case that the distributed ledger will be employed in.

Blockchain bloat

As ledgers are designed to retain all previous transactions, the ledger's size will increase. This increase in size will continually need to be forecast against both the capabilities of the network and the future behaviour of the users. For example, the increasing popularity of Bitcoin is having an exponential influence on the size of that blockchain. This bloat has the potential to detract from its utility if the size becomes too great for everyday participants to readily use.

Data spill

If something illegal, unconscionable, classified or otherwise objectionable is entered onto the ledger, it is there forever. The first question is, does this invalidate your continued use of the ledger? The second question is, if you need to 'roll-back' the ledger, how do you retrieve, or retract the versions of the ledger that have been distributed to the other participants in the network? What governance system needs to be in place for this to happen? What impact does a distributed ledger have on the ability to be forgotten? In some jurisdictions, such as

the European Union, citizens have a right to be forgotten. What does it mean if a court, or other authority, orders a transaction to be removed 'as if it had never occurred', and it can't be? Today's users appear to have accepted information being permanently online once posted. While blockchains, such as Bitcoin, offer pseudonymous transactions, if a pseudonym is identified and linked to a user, then that user's transaction history becomes visible. Could a data breach causing the disclosure of a history of transactions alter public perception? What about the perception of organisations on data permanency?

There has been research²⁷ into the ability to redact transactions / entries into distributed ledgers, however there is still the question of retrieving / retracting the previous versions. This presents a contradiction for the ledger. If the reason distributed ledgers are trusted is because they contain a permanent and persistent record of all transactions, what is the longer term impact on the trust of users from redacting these ledgers? Particularly future users who were not part of the decision to redact the ledger?

Needle in a 'block-stack'

As a permanent and persistent record, the evidentiary trail of the ledger could feasibly be used against an organisation or individual where the ledger documents something they ought to have known and had an obligation to act upon. The visualisation and analytical interrogation of ledgers is an emerging field, however, advances in this are expected to grow rapidly due to the significant value it could generate. Such tools could demonstrate insights that could be held against organisations and individuals. The increasing volumes of data being collected and stored by organisations pose the risk of not knowing what information is available already, however distributed ledgers pose the additional vulnerability of making these records more accessible, and permanent. Data that has previously thought to be de-anonymised, such as metadata, could be re-identified. What does this mean for privacy if the data cannot be removed or redacted?

COMPUTER PROCESSING POWER

There are issues associated with the increasing rate of processing power. As Moore's law continues²⁸ with a doubling of processing power every 12 – 18 months, or potentially if there is a stepwise change brought about by a colossal increase from quantum computing, there may be significant consequences to existing distributed ledger infrastructure - hardware and software.

Marketplace asymmetries

The proof-of-work method relies upon a mathematical puzzle that can be adjusted in order to make a computer spend (on average) a fairly specific amount of time working on it. The current proof-of-work puzzles cannot be made hard enough for a quantum computer; they would always be trivial to solve. Quantum computer puzzles are already available, however the issue is that if the introduction of quantum computing is not uniform (and it almost certainly will not be), then there will be “haves” and “have nots” in marketplaces that benefit the haves. The questions are, ‘What are the conditions for a given distributed ledger to transition to any new advanced computing platform? Will proof-of-work be the only consideration for this transition, or will other emerging innovations also be susceptible to this disruption?’

Confidentiality

Encryption standards are continually increased in order to maintain their strength against increasing computer power.²⁹ Over time faster computers and newly discovered flaws in encryption make this security more easily defeated. If the information stored on distributed ledgers is encrypted in order to control access to it, or otherwise protect it, the challenge is that these persistent entries will retain the encryption they were created with as the ledger ages. Ledgers that are decades old will have to contend with vastly more powerful computers, potentially capable of easily defeating the encryption of older entries.

LOST IN TRANSLATION

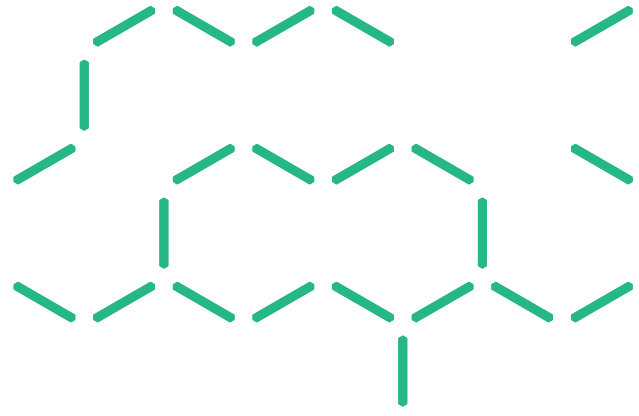
Many other distributed ledger products and platforms, are based on the Bitcoin ‘source code’. This code is freely available to download, re-engineer and/or re-purpose. The limitations of Bitcoin (transaction volume and frequency) designed into the system in order to enable the necessary consensus, incentive and immutable ledger mechanisms, have been transferred to these Bitcoin inspired products and platforms. Modifications to, and experiments with, both the code and the function of the three underpinning components are happening (including private, permissioned and proprietary ledgers), although at this time there is still a suboptimal understanding and appreciation of the implications and benefits of these changes, in part due to the lack of an agreed language.

The lack of a formal taxonomy for an emerging technology architecture is not unusual, but does have a negative impact on the ability to participate in meaningful discussions about possible implications. The ability for software to be offered en masse presents the potential for distributed ledgers to be introduced as a new method of transacting and recording information in various industries and jurisdictions. Considering the implications of these implementations is complicated by the introduction of unprecedented, novel and emerging use cases. Consequently, risks and opportunities may be overlooked in conversations between technologists and non-technologists, as well as presenting barriers to learning and exchange across the technical community.

A proposal has been submitted in draft by the British Standards Institute (BSI) to the International Standards Organisation (ISO) Technical Committee (TC) 307 Blockchain and distributed ledger technologies, for the development of terminology and taxonomy standards for blockchain. The ISO TC 307 resolved for the BSI to submit the final proposal in May 2017 and work on the standard will commence thereafter.

²⁸ Intel, 2015

²⁹ National Institute of Standards and Technology, Computer Security Division, Computer Security Resource Centre, 2014



INTEROPERABILITY

Standards enable innovations to occur either-side of defined interfaces.³⁰ These junctions are important as it enables complex ecosystems to form and evolve. They require a relatively stable and defined system, however, in order to be relevant and drive innovation. Interoperability is more than a technical configuration; there must be trust in the market that the standard will be adhered to. The participation of numerous countries in the current international standards development exercise, however, makes the global adoption and uptake of relevant standards more likely.

Defining standards too early in the evolution of a technology lifecycle could be detrimental, as competition for innovation and commoditisation could produce counterproductive practices and alliances that fragment the market. When competing, the better standard may not win. If organisations move too early, potentially better alternatives could be stifled, and if they move too late the costs of switching to the standard will be higher for existing users.

One of the main drivers for interoperability appears to be an extension of the original digital currency use case, in particular the ability to remit currency. If different ledgers are able to trade and exchange value between themselves and the real economy, there is a potential for a significant amount of liquidity to be injected into the global market. This liquidity presents significant challenges in the highly regulated banking and finance sectors.³¹ Consequently, entwined with interoperability standards is the requirement to establish complementary identity standards and/or regulations.

Interoperability also occurs at the legal layer. ‘Smart contracts’ are essentially programmable transactions (sometimes referred to as programmable money) that automate business processes. Defining contractual performance in software requires prudence and forethought. Hundreds of years of case law, legal tests such as ‘the reasonable person’ test, and the chaotic nature of real-world events and human frailties present an environment that is impossible to entirely emulate in code. This software is not a contract in reality, and ideally should exist wrapped within a legal framework that links the code with a contract.³² Perhaps the term ‘automated contract tools’,³³ or ‘automated transaction tools’ may lend themselves to less confusion. Technologists need to appreciate the legal risks, and opportunities, present in the problem they face. In worst case scenarios, irrevocable transfer of title could occur, or material amounts could be claimed by parties unable to exercise remedies otherwise available to them at law. Consequently, distributed ledgers need to be tested for failure in both an operational and a legal sense.

Whilst software is global, the law is not. Complex legal questions may occur when executing ‘smart contracts’ across multiple jurisdictions. In particular, the question of what jurisdiction the ‘smart contract’ was operating in is a fundamental determination. The distributed ledger could also potentially be required to be compliant with an unwieldy number of legal and regulatory frameworks for many, if not all the jurisdictions it is operating in.³⁴ Customary law and trade practices are often benchmarks that support dispute resolution in multi-jurisdictional scenarios.³⁵ The disruptive potential of distributed ledgers includes potentially new business models, and new value-chain participants, however, this means accepted industry norms are yet to be formed and tested.

³⁰ An interface simply being a format, or gateway that separates different technologies which are combined together in a value chain. For example, a power outlet is an interface. Innovations and regulations to the power grid and innovations regulations to the device using the electricity are separated.

³¹ Eversheds Sunderland, 2016

³² Christie, 2016

³³ Bank for International Settlements, Committee on Payments and Market Infrastructures, 2017

³⁴ Eversheds, 2016

³⁵ Benson, 2007

SCALABILITY AND PERFORMANCE

Descriptions and discussions of distributed ledgers often centre on Bitcoin but this can be confusing and counterproductive as it represents a very specific use case. The Bitcoin network's design limitations make it unlikely to ever compete with global commercial banking and finance systems. Bitcoin transaction volumes are several orders of magnitude lower than credit card systems, and the batch process takes at least ten minutes to occur, with transactions needing to wait at least an hour in order to be confirmed. In practice, transactions frequently take far longer than this, with preferential prioritisation given to transactions with better commissions. On top of this, the proof-of-work method means the blockchain may have multiple miners solving the puzzle and creating a legitimate block for the same round, essentially forking the chain into two or more blockchains. Until this fork is reconciled, there is no certainty that transactions being entered will exist on the reconciled blockchain as only one blockchain (the longest) will remain. In 2013 a Bitcoin fork lasted 6 hours³⁶, leading to this amount of time being the defacto standard for Bitcoin transaction certainty.

Fuelled by its own popularity, Bitcoin's distributed ledger continues to grow; the sheer size of this file may eventually become unmanageable, eclipsing the capabilities of the network that originally supported its emergence.

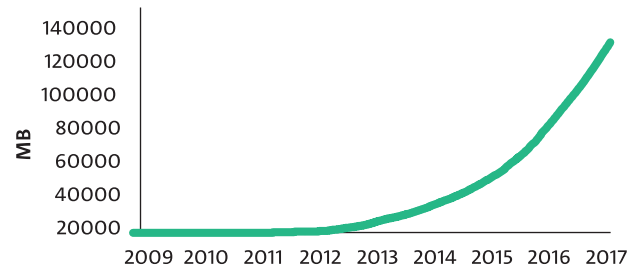


Figure 4: The size of the Bitcoin Blockchain

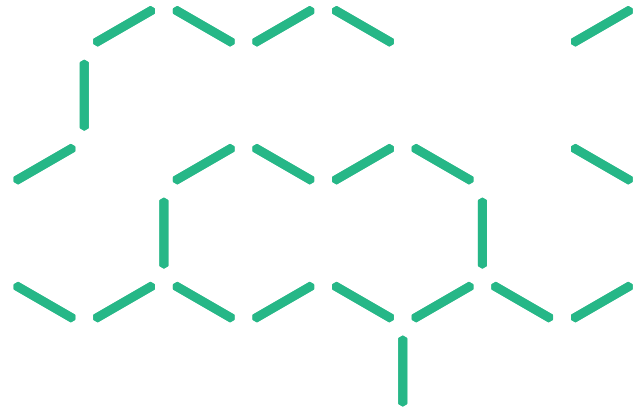
Source: Blockchain.info, 2017

Many other distributed ledger products and platforms are based on the Bitcoin 'source code'. This code is freely available to download, re-engineer and/or re-purpose. The limitations of Bitcoin (transaction volume and frequency) that was designed in order to enable the necessary consensus, incentive and immutable ledger mechanisms, have been transferred to these Bitcoin inspired products and platforms.

Sharding is an established technique of breaking a database into separate independent pieces. These independent pieces, which can be processed concurrently, may significantly increase the throughput of the overall system. Sharding has been proposed to improve the performance of blockchains. This involves operating parallel blockchains for proof-of-work methods to concurrently mine them. Although the requirement to traverse the various blockchains in order to establish transaction histories, consequently results in performance gains that are sublinear at best.³⁷

³⁶ Buterin, 2013

³⁷ Evans-Greenwood, 2016



2.2 Trust

Traditionally, the telecommunications industry has been regulated as being essential to public health, interest, and welfare. Hence a core component of its regulatory model was to expand service to give everyone access. In many countries access to basic service is now considered a necessity of modern life. Historically, the financial services industry has been regulated by the premise that trust and confidence are paramount to the orderly movement of trade, goods, and money. And given that a special trust is conferred on financial entities, they must conduct their business in a safe, sound and prudent manner.

World Bank 2002 ³⁸

The English Law concept³⁹ of trust arose in the days of knights going on crusades. The knight would place his lands in the hands of a trustee who was expected to treat the lands in good faith and hand them back to the knight on his return. This concept of trust remains with us today in our digitised world where we have to rely upon many actors, who we will never meet, to act in good faith on our behalf. When considering trust, the question being asked is, ‘who are you trusting to do what, and when?’, which is highly contextual. Consequently, trust is often granted for only a very particular application, and usually a set period of time.

It has been recognised for several decades that modern society has become dependent upon electricity, telecommunications and banking.⁴⁰ Indeed, advances in telecommunications, and its widespread adoption, have seen access to the internet considered a human right.⁴¹ The nature of society’s dependency on these utilities has advanced in parallel with their respective wide-scale adoption and online connectivity. Our societies have no choice but to trust them. The fusion of finance and technology, known as ‘fintech’, poses the question, ‘what measures are now required in order to establish trust in our current digital age, and emerging data-driven future?’

Blockchain has been widely celebrated as being able to generate trust on the internet, where trust is difficult to establish.⁴² What is the blockchain trusted to do, and for how long, is a fundamental question. The answer(s) to this will have an overarching impact on the development of this technology and its adoption. In Bitcoin, that digital currency can be trusted to retain its integrity because it cannot be counterfeited. The question is, ‘how will blockchain, or other trust building integrity methods, perform for use cases beyond digital currency?’ Or in other words, ‘what else will it be trusted to do?’

The challenge with software is, for the most part, that is essentially a black box.⁴³ Trust is subjective, conditional and contextual.⁴⁴ Something or someone is trusted to perform a particular action. For example Bitcoin, having been in operation since 2009, has demonstrated that it will do what it is intended to do. Newer distributed ledger technologies, however, require time to build their reputations and awareness for what they can be trusted to do. Consumers seek competence, for which reputation is a proxy.⁴⁵ Research demonstrates that trust is tightly coupled with performance. Poor performance quickly erodes trust, and people’s trust in machines erodes much faster than in people.⁴⁶

Understanding technological capabilities is paramount for regulators so they may ensure they are able to set appropriate regimes with respect to information disclosure, fair commercial practices, such as quality of service, and dispute resolution and redress.⁴⁷

38 Sadowsky, Dempsey, Greenberg, Mack & Schwartz, 2003

39 Grimaldi, & Barrière, 2004

40 McCullagh, 1998

41 United Nations General Assembly, 2016

42 The Economist, 2015

43 Rice, 2007

44 Hawley, 2012

45 Ibid

46 Interview with Dan Conway, Research Engineer – Interactive Behavioural Analytics, Data61 (CSIRO)

47 OECD, 2015

2.2.1 THE TRUST MACHINE

The core benefit is the underpinning capability of distributed ledgers to establish a fact at a given point in time, which can then be trusted.⁴⁸ Distributed ledgers achieve this through automating the three roles of the trusted third party: validating and safe guarding transactions, and then preserving them.⁴⁹

By enabling facts to be stored in a permanent and persistent fashion, the distributed ledger is able to provide a series of benefits, the most prominent of which has been to provide global consistency – a requirement for any digital currency. The main business benefit for many fintech use cases is reduced, or zero, counter-party risk. The logical extension of establishing facts in a chronological order is the ability to send and receive messages that have a high integrity in terms of both the message and its source. This capability presents many potential productivity benefits well beyond fintech.

Permanent and persistent ledgers produce value from this trust through the following functions:

Oracles

Through establishing this audit trail, the distributed ledger is also able to act as an oracle. An oracle is any source of information that is deemed to provide credible and reliable (trusted) information. As an oracle, a distributed ledger can be used as a reference that contributes to the integrity of other transactions. A distributed ledger could be an oracle for identity, content and/or transactions. For example, a distributed ledger may act as an oracle that records the data from trusted weather sensors and stations. This record could be used by farmers and their insurers as an agreed set of facts used for insurance claims of crop damage.

In cyber security, a distributed ledger could be used to publish the digital fingerprint, or hash, of an authentic and trusted software/firmware/security update so that a user could validate, and trust, what they download. A distributed ledger could also be used as a record of how a device should be configured, and if the hash of the configuration of a device is found to be different, the device would be checked to see if it is misconfigured or hacked.

Provenance

Distributed ledgers can store digitised representations of real-world transactions that may be trusted to prove the history of an asset or object. By tracing the transactions, the identity of the asset or object (or the current owner) can also be demonstrated. Whilst this may be easier for an easily identifiable asset like a diamond⁵⁰, a commodity like grain or milk generally requires a proxy for each asset unit such as an RFID tag – increasing the assurance being provided but not providing absolute provenance. Provenance of Australian primary resources exports would provide protection for our markets and brand.

Accountability and Auditability

The permanent and persistent storage of assertions, or transactions, allows for them to be trusted for governance or evidentiary purposes.⁵¹ For example, forensic analysis and discovery processes could be conducted without the need for special methods, expensive technologies, or significant resources being employed. The clear benefit here is reduced court costs where a jurisdiction recognises the facts in the distributed ledger as admissible. These reduced costs would most likely create positive externalities such as improved behaviours, like honesty, encouraged by the transparency and immutability of the ledger.

Blockchains present opportunities for regulators to access high integrity records of transactions in real or near-real time. Programmable transactions and automated contract tools would enable regulators to enact granular and risk-based market controls aligned with this surveillance. This unprecedented level of engagement would open pathways to productivity gains and risk management if managed appropriately. Financial transactions and markets would be potentially provided with increased liquidity if compliance processes, including Anti-Money Laundering and Counter Terrorism Financing (AML/CTF) regulations were automated.⁵²

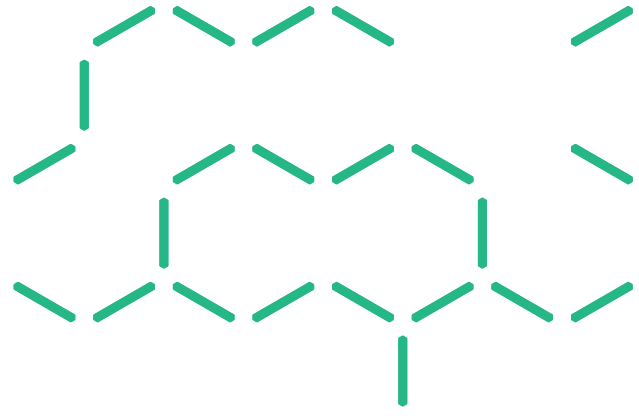
48 The Economist, 2015

49 Mainelli & Mills, 2016

50 Everledger, 2017

51 Morrison & Foerster LLP, 2017

52 Eversheds Sunderland, 2016



2.3 Identity

Identity is... [the basis for] trust and confidence in interactions between the public and government; it is a critical enabler of service delivery, security, privacy, and public safety activities; and it is at the heart of the public administration and most government business processes. How identity information is collected, used, managed, and secured is of critical interest to leaders in the public sector.

Government of Canada⁵³

Digital identity is verging on a human right. Electricity, telecommunications and banking have incrementally established themselves as essential pillars of our society.⁵⁴ In order to operate in our economy, digitally identifying users has become critical to establishing trust in transactions, and for accessing essential services. Digital identification services currently verify claims about the attributes of an identity, usually by assessing the provenance of a supplied document.

In our globalised world, every commodity consumed corresponds to the movement of people, and/or materials across locations.⁵⁵ The underlying supply chains, however, are often opaque to the end consumer. Creating transparency and provenance for consumer goods, by identifying and cross-referencing their relationships with locations and people, enhances trust and confidence in these transactions.⁵⁶ Proof of identity is, however, one of the most fundamental, often challenging, and resource-intensive transactions involved in our heavily digitised world.⁵⁷

Identity is the assessment of verifying personal attributes, personal history, relationships and/or transactional histories. The assessment of identity is used to minimise any perceived gap in trust. This gap is proportional to the measure of risk, which reflects the perception of the identity and any potential losses. The trade-off is often a loss of privacy in exchange for access to high value transactions. The downside has historically been the loss of privacy where the transaction is asymmetrically of moderate to minimal value to the individual being vetted compared to the risk presented to the other party.

For example where a patron must display their identification in order to check-in at a hotel, or enter a licenced premises. In order to verify certain attributes of their identity to complete the transaction they also expose other attributes of their identity they may not wish to disclose. This disclosure places all of their attributes, on that document, at risk of further unwanted disclosure or illegal use.

Technology is fundamentally changing our ability to represent ourselves. At the same time the nature of our connected world is changing our perception of identity and trust. Consequently, new models for identification are emerging, although their implications are not necessarily clear at this time. First the old model of a singular state-issued credential evolved into an augmented and networked approach that uses the state issued credential as a start. Now the current evolution is towards knowledge-based aggregations of attributes of identity, often much more under the user's control. This includes things like reputation scores from social media, peer-to-peer sharing, and gig economy platforms.

53 Government of Canada, 2011

54 McCullagh, 1998

55 Steiner, 2015

56 Williams, 2015

57 ADCCA, 2016

If designed well, distributed ledgers have the potential to provide answers (by acting as trusted oracles) that do not present a privacy risk. These ledgers may hold and selectively share verified claims for attributes of an identity, along with the provenance of the verification or source document. For example – yes, this is John Doe, or yes John Doe is old enough to enter these premises, or to receive this senior citizen benefit, but without providing further extraneous personal information (e.g. date of birth or address). There is a caveat here: distributed ledger use cases often describe them as metadata repositories. These repositories may potentially violate rights to privacy more so than ledgers containing identity attributes by recording behaviours and indicating sensitive information.

Transactions in any ledgers are predicated on the integrity of the identities involved in these transactions. Ledger transactions are generally either about change of ownership, or the recording of a statement of fact. Consequently, the ability for a ledger to identify the parties involved is paramount to the integrity of, and trust in, the transaction. Even though proof-of-work is the current standard in producing integrity for blockchains, the use of trusted known (identified) nodes is emerging, and it is highly plausible to imagine distributed ledger methods based entirely on the trust attributes of reputation and relationships (referrals) being used in the future.

The implementation of blockchain-enabled identity systems would mean more tools available for markets to assure and assess identity in order to assure themselves of appropriate security risk management. Specialised identity ledgers would be a practical approach to managing identity, and associated regulatory compliance, and for facilitating interoperability between distributed ledgers. Whilst manual processes manage identity in today's world where more than 80% of the money supply is currently kept in traditional distributed ledgers⁵⁸, the question is, 'what identity management processes and infrastructure do we need in in order to maintain and increase productivity for tomorrow's world, which is becoming ever more automated and digitised?'

58 Clark & Whitbourne, 2009

3 IMPLEMENTATION CONSIDERATIONS



‘In 2009, the first bitcoin transaction took place. Until recently, many people viewed the idea of such an alternative currency which existed only virtually, as a mere curiosity, another strange development of the computer age. But times have changed.’

C.D. Howe Institute⁵⁹

When considering the implementation of a distributed ledger solution, like any technology project, the approach should be technology agnostic, focusing on the problem to be addressed. If after appropriate consideration, the feasibility of a distributed ledger solution is explored, then assumptions and regulatory requirements should be reviewed in order to ensure the specific characteristics of a distributed ledger do not violate any requirements, and that no new opportunities or risks are being overlooked.

Distributed ledgers are a type of database, but the trade-offs made in order to increase the integrity of the system often make it less efficient (due to proof-of-work/mining) and more costly to operate than a distributed database.⁶⁰ The question is, ‘what is the value proposition of the solution?’ Successful business/use cases illustrate the projected return on investment, now and into the lifespan of the system, which may be several decades into the future. Consequently, strategic thinking on the emerging future environment the ledger would operate in is beneficial.

The literature on IT project management failure attributes risks to both technology and management.⁶¹ Although technology is becoming more robust with time and techniques for improving quality are rapidly maturing, the ‘lure of the leading edge’, however, remains a seductive critical failure factor, and may influence decision makers towards subjective investments.⁶² Consequently, decisions made in reaction to perceived threats of disruption and opportunities of innovation may influence suboptimal solution pathways.

Distributed ledgers are not a silver bullet, they are one tool within a toolbox of both established and emerging technologies that may be called upon to face a given challenge.⁶³ A new distributed ledger would also be only one component of the overall ecosystem.⁶⁴ It would not be introduced onto a blank canvas. The organisational context, and human factors, are also crucial as the ledgers would interact with, adapt to and evolve with existing business and social structures. Consequently, clear-headed consideration on the role the ledger takes in this ecosystem would assist in providing assurance that it will be a value-adding component now and into the future.

The complexity of the impact of these ledgers in terms of regulation and business practice should not be underestimated. System testing is crucial for any implementation, with distributed ledgers however, testing for failure is extremely important, given the potential impacts. Like safety systems, distributed ledgers should fail safe, especially where the risks are materially significant.



The complexity and necessity of cross-domain knowledge and education is brought to the fore by blockchain.

⁵⁹ Koepl & Kronick, 2017

⁶⁰ ‘Digital currency transfer and long-term storage of transactional data may be less expensive. However, program execution and storage of big data may be more expensive.’ Staples et al, 2017

⁶¹ Flowers, 1996

⁶² Ibid

⁶³ ‘DLT is one of many transformative new technologies that will shape future financial services infrastructure and should be seen as part of a toolbox.’ World Economic Forum, 2016

⁶⁴ Staples & Zhu, 2017

3.1 Skill requirements

The trend for the Australian economy is towards more highly skilled labour, with this sector projected to double from 1991 to 2019.⁶⁵ In order to support this workforce, education and training are becoming more important than ever.⁶⁶ Digital literacy is needed along with traditional numeracy and literacy.⁶⁷ This will most likely be true for many jobs, driven by trends in automation and the growing digital immersion of our economy.

The complexity and necessity of cross-domain knowledge and education is brought to the fore by blockchain. Blockchains can be fraud controls, potentially cyber security controls, and are utilised in digitised transactions that represent the performance of legal contracts, can and do operate across multiple jurisdictions, simulate or interact with banking and finance systems. They are increasingly being used to record activities, actions and assets in the real world. In addition to the risk and opportunities that lurk in the intersection of these various professional domains, the permanence and persistence of new distributed ledgers presents challenges and risks that are novel in information systems. Consequently professionals and practitioners from many disciplines would be required to be engaged in order to balance risk and optimise reward.

Consequently, in order to capitalise on these opportunities and minimise their risks, IT professionals would require an awareness and appreciation for the fields of accounting, audit, fraud control, law, banking and finance, and any relevant sector in which a given blockchain will operate. While cross-domain knowledge requirements are not an issue isolated to blockchain and distributed ledger technologies, the significant potential impact of their risks (especially legal risk) coupled with the relative immaturity of the field suggests a prudent approach is warranted. Public and private sector initiatives, such as training, guidelines and standards, would assist technical and non-technical professionals realise the benefits, and reduce the risks, of adoption.

3.2 A conceptual shift

Given this novelty, and relative immaturity, of blockchain innovation, there are a series of suggested considerations to be undertaken when assessing the viability of these solutions:

- The volume of transactions on a ledger will increase if the digital asset requires additional record-keeping. Significant transaction record keeping changes may require a redesign of the ledger's format.
- A distributed ledger does not need to be a dis-intermediator in order to generate value.
- A distributed ledger does not need to have a crypto-currency.
- Distributed ledgers may provide value as a fraud resistant and tamper evident record.
- Persistent ledgers could present problems, such as for privacy and perpetual agreements.

3.2.1 STABLE DATA

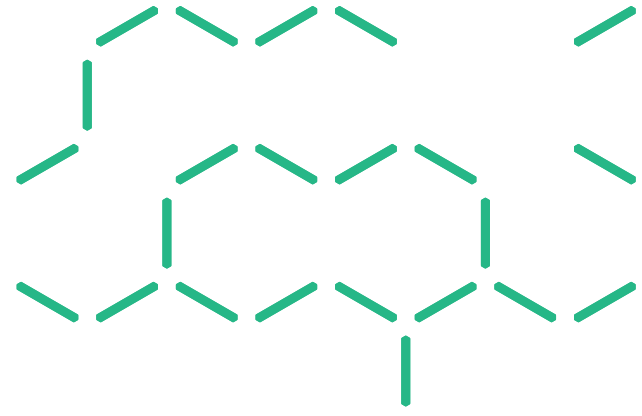
The volume of transactions on a ledger will increase if the digital asset requires additional record keeping. Significant transaction record keeping changes may require a redesign of the ledger's format.

Given the overhead required to provide integrity in a distributed ledger, particularly in a proof-of-work method, the stability of the data, about which the transactions are being made, should be considered. Any network limitations, especially due to system growth and user adoption should be weighed against the necessity to update the details of the underlying assets of the ledger. These conditions may appear stable now, but may change over time. Examples of stable data include land parcels and buildings on land titles registries that may exist for centuries, and most biographic data, such as date and place of birth, which does not change.

65 Hajkowicz et al, 2016

66 Ibid

67 Ibid



A principal design question, with respect to stable data, is about the governance of the ledger. What capability would an organisation have to respond effectively to a regulatory change (i.e. a change impacting the format, privacy provisions, or records management of the information) about the transactions? If the organisation is using an unpermissioned public ledger, would the organisation be able to make the required changes to the ledger for future transactions, or retract/redact the necessary historical transactions or information? How would the organisation retrieve or destroy historical transactions held by other organisations holding copies of the ledger? Clearly stable public-domain data is the safest option, however, risk assessments would be needed to consider the potential for changing requirements, regulatory or otherwise, and the required risk treatments (avoid, mitigate, share, or accept).

Bitcoin Unlimited

Bitcoin's design constraint, a block size limit of 1MB (which supports three to seven transactions per second) is proving insufficient, resulting in significant delays with the transaction queue, in February 2017, reaching an all-time high of over 100,000 transactions.⁶⁸ Consequently, a group called Bitcoin Unlimited is advocating for removing the block size limit. So far, actions by Bitcoin Unlimited have caused divisions in the Bitcoin community.^{69 70} Bitcoin Unlimited have released updates to the Bitcoin software in order to enable the removal of the block size limit. One update contained a bug that resulted in a miner losing 13 Bitcoins (~USD\$17,000)⁷¹ and another update introduced a cyber security flaw that saw half of Bitcoin Unlimited's users attacked.⁷²

This example highlights both the difficulty of governance, and the potential impacts of sub-optimal modifications, with distributed ledgers.

3.2.2 HAND-OFF POINTS

A distributed ledger does not need to be a dis-intermediator in order to generate value.

Nobel Laureate Ronald Coase's theory of the firm argues that firms arise because hierarchical structures reduce transaction costs. Online platforms have the capacity for purchasers (employers) and providers (employees) to transact quickly, efficiently and with a clearer picture of the risks and rewards. This dis-intermediation potentially removes or reduces transaction costs and information asymmetries. Consequently, in the digital era there is uncertainty on whether the firm would remain the most efficient means of organising labour.⁷³

Dis-intermediation is often cited as one of the more important benefits of distributed ledgers. Their ability to reduce friction, however, is not limited to dis-intermediation. Reductions in transaction time and cost, and improvements in fraud and corruption control may lead to the establishment of greater levels of confidence, trust and productivity for institutions and existing multi-party transactions. Consequently, firms may have a new lease on life.

Trade finance and logistics have presented themselves as prime use-case candidates. The visibility of consignment locations alone offers a dispute management and efficiency mechanism. Each hand-off in a supply chain reduces line-of-sight and introduces the potential for fraud, theft, accident and human frailty. Many legacy supply chains are also not necessarily understood end-to-end by their users. Hand-offs from Australia to an overseas port may range from the tens, into the hundreds. Providing greater visibility of these hand-off points may present value outweighing the costs and limitations of the architecture. By 2025, Australia's trade is expected to increase 129%, with containerised trade to almost double from 7.2 million units in 2013 to 13.6 million.⁷⁴

68 Redman, 2017

69 Hertig, 2016

70 Hertig, 2017

71 Ibid

72 Woo, 2017

73 Hajkovicz et al, 2016

74 Department of Infrastructure and Regional Development, 2014

By contrast, the original Bitcoin use case and initial wave of subsequent blockchain examples were self-contained. Title transfers occurred for digitised bearer assets that were represented on one ledger. Bitcoins changed hands, and ‘smart contracts’ were processed, all in the virtual world. Real world processes that interface with distributed ledgers are very messy by comparison, and may not provide absolute certainty of the transaction, but may provide something better than what is currently available. These solutions may benefit from identity and transaction ledgers running in parallel.

Hand-off use cases

Land Titles

There are many examples of governments implementing blockchain solutions for the conveyancing of land titles such as Sweden,⁷⁵ the Republic of Georgia,⁷⁶ and Ghana.⁷⁷ Land title registers were one of the original examples of the benefits and productivity of centralised registers. These new distributed ledgers generate value through red tape reduction and increased transparency, which lead to the benefits of reduced transaction time, cost reduction, and safe-guards against fraud and corruption.

Supply Chains

Letters of credit for international trade finance⁷⁸, online booking sites⁷⁹ and share trading^{80 81} are all examples of multi-party transactions improved by distributed ledgers increasing visibility and providing trustworthy documentation, which reduces transaction times, reduces fraud and errors, and leads to greater confidence and certainty in the process.

3.2.3 INCENTIVE

A distributed ledger does not need to have a crypto-currency.

The motivation for participating in the proof-of-work method is effectively entrance into a digital currency lottery in exchange for the contribution of electricity, internet access, computer hardware, and associated cooling. Consequently, the costs of ensuring the integrity of the ledger are defrayed across the market. Bitcoin emerged with the availability of excess consumer network bandwidth and computer processing time.⁸² When these resources became cheap enough there was willingness for market actors to invest their electricity, computer’s effort, and internet access for potential Bitcoin rewards offered through the mining process.

Distributed ledgers do not necessarily need to offer digital currency as incentive. There are alternative, and emerging consensus and integrity methods that do not require proof-of-work to be undertaken. Currently these other methods are generally being applied to permissioned, and private distributed ledgers. In these situations, the incentive for participation should be clearly articulated in order to manage expectations for involvement, and return on investment. Options for incentives include value propositions such as visibility of supply and value chains, and other fraud-control features. The governance of private distributed ledgers should articulate the value it provides.

75 Lantmäteriet, Telia & ChromaWay, 2017

76 Bitfury, 2016

77 Bates, 2016

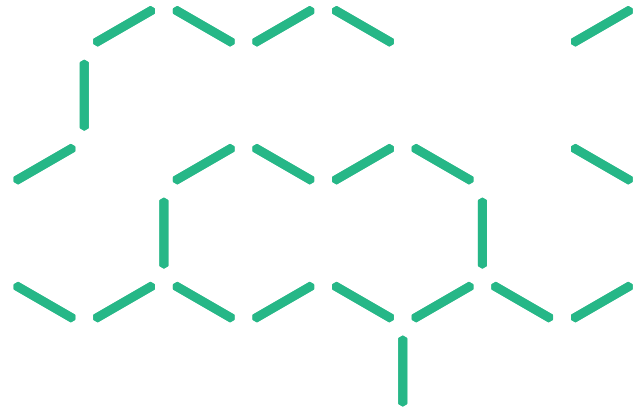
78 HSBC, Bank of America Merrill Lynch, IDA Singapore, 2016

79 Microsoft News Centre, 2016

80 Overstock, 2016

81 Harkness, 2016

82 Deloitte Centre for the Edge, 2015



Adding additional digital currencies to a crowded market, for new ledgers, is not without risk. New currencies face fluctuating exchange rates and valuations, are challenged to motivate user adoption, and are reliant on a committed consumer/user-base, meaning that Bitcoin will most likely remain the dominant non-fiat digital currency into the foreseeable future. It is worth noting that the incentives through proof-of-work methods will eventually revert to commission-based fee-for-service models because the issuance of digital currencies is limited by design and will run out, in order to create an artificial scarcity. Whilst these blockchains will remain public and permission-less, the market's behaviour, and ability to maintain trust, will be tested as they enter a new stage of this experiment. Please refer to the earlier 'mining' break-out box for further discussion on this point.

ALGORAND⁸³ – A better way?

Published in October 2016, Algorand presents an alternative integrity method to proof-of-work/mining for publicly distributed ledgers. Instead of competing to solve a cryptographic puzzle for monetary reward, Algorand uses a process called cryptographic sortation to select an ever-changing committee, like a jury randomly elected from amongst all of the users, which then verifies and votes on the next block. Given that sortation produces a random selection of individuals to be involved in the process, there are not the issues with the concentration of power being seen in the Bitcoin mining pools. This process requires negligible computational power and generates a transaction history that will not fork.⁸⁴

Given the early stage of development that blockchain finds itself in, it is highly plausible that competing, or even better, methods for generating integrity in distributed ledgers could be designed and implemented in the short to medium term.

3.2.4 FRAUD

Blockchains may provide value as a fraud resistant and tamper evident record.

Blockchains are clearly fraud controls⁸⁵, because of the inability to alter their transaction records and inbuilt transaction validation processes. Currently the most common method of concealing fraud is by creating and altering physical documents.⁸⁶ Active fraud detection methods correlate with lower median losses and durations, and quicker detection times for fraud schemes.⁸⁷ Consequently, blockchains provide unalterable and readily accessible distributed ledgers that can be used for transaction validation preventing fraud and providing forensic documents for detecting it.

The vast majority of economic crime in the Australian public sector falls into five categories: asset misappropriation, procurement fraud, bribery and corruption, cybercrime, and accounting fraud.⁸⁸ Distributed ledgers could be used to manage document creation and alteration, as well as provide integrity, accountability and auditability for transactions in order to provide active surveillance and counter-measures to all of these five economic crimes.

Mining, wholesale trade, banking and finance, government and public administration (particularly Federal Government), and manufacturing industries present the largest targets for fraud, in that order.⁸⁹ Although small and medium enterprises do not necessarily present the same scale of fraud, because they implement significantly less fraud controls, they are often left extremely vulnerable to significant and material damages.⁹⁰ In descending order, fraud schemes tend to originate in accounting departments, operations, sales, executive/upper management, customer service, purchasing, and finance.⁹¹ Clearly the implementation of a distributed ledger enabled automated compliance solution would reduce auditing and compliance costs as well as provide opportunities for continuous audit, AML/CTF and know your customer (KYC) verification, and automated tax filing.⁹²

83 Micali, 2016

84 Ibid

85 Association of Certified Fraud Examiners, 2014

86 Association of Certified Fraud Examiners, 2016

87 Ibid

88 PricewaterhouseCoopers, 2016

89 Association of Certified Fraud Examiners, 2016

90 Ibid

91 Association of Certified Fraud Examiners, 2016

92 World Economic Forum, 2016

Fraud is an underreported crime. In 40% of disclosed cases⁹³, victim organisations do not refer the fraud to law enforcement due to fears of bad publicity, or a desire to avoid fines (in heavily regulated environments).

Whilst there is disagreement about how disruptive the impact of automation will be on the workforce, it is agreed that all types of work and employment will be touched, although to differing degrees. Disaffected workers will be obvious candidates for fraud risks, particularly in industries heavily, and unexpectedly, disrupted by automation. Long-term wage freezes, or slow growth compared to cost of living increases, could also present fraud risks if automation fuels inequality.

Expanded globalisation, facilitated by automation and emerging technologies including distributed ledgers, could increase interactions between cultures that have not yet negotiated customary or social norms. 'Facilitation payments', and other costs of doing business with certain countries and cultures, present fraud risks to organisations and individuals subject to global regulatory regimes that are becoming ever more sophisticated and cross-jurisdictional.^{94 95}

Fraud control example

The UK government's Department for Work and Pensions (DWP), working with Govcoin, have deployed a blockchain enabled welfare payments system as a fraud control tool.⁹⁶ The DWP provides roughly £166 billion in welfare support per year, of which about £3.5 billion is erroneously overpaid because of fraud (£1.2 billion), claimant error (£1.5 billion) and official error (£0.7 billion).⁹⁷ Less than one third of these overpayments, however, are recovered. There are projections that overpayments could trend towards £5 billion per year.⁹⁸

3.2.5 PROBLEMS OF PERMANENCE AND PERSISTENCE

Persistent ledgers could present problems, such as for privacy and perpetual agreements.

As previously mentioned, the finality of the transactions in blockchains, and potentially in other emerging distributed ledgers, means that situations may arise where information is recorded inappropriately or illegally, and cannot be removed. The permanence and persistence of distributed ledgers present challenges and risks that are novel in information systems.

The potential impacts of the permanence and persistence of this information could be seriously detrimental to the privacy of individuals, which could impact their dignity, and even disempower them. These potential privacy challenges would require good designs and good governance in order to be prevented, and managed. Without these controls, unintended consequences, such as with the use and collection of metadata, may occur with serious ramifications for privacy. Governance models for public blockchains have been demonstrated to be problematic. Regulators with carriage and oversight of privacy and information security would need to consider the potential for breaches where previous responses and mitigations are no longer effective.

Commercial arrangements where private ledgers are established and distributed amongst a consortia are already starting to occur, particularly in the banking and finance sector. The governance arrangements amongst the participating entities here would be expected to be robust and thorough. If one of the entities were to leave the consortia they would be expected to be provided with a copy of the ledger for compliance and regulatory purposes. The problem with the permanence and persistence of these ledgers, however, is that the termination clauses for these agreements may have to remain in effect, potentially in perpetuity.

93 Association of Certified Fraud Examiners, 2016

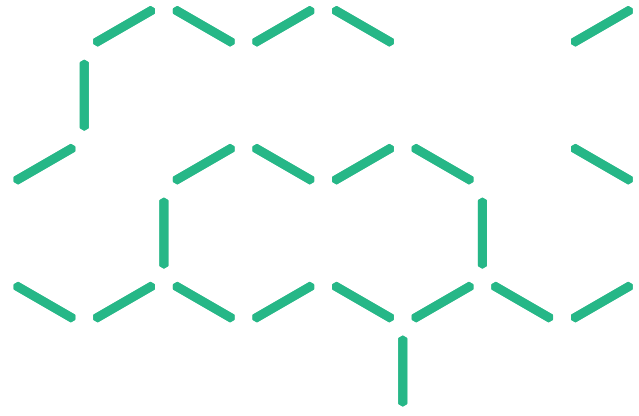
94 The United States of America's Foreign Corrupt Practices Act of 1977 (FCPA) declares the bribery of foreign officials illegal and applies to any person who has a certain degree of connection to the United States and engages in foreign corrupt practices.

95 AUSTRAC's Fintel Alliance: Innovation Hub

96 UK Government Chief Scientific Adviser, 2016

97 Ibid

98 Ibid



Members who exit a consortia would have access to the transaction data of the other members, and vice versa. Unless there is an enduring agreement covering the use of this data, and sufficient compliance controls are in place, there could be significant post-termination issues where the data could be leveraged and/or disclosed. Data held offline could be subject to decryption. Regulators would need to consider amending their guidance and regulations for these situations.

3.3 Design trade-offs

Blockchains offer a trade-off between integrity and efficiency.

The Bitcoin network's design limitations make it unlikely to ever compete with global commercial banking and finance systems. As the demand for Bitcoin transactions has increased, delays have become more common. Fuelled by its own popularity Bitcoin's distributed ledger continues growing at a linear rate (currently standing at 110GB).⁹⁹ The sheer size of this file may eventually become unmanageable, eclipsing the capabilities of the network that originally supported its emergence.

Different types of ledgers may present solutions to the challenges of transaction speed and storage. Categorising ledgers as identity, content or transaction ledgers, which work together, may provide a useful method to throttle their volume versus frequency; with content ledgers storing more data but adding transactions less often than a transaction ledger; and identity ledgers acting more like an oracle and being read and analysed more often than having transactions added.

Although Bitcoin's method will not scale to compete with the performance of the international credit card system, the required performance depends on the respective use case. A risk assessment should be conducted on the future performance of a new blockchain system.

In Bitcoin, the fact that all market actors are able to interrogate and be assured of all transactions is important for their continued faith in the value of the digital currency. Their incentive to participate in the integrity processes is bound to their desire to maintain this value. In other use cases where global consistency is not a concern to all actors in the market there may not be a need to maintain a complete local copy of the ledger. The increasing popularity of Bitcoin has seen a rapid increase in the size of its ledger.

This rate of increase in the ledger may force users to not inspect it as the size becomes too much for their storage. The Bitcoin ledger contains a relatively small amount of transaction detail around the change of ownership of the digital currency. Consequently, it is necessary to consider the size and rate of the transactions involved, the network capabilities and performance required for any given distributed ledger system. Too much content stored on the ledger at too fast a rate and the system may be unusable for certain users.

As with any software system, there are several trade-offs and design decisions that improve the performance of one aspect of a system at the expense of another. Some examples include:¹⁰⁰

- Encrypting data before storing it on a distributed ledger may increase confidentiality, but would reduce performance, and may harm transparency or independent auditability.
- Storing only a hash of data on the ledger and keeping the contents off the ledger would improve confidentiality and may improve performance, but partly undermines the distinctive benefit of distributed ledgers in providing distributed trust. This may create a single point of failure, reducing system availability and reliability.
- Using a private instead of a public ledger may allow greater control over the admittance of processing nodes and transactions into the system, but will also increase barriers to entry for participation and thus partly reduce some of the benefit of using a distributed ledger.
- Blockchains that use Nakamoto consensus, such as Bitcoin or Ethereum, require waiting for a large number of confirmation blocks in order to increase confidence in the integrity and durability of transactions, but this often increases latency and may impact service availability.

⁹⁹ Blockchain.info, 2017

¹⁰⁰ Staples & Zhu, 2017

3.4 Next steps



Considering the state of innovation and the significant investment in distributed ledgers, change will be a constant in the short to medium term. This report has explored the human, procedural and technology factors related to this emerging technology. This exploration, especially given the expected rate of change and innovation, is far from over. The remainder of this report will explore plausible future situations resulting from key uncertainties in technological developments, user adoption and regulatory support. The private and public sectors would benefit, however, from further research into the following areas:

- **Privacy Implications**
Guidelines, training, regulations and other mechanisms may be necessary, as part of a framework to ensure unacceptable privacy breaches from the misapplication of distributed ledgers are prevented. Conducting risk assessments on emerging use cases would provide an analysis of the current gaps needing to be filled.
- **Digital Currencies**
If a foreign jurisdiction were to establish a fiat digital currency, this may influence other jurisdictions to follow suit. Several jurisdictions have, and are, examining the potential for a digital currency. The benefits, risks and uses are not clearly understood at this time.
- **Economic Modelling**
As 'sunrise' industries, or new business models emerge, there may be uncertainty over the viability and impact of their presence. Economic modelling would provide advice to regulators and industry on the sustainability and potential for new opportunities.
- **IoT Security**
As the number of devices rapidly grows, and these devices are being installed into critical infrastructure and everyday equipment, they will become part of the foundation for our society. In researching IoT security, by extension we are protecting our society. Distributed ledgers potentially have a significant role in this.
- **Intellectual Property (IP) Management**
IP management presents a significant economic opportunity for Australia's future. Research into effective platforms that manage the provenance and integrity of IP may unlock significant economic activity and new business models.
- **Digital Identities**
More sophisticated methods for enabling transactions would assist in facilitating the digital immersion of the economy. Digital identity management presents the benefits of bolstering trust and certainty for economic activity, but poses challenges in terms of privacy and security. Research into policy and technology options would inform regulators and industry of ways to balance the related risks and rewards. Significant digital infrastructure enabling digital identity management could be considered a national asset, and a competitive advantage.

4 OUR FUTURE WORLD

This report has been informed by CSIRO’s megatrends research¹⁰¹, which provides an assessment of a future with increasing natural resource scarcity, pressures on biodiversity and the global climate, a changing world economy, an aging population with escalating healthcare costs, the rise of the digital economy, and shifting styles of engagement with consumers, societies and individuals. Our most recent megatrend is the ‘innovation imperative’ for developed countries who face negative consequences if they fail to increase their rates of innovation. As discussed, distributed ledgers present significant innovation opportunities for productivity gains.



Table 1: List of the megatrends

MEGATREND ¹⁰²	FOR THIS MEGA TREND, A DISTRIBUTED LEDGER COULD PROVIDE:
 <p>More from less</p> <p>Innovation will be required to meet human needs by more efficient use of mineral, water, energy and food resources in light of escalating demand and constrained supply. Climate change and land use patterns will place pressure on water and food production systems, while mineral and petroleum resources will be deeper and harder to access. At the same time population growth and income growth are placing upward pressure on demand for these resources.</p>	<p>New ways to record agreed facts that can be used as trusted information sources, or oracles, to more effectively and equitably manage resources, and disputes.</p>
 <p>Planetary pushback</p> <p>Changes in earth systems from the global to microbial will create challenges for humanity. At the microbial scale, widespread, excessive and incorrect use of antibiotics is associated with an increasing number of resistant strains of bacteria, posing a serious threat to human health. At the regional scale, agricultural production systems are challenged by herbicide and pesticide resistant pests and diseases. At the global scale, greenhouse gas emissions are changing climate systems, raising temperatures and resulting in more frequent extreme weather. More positively, governments, companies and societies are doing more than ever before to combat these challenges.</p>	<p>Monitoring of the sources of outbreaks of pests, or animal and plant diseases, and managing their fallout by the ability to track and trace consignments, and the movements plants and animals, would be possible with much greater accuracy and granularity. Border surveillance and protection would be greatly enhanced and more proactive, especially by leveraging the IoT.</p>

101 Hajkowicz et al, 2012

102 Diamond, 2005

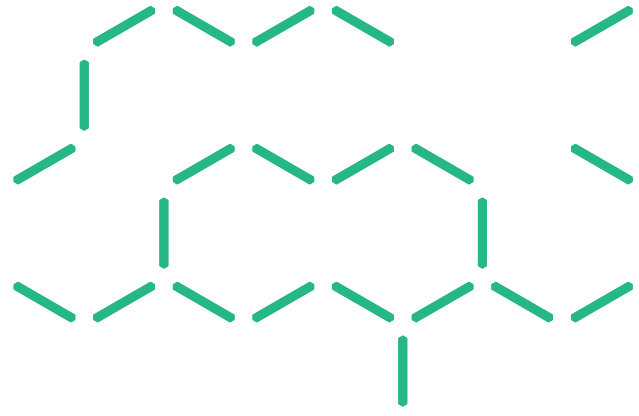
Table 1: List of the megatrends continued

MEGATREND ¹⁰³	FOR THIS MEGA TREND, A DISTRIBUTED LEDGER COULD PROVIDE:
 <p>The silk highway</p> <p>The world economy will continue to shift from west to east and north to south.</p> <p>The rapid growth of emerging economies will see billions of people transition out of poverty and into the middle income classes. With China and India becoming the new economic powerhouses, new export markets, trade relations, business models and cultural ties will be developed for Australia. Rapidly growing Asian economies are transitioning from industrialisation phases into advanced service economies demanding education, healthcare, entertainment, tourism and financial services.</p>	<p>Opportunities to generate systems that provide high integrity provenance solutions for highly valued Australian goods, and at the same time reduce friction, counterparty risk and fraud in supply chains servicing this growing market.</p>
 <p>Forever young</p> <p>The aging population will be an asset, providing a wealth of skills, knowledge, wisdom and mentorship. However this will also present challenges, such as a widening retirement savings gap and rapidly escalating healthcare expenditure.</p> <p>This will change people's lifestyles, the services they demand and the structure of the labour force. People will likely retire later in life, gradually wind back and change duties in a tapered model of retirement and spend increasingly large sums of money through the healthcare system to combat age-related illnesses.</p>	<p>Opportunities to create new anti-fraud safe guards. There are three components to the fraud triangle, which is used to explain why fraud is committed. They are pressure, opportunity and rationalisation.¹⁰⁴ The forever young megatrend presents a landscape in which the pressure to commit fraud may be increased.</p> <p>The aging demographic – also known as the silver economy¹⁰⁵ – would plausibly generate pressures on a shrinking Australian tax-base due to longer lifespans, increasing health and aged-care demands, and their political capital to influence their benefits. This pressure to commit fraud would plausibly be exerted upon the elderly in economic distress, those who care for them, and the generation behind them who perceive their career opportunities and entitlements as limited in this environment.</p> <p>The medical and aged-care equipment connected to the internet (IoT), would plausibly be secured by distributed ledger systems. These devices would also be able to provide aggregated and anonymised patient data, or 'population surveillance', that would be used to deliver customised medicine and better patient care, and forecast infrastructure requirements and service design.</p> <p>Distributed ledgers would plausibly have significant potential to improve the efficiency and accuracy of patient data across increasing numbers of healthcare providers. Although privacy requirements remain an issue.</p>

103 Hajkowicz et al, 2012

104 Cressey, 1973

105 Standards Australia, 2017



Digital immersion

The world will continue to be increasingly connected. People, businesses and governments are increasingly moving into the virtual world to deliver and access services, obtain information, perform transactions, shop, work and interact with each other. The rapid growth in connectivity will change organisational and individual behaviour, reducing the level of in-person interactions. Exponential growth in computing power, device connectivity, data volumes, internet users, artificial intelligence and technological capabilities will transform the way we live.

Safety and security in a digitally immersed world, which requires trusted systems, identities and transactions. Distributed ledgers present the potential to address these issues and transform the internet of things into an internet of trust.

In an environment with massive data volumes, it is worth noting, however, that distributed ledgers may not be suitable for Big Data solutions.

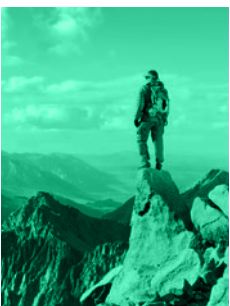


Porous boundaries

Digital technology transformation combined with globalisation will reshape organisational designs, governance systems and employment models. This will continue to break down traditional boundaries around countries, regions, companies, governments and professional fields. New horizontal networks are being constructed leading to a much more agile and flexible landscape for these segments. The peer-to-peer economy is set to bypass many of the traditional intermediaries in banking and finance, retail, tourism, transport, knowledge work and many other industries. Successful models hinge upon intelligent connectivity within rapidly evolving networks.

Records of when you worked, who you worked for, and being able to track and trace the intellectual property you created, or added value to, would greatly empower new ways of working and new business models.

Distributed ledgers may be particularly suited to projects being carried out across networks of individuals and companies, as opposed to the traditional single organisation model.



Great expectations

As populations grow wealthier, demand will rise for services and experiences over products. People will have an increasing expectation for personalised services that meet their unique needs and wants whilst being delivered en masse. While wealthy people have great expectations, the billions of poor people in the world continue to have basic expectations – a gap that will be a priority for the international community to close in the coming decades.

High integrity identity systems coupled with transparent and accurate transaction ledgers that give citizens and governments greater certainty over entitlements, benefits, and taxation.



5 SCENARIOS

The strategic foresight process gathers inputs through research and scanning, analyses what appears to be emerging, interprets why this is the case and then suggests what may happen next in order to provide context that expands the perception of strategic options to decision makers. Consequently this process is intended to inform strategy and strategic planning.

The outputs of the strategic foresight process includes scenarios. Strategic foresight is a process that imagines ‘what if?’ and illustrates these questions through scenarios that present the decision maker with an engaging image of the future. These plausible futures are designed to present questions in the forms of opportunities, risks, and implications for their consideration.

Scenarios are a tool for arranging arguments for alternative future environments that will be influenced by decisions made today. They are evidence-based stories about the future with implications for present-day decision making. This report uses this tool to examine the intersection of trends in technology, behaviour and the regulatory environment. We do this in order to both identify potential blind spots, and to challenge assumptions and orthodoxies, so as to identify emerging opportunities and risks.

The perception of opportunities and risks influences our capacity to navigate them. Opportunities and risks may not be anticipated before they arrive, and they may not be perceived when they do. If they are perceived they may not be addressed, or if they are, these efforts to mitigate the impact may not succeed.¹⁰⁷ Scenarios are designed in order to provide the reader with a perspective on plausible opportunities and risks, with some consideration of how to address them.

A use case is a description of how an actor, such as a human, interacts with an information system in order to achieve a goal. In this strategic foresight study, ‘use cases’ are the focal points of these scenarios.

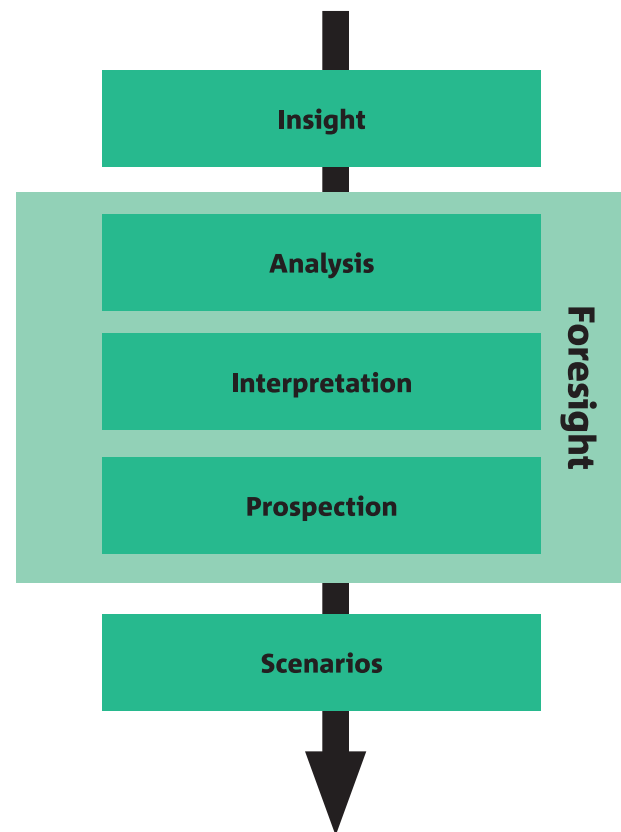


Figure 5: The Generic Foresight Process

Source: Adapted from Voros, 2003

107 Diamond, 2005

5.1 Scenario summaries

Scenarios were famously utilised by Shell in the 1970s to create a competitive advantage in the face of a disruptive oil shock. The four scenarios in this report follow the four archetypal categories of aspiration, transformation, new equilibrium and collapse. None of these scenarios, or the events described within them, are suggested as being more likely than the other, nor are the events from only one scenario likely to materialise; reality is rarely this simple. The time horizon for these scenarios is 2030 for illustrative purposes only, and is not a prediction of when actual events may occur.

Below are summaries of the scenarios and the key questions they raise:

REGULATION ON RAILS, ASPIRATIONAL SCENARIO

In this scenario we imagine a future where governments and the public sector have recognised the risks and potential of emerging technologies and provided leadership by embracing a cohesive regulatory regime that supports and leverages them. Distributed ledgers are employed to increase trust in government activities through identity management, fraud control, programmable money/ transactions (smart contracts), and regtech. High levels of regulatory support and regulatory automation, private and public sector adoption and technological innovation and development have led to significant improvements in productivity, with the Australian economy riding the Distributed Ledger Express on a track towards emerging and sunrise industries, including additive manufacturing and digital intellectual property.

Key questions:

- How should government deliver services in 2030?
- How should the government and public sector keep itself aware of emerging technologies, such as blockchain, and conduct the research and development to build the skills, policy, and technology required to deliver the services society will demand, and drive growth?

THE SHERIFF ON THE DIGITAL SUPERHIGHWAY, TRANSFORMATIONAL SCENARIO

In this scenario we imagine a future where industry adopts a leadership role in the adoption of the IoT and distributed ledger technology. The IoT has continued on its projected exponential growth curve and is in part responsible for a similar growth in the amount of data being generated. Industry standards and distributed ledger technologies are used to manage the cyber security and data provenance problem created by the intersection of these two growth trends. In order to create an internet of trust, which could be harnessed to increase productivity, there needs to be a sheriff on this frontier, and distributed ledgers have been deputised.

Key questions:

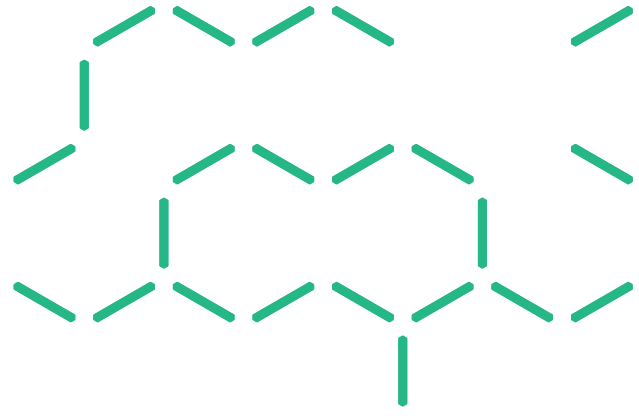
- How could Distributed Ledger Technologies help provide safety and security for our data-driven future?
- How should the private sector generate trust for the digital transactions and economic activity of the future?
- How should the private sector maximise the potential of the IoT?

A BUMPY RIDE, NEW EQUILIBRIUM SCENARIO

In this scenario we imagine a future where the actions of the market are unregulated and there is no leadership or industry guidelines or standards. Blockchains and other distributed ledger technologies proliferate, and compete with each other and more traditional financial products that enjoy a renaissance. The lack of standards and regulation leaves the public with a sense of uncertainty in the quality, longevity and credibility of these products. Whilst technological innovation improves, a lack of regulatory support and a lack of trust from users and industry (who are wary of a technology with a trail of pot holes in its recent past) means the pathway to the productivity potential of this technology is not smooth.

Key questions:

- How may the market behave if left to its own devices?
- How may public and private sector organisations provide leadership and direction to the market in order to minimise risk and optimise rewards? Particularly where innovation occurs offshore and Australia is in a position where it would need to accelerate research and development in order to remain competitive.



A SLIPPERY SLOPE, COLLAPSE SCENARIO

In this scenario we imagine a future where the worst outcomes that could occur, have occurred. The intention is for decision and policy makers, and any other relevant stakeholders to consider why these events may occur and consequently, how to prepare for, prevent, respond to and/or recover from them. This process is known as a pre-mortem. The failures in this scenario stem from the combination of technological and regulatory issues that have led to an abandonment of the blockchain brand.

Scenarios were famously utilised by Shell in the 1970s to create a competitive advantage in the face of a disruptive oil shock.

Key questions:

- Why may institutions and users become averse to the use of Distributed Ledger Technology?
- How should the public and private sector ensure the relevant engagement and interaction of professionals and practitioners, from the various domains involved, in order to avoid the failures outlined in this scenario, and discover the ones that are not?
- How should both sectors provide certainty to investors and innovators operating new technologies and business models?

Table 2: List of the scenarios

SCENARIO	TECHNOLOGICAL DEVELOPMENT	USER ADOPTION	REGULATORY ENVIRONMENT
Regulation on rails	▲	▲	▲
The sheriff on the digital superhighway	▲	▲	◀▶
A bumpy ride	▲	◀▶	◀▶
A slippery slope	▼	▼	▼

Legend: Positive outcome ▲ Neutral outcome ▶ Negative outcome ▼

5.2 Aspirational scenario: Regulation on rails

DRIVERS FOR CHANGE	TECHNOLOGICAL DEVELOPMENT	USER ADOPTION	REGULATORY ENVIRONMENT
Direction of change	▲	▲	▲
‘Any sufficiently advanced technology is indistinguishable from magic.’ ¹⁰⁸			
KEY QUESTION:			
How should government deliver services in 2030?			
In this scenario, we imagine a future Australia where distributed ledgers have been recognised by government as an essential service for society. User adoption has also increased exponentially, supported by this proactive position taken by government. Digital Currencies, The IoT, Fraud Control, ‘Smart Contracts’, and Regtech are use cases that drive this growth.			

THE WORLD OF 2030

In this future, Australian governments and public sectors identify that software impacts on the entire spectrum of society, the economy and governmental activities.¹⁰⁹ They also recognise that the IoT’s benefits depend to a large extent on their capacity to create adequate regulatory frameworks in areas including security, privacy and consumer policy.¹¹⁰ This best case scenario is a world where the public find online government services safe, secure and seamless.

Collectively they have aspired to embrace technology in order to optimise their operations, governance, and service delivery. Distributed ledgers are a crucial part of a larger toolkit of emerging technologies that have been harnessed for better performance, and positive externalities to society and the environment.

Fraud is a factor in any future. Manual auditing processes do not scale, especially for complex systems. Compliance costs today are considered to be in the order of \$AUD250 billion¹¹¹, and regulation costs are estimated at \$AUD190 billion¹¹², with both projected to climb.¹¹³

Currently more than one million Australians are employed in compliance roles. Fraud is generally hard to detect and prosecute, however it is especially hard when you are unable to determine when decisions and actions occurred, or even who actually undertook them. Distributed ledgers could remove this uncertainty and create evidentiary records that deter fraud and corruption.

Harnessing the political will and foresight to exploit the opportunities of emerging technology, safeguard the country and communities against risks, government services are created that appear magical, and create significant trust compared to previous processes. Australia becomes a jurisdiction of choice for business. Corporate Australia takes notice and adopts these innovations in the private and community sectors, increasing productivity and decreasing fraud through automated compliance.

Corruption increases transaction costs and uncertainty.¹¹⁴ Some of these costs are due to the requirement for additional monitoring and enforcement.¹¹⁵ High levels of corruption, and related uncertainty, may also stifle entrepreneurship and innovation.¹¹⁶ Perceptions of corruption are correlated with GDP, indicating that those countries in which people perceive government to be more trustworthy have better performing economies. The enhanced transparency and certainty offered by digital ledgers may lower corruption. While this would be most beneficial in countries where corruption is high to begin with, it could improve trust everywhere, so in this scenario Australia’s Corruption Perception Index score would rise.

¹⁰⁸ Arthur C Clarke

¹⁰⁹ Rice, 2007

¹¹⁰ OECD, 2015

¹¹¹ Deloitte Centre for the Edge, 2015

¹¹² Ibid

¹¹³ In the United States of America, these figures are in USD trillions.

¹¹⁴ OECD, 2016

¹¹⁵ Ibid

¹¹⁶ Ibid

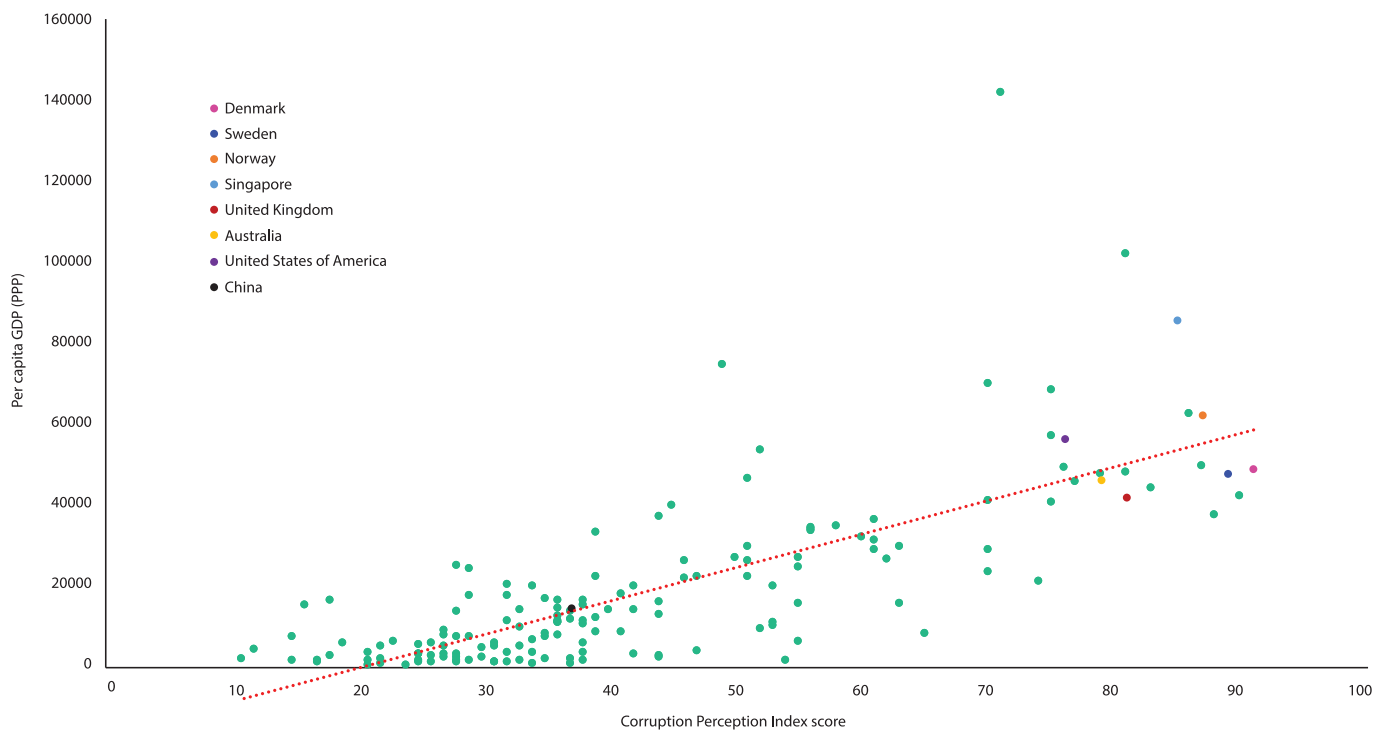
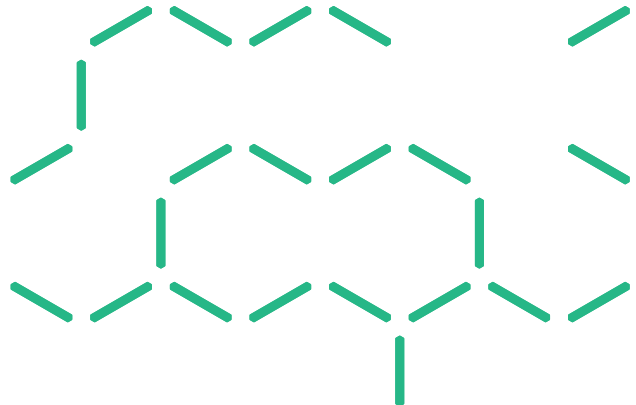


Figure 6: The positive correlation of trust in the government and GDP

Sources: Transparency International, 2015, and World Bank, 2015.

A NEW ECONOMY

Globally manufacturing-bases are declining, in part due to automation, and are shifting towards jurisdictions with lower wages, as they have been for decades. The recent innovation rates of additive manufacturing (3D printing) offer significant benefits to Australia. Logistics is an expensive cost of both doing business and living in a geographically dispersed country like Australia. Being able to print inventory on-demand significantly alters supply chains and increases competition, and the country's competitive position. This would see Australia take a similar shift to what has been seen in China, where the focus is now on having products that are, 'created in China' (or designed) over, 'made in China'.¹¹⁷

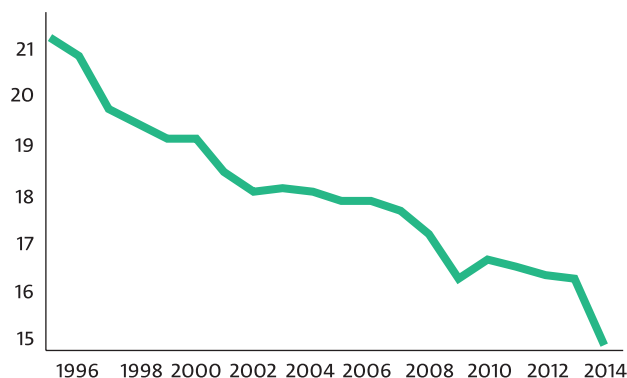



Figure 7: Manufacturing, value added (% of GDP)

Sources: World Bank national accounts data, and OECD National Accounts data files.

In this environment, the creation and protection of digitised intellectual property becomes fundamental to the sustainability of existing and emerging industries, and for the country's economic prosperity. Could design replace manufacturing as an employment base? Appropriate regulation and digital regulatory controls are also necessary for the oversight and management of prohibited and controlled items. Distributed ledger enabled systems provide an opportunity to manage and regulate the identity, digital content and transactions involved in the trading and exchange of intellectual property. The management of intellectual property may become a capability of national importance in this future world. Placing IP management at the centre of public policy is seen by some as a critical enabler for both attracting IP intensive industries and building capacity for innovation.¹¹⁸ Intellectual property fraud and theft may become our largest economic threat. Government initiated Regtech platforms could assist Australia transition to this new economy.¹¹⁹



Government-initiated Regtech platforms could assist Australia transition to this new economy.

A DAY IN THE LIFE OF 2030 – REGULATION ON RAILS

Jane climbs into her driverless car and reclines. It has been a busy day, and she is thankful for the short break the trip will give her, much like when she used to catch the train. As Jane relaxes she is briefly grateful for the government's cyber security and safety standards that have made driving safer than walking. 'It is amazing that we used to accept road accidents as usual, especially considering that more than 95% of crashes were caused by human error,' Jane thinks as the thousands of IoT devices managing her trip, entertainment, comfort, and safety carry on without missing a beat.

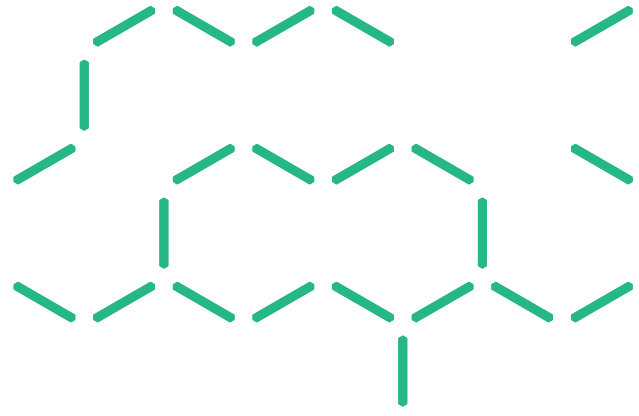
Jane activates the user interface on her augmented reality glasses and brings up the government's service delivery portal. Her board has just approved a proposal to establish a spin-off project, and it needs to be registered. The proposal is a licence and credential authentication service that uses facial recognition and biometric identification to match an individual to their database of qualifications, certifications, licences and credentials. It does this by using a distributed ledger that keeps the identification secure. Jane hopes their product will be used by consumers interacting with tradespeople and professionals, citizens interacting with authorities and hopefully by driverless cars autonomously interacting with mechanics, law enforcement and passengers.

The user interface verifies Jane's identity and assists her in completing the registration of the new business. It does this by listening to Jane's proposal and presenting her with all, and only, the relevant legislative and regulatory requirements that need to be complied with. Recognising that the business will be selling a technology product, the interface prompts Jane to provide the details of the board for the new business in order to ensure they have the appropriate technology governance qualifications. Once checked against the universal education transcript ledger the interface then prompts Jane for assurance on the quality of the code.

¹¹⁸ Davidson & Potts, 2016

¹¹⁹ Regorous

Data61 is developing Regorous to provide a solution to the often complex, tedious, and inefficient processes of manual regulatory compliance. Regorous is built using Defeasible Deontic Logic technology, which maps rules, regulations, and business processes into equations, allowing for automated regulatory compliance checking and reporting. For instance, the PermitME application – an 'automatic concierge' designed for new businesses – automatically assesses a user's business proposal against the legislative requirements, and prompts the user to provide the relevant information to the correct authorities at the right time. Existing businesses can also have their compliance checked automatically by Regorous. Finally, the technology allows users to write new legislation in the 'logic language' of Regorous, as well as translating existing contracts and legislation into machine-readable logic. The automatic processes enable greater speed and assurance of compliance, while offering the potential to reduce the associated costs.



Several systems are available for Jane to choose: a government offered automated code quality tester; a qualification check of the coders; or a distributed ledger backed certification from a qualified code tester. In order to help Jane make her choice, the interface assists Jane in completing a risk assessment for the use cases the product will be registered for.

The risk assessment analyses the insurance, financials for the new business, the context of the particular use case, the distributed ledger's architecture, and the jurisdictions in which it will operate. By being able to immediately verify the insurance, financial and qualifications details, the interface is able to offer the risk assessment and suggest the next courses of action Jane should take in registering the new business.

Although the government's automated code quality tester is certified as not able to copy or read the source code, out of an abundance of caution Jane is careful not to expose their code outside of their sandpit. Jane opts to submit the identity of the accountable coders who have relevant qualifications in the necessary privacy, security and legal aspects of the use cases, and completes the registration

COMMENTARY

In this scenario, the creation of mutual trust in the public and the government enables the provision of automated service delivery. Identity management and fraud control are at the heart of this and are essentially the rails on which the service is run. The activities in this scenario are also facilitated by blockchain enabled academic transcripts and programmable money. Blockchain-enabled academic transcripts are already starting to emerge.^{120 121} Programmable money is a significant, if understated, aspect of this scenario, regardless of the existence of a fiat digital currency. The European Parliament has recognised the positive impact distributed ledgers would have for consumer welfare and economic development and their Committee on Economic and Monetary Affairs has called for regulation to manage the associated risks involved.¹²² The positive regulatory regime in this scenario has enabled a digital transformation of service delivery resulting in red tape reduction, reduced transaction times and cost, and increased regulatory compliance.

Distributed ledgers could be developed to improve government service delivery today. For example medical practitioners and allied health professionals are required to manage multiple digital identities with manual processes for renewal and re-enrolment, which can lead to disruptions in service delivery. Re-enrolment can be triggered by relocations of service delivery as Medicare provide location-based pricing. A suitable distributed ledger system that managed the multiple digital identities of the provider, would greatly reduce related service disruptions. Additionally, if the system could provide assurance of the location of delivery of their services (potentially through blockchain-enabled GPS systems), this would enable significant reductions in related transaction costs.

Key question:

How should the government and public sector keep itself aware of emerging technologies, such as blockchain, and conduct the research and development to build the skills, policy, and technology required to deliver the services society will demand and drive growth?

120 Dodd, 2017

121 University of Nicosia, 2017

122 von Weizsäcker, 2016

LEGAL



By recognising and setting rules for the use of distributed ledgers for the performance of contracts, evidence and recording of transactions, governments have provided certainty to business, the public sector, citizens and law enforcement for the conduct of their activities and have provided powerful tools that reduce costs and improve behaviour.

This use of distributed ledgers, coupled with the automation of regulatory compliance¹²³ has made Australia a jurisdiction of choice for business, with positive improvements to governance and transparency indicators, as well as global market confidence in Australia's economy.

The recognition of the IoT as an essential service has led to the setting of minimum acceptable standards, along a risk-based approach, in order to ensure the safety and well-being of communities. Non-technical regulators have become involved in the setting, review and enforcement of these standards in sectors where misconfiguration or malfeasance now has real-world risks and impacts. Maintaining trusted advice on the creation of these standards for emerging technologies and use cases is a priority on the government's agenda.

INNOVATION



The ability for distributed ledgers to provide anonymised, and aggregated data enables governments to engage in population surveillance in the interests of public health, well-being and economic prosperity without violating privacy, if it is properly designed.

This has enabled health departments to better manage their patients, and future infrastructure requirements based upon data collected from environmental and medical IoT devices, while maintaining their privacy and safety.

Transport and infrastructure departments are able to better predict infrastructure failures, and consequently prioritise preventative maintenance through the analysis of data from their own, and third-party devices, which are trusted thanks to distributed ledgers.

QUALITY

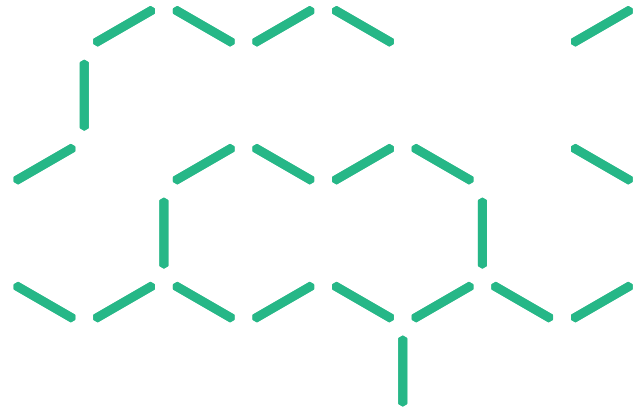


Given the identification of the importance of software, government-mandated standards for code checking have been implemented and incentives and services are offered to ensure sufficient quality.

The standards set contain both technical and managerial requirements and roles. Boards are mandated to obtain relevant qualifications in technology awareness, including associated governance, risk and compliance components. Specific technical products are required to be certified by individuals with relevant qualifications in specific domains, again in a risk-based fashion that started with commerce, finance, and legal areas.

Academic transcripts and licences managed on publicly accessible distributed ledgers have been introduced by the government to improve the transparency and integrity of the education sector, and also to facilitate their requirements in meeting these standards. The tertiary education sector embraces this innovation and uses this infrastructure to offer degrees that are heavily customised by students in order to address emerging industries. Universities focus on core strengths and niche offerings with their subjects and courses being recorded on a universal distributed ledger with students attending multiple institutions.

Instead of relying upon costly proof-of-work methods for this distributed ledger, the academic sector uses a reputation-based system. They leverage their existing reliance on the reputation of their institutions, senior staff and registrars and aggregate this with the identification and reputation of their lecturers, which is all underpinned by a government-led identity platform.



<p>USER ADOPTION</p> 	<p>The literature on the adoption of innovation demonstrates that examples of adoption by trusted entities leads to an uptake in further experimental adoption. In other words, when someone sees someone they trust use something new and it all goes well, they will try it themselves.</p> <p>If distributed ledgers provide the transactional data at a granularity and accuracy that the regulators can use to efficiently and effectively monitor compliance, then the private and community sectors may engage with new regulatory models, or new technology for their own compliance processes.</p>
<p>INTEROPERABILITY</p> 	<p>Cross-border data and information flows are increasingly important to the Australian economy, especially as the global centre of gravity for the middle-class shifts towards Asia. Being able to produce trust and provenance with respect to online interactions and intellectual property would be a competitive advantage.¹²⁴</p>
<p>DIGITAL CURRENCY</p> 	<p>The introduction of programmable digital currencies and financial services platforms underpinned by distributed ledgers provides Australia with several competitive advantages:</p> <ol style="list-style-type: none">1. Protection against the monetary shock of a material wealth transference away from AUD into a disruptively emergent digital currency. There is concern that without government intervention, such a shock could potentially impact Australian monetary supply policy.2. Increased ability to enter a currency union with a significant trading partner, especially if that partner develops a fiat digital currency or financial distributed ledger platform.3. The establishment of an identity platform, potentially distributed ledger based, could also provide compliance with know your customer (KYC), and know your customer's customer (KYCC), an emerging and challenging regulatory position, making significant compliance savings and meeting Anti-Money Laundering and Countering Terrorism Financing (AML/CTF) requirements.4. These systems could also automatically provide taxation and customs revenues without a human invading the privacy of the parties involved in the transaction, especially where IoT devices are able to verify that the corresponding real-world activities are legitimate. This process, however, does not abrogate the requirement to design systems that protect personal information and metadata. Although the use of zero knowledge proofs and other emerging methods, may provide privacy by design.5. The IoT provides an infinitely greater surveillance of the border, especially cargo at the ports and post through the air stream, where a blend of public and private sector assets can be trusted to provide situational awareness for pest, diseases, controlled items, and drugs.¹²⁵

¹²⁴ Standards Australia, 2017

¹²⁵ Hyperspectral Imaging is a different way of collecting photographic information. It is much more powerful than traditional photography, and provides significantly more information about a scene than can be seen with the human eye. Hidden details can be found, and material properties can be discovered. Data61's Scyllarus platform obtains hyperspectral data from standard IoT cameras (such as smartphone cameras) and through the application of Computer Vision and Machine Learning can detect crop disease and find elusive evidence on a crime scene hidden to the naked eye.

5.3 Transformational scenario: The sheriff on the digital superhighway¹²⁶

DRIVERS FOR CHANGE	TECHNOLOGICAL DEVELOPMENT	USER ADOPTION	REGULATORY ENVIRONMENT
Direction of change	▲	▲	◀▶
<p>‘Cybercriminals will change their activity if the IoT becomes the principal centre of value creation in many industrial, economic and government processes.’¹²⁷</p>			
<p>KEY QUESTION:</p> <p>How could Distributed Ledger Technologies help provide safety and security for our data-driven future?</p> <p>In this scenario, we imagine a future Australia where distributed ledgers have become a utility service that is relied upon by society, and is thought of as simply a cost of doing business. User adoption has also increased exponentially, although most users are unaware of the distributed ledgers being used to support their world, which is digital. Regulatory support has been mixed, with industry being the primary driver for standardisation and interoperability. The IoT, international trade, and banking and finance use cases have driven this growth.</p>			

THE WORLD OF 2030

In this future, the private sector has marshalled its resources, networks and connections in order to make distributed ledgers that provide law and order and have transformed how we use the information superhighway. With distributed ledgers acting as trusted oracles for identity, content and transactions, society is empowered to embrace the full potential of technology.

In this future, people will be augmented by technology in all aspects of their lives. In the work tasks they perform, their recreation, the way they relate and communicate with others locally and around the world, and in their health and well-being. The flip-side to this augmentation is their reliance upon this technology for their safety and security when technology is so pervasive, and woven into the very fabric of their day-to-day lives.

The projected increase in the IoT has been realised and sensors, actuators (motors), locks, and all manner of devices are implanted in everyday items, people, and infrastructure to create incredible benefits. The challenge presented by the IoT is that as these devices, and the

software that runs them, are effectively governing the administration of the real world. They have become the law, and their coders are essentially writing the law.¹²⁸ In cyber space, the sole adjudicator is software.¹²⁹ But while the IoT and software are global, the law is not.¹³⁰ Consequently, to ensure that the IoT meets the needs of the community, industry and regulators, it should act as an ‘Internet of Trust’, as trust is fundamental for productivity.¹³¹ Distributed ledgers are used to ensure the integrity of IoT devices, their configurations, and the authenticity of software, and updates. There needs to be a cop on the beat, and in this ‘cloud by default’, globalised-world studded with devices, distributed ledgers have been deputised to deliver trust.

Higher levels of belief in how trustworthy everyone in a country is, is positively correlated with the average per capita GDP. With a growing trend of more IoT devices than people, it would be interesting in the future to analyse the correlation of the perception for the trustworthiness of these devices, in a given jurisdiction/country, against the respective average per capita GDP. Would this also be positively correlated?

¹²⁶ The information superhighway or infobahn was a 1990s term for the internet and was associated with United States Vice-President Al Gore.

¹²⁷ Center for Long-Term Cybersecurity, University of California Berkeley, 2016

¹²⁸ Rice, 2007

¹²⁹ Ibid

¹³⁰ Greverie et al, 2014

¹³¹ OECD, 2015

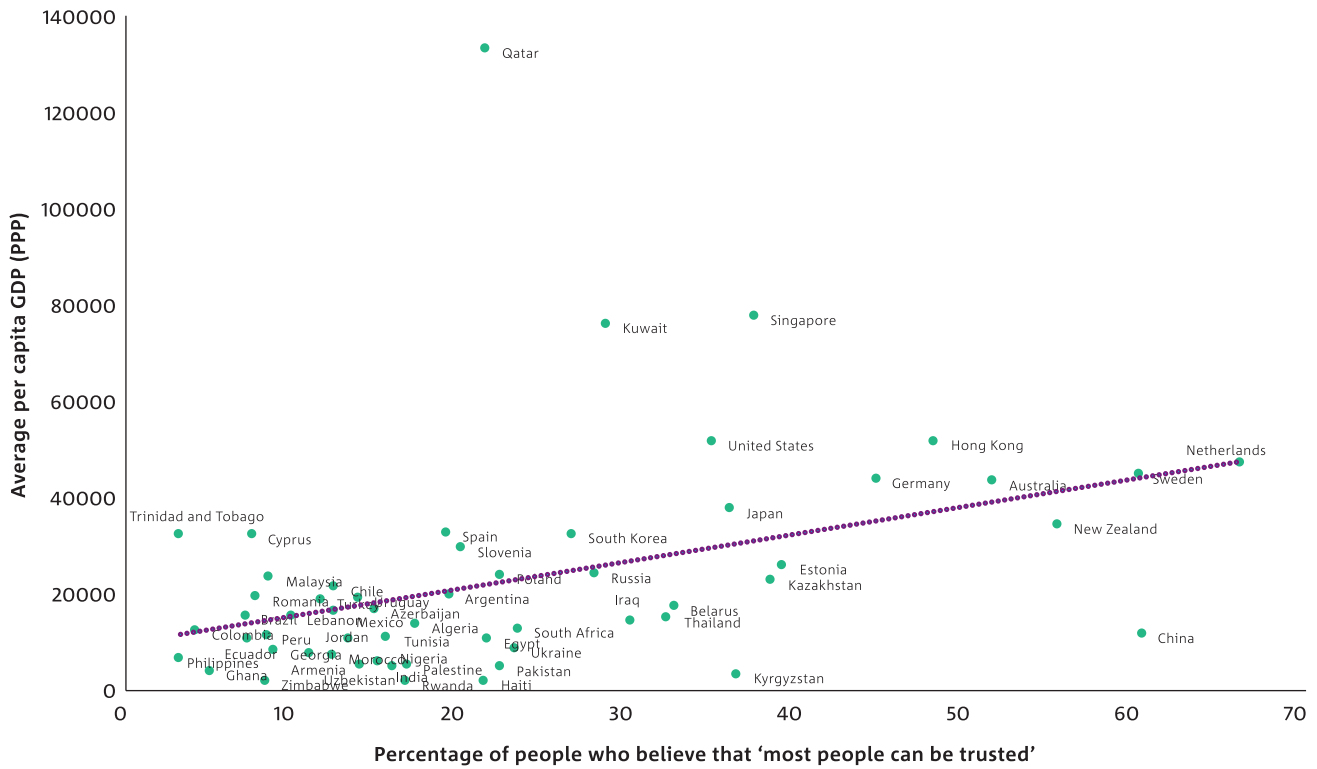
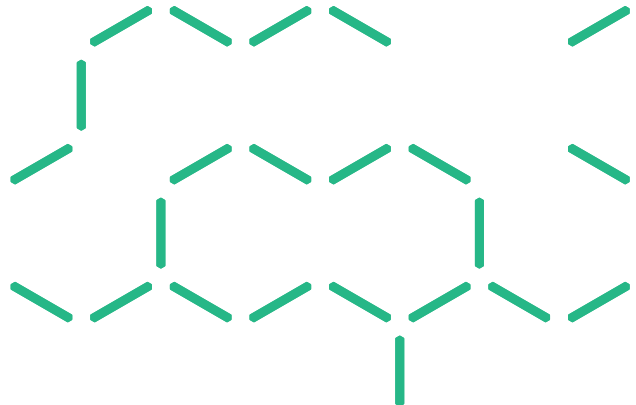


Figure 8: Percentage of people who believe that “most people can be trusted” measured against GDP.

Sources: Trust data from World Value Survey 2010—2014: the percentage of people who believed that ‘most people can be trusted’ GDP data from the World Bank: average per capita GDP (PPP) 2010—2014

THE INTERNET OF TRUST

This projection includes multiple estimates from various sources. The line of best fit describes a commonly witnessed technology adoption curve. It is also common for adoption curves like this to be discounted, as people tend to consider linear projections, consequently becoming surprised by the significant increases. Will there be another order of magnitude increase, or greater, in the number of IoT devices from 2025 to 2030?

IoT Expansion

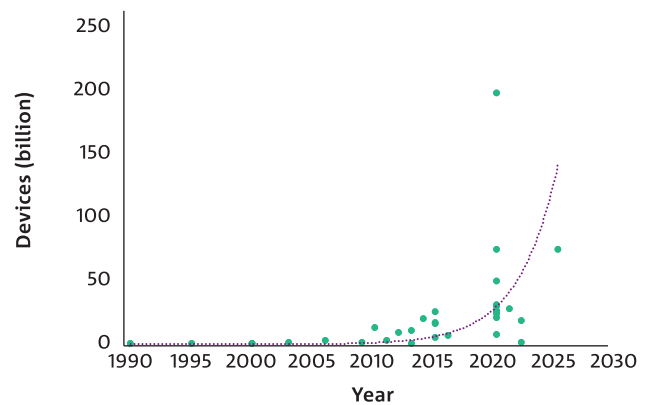


Figure 9: The Internet of Things (IoT Prediction Curve)

Sources: Howard (2015), Proffitt (2013), Evans (2011), Intel (n.d.), Gartner (2013, 2014, 2015), Machina Research (2013), Soderbery (2013), ABI Research (2013), Navigant Research (2013), IDC (2014), Lucero (2016), Cisco (2016), Danova (2013), Lund et al (2014), Business Insider (2016), Ericsson (2011)

Table 3: The emerging scale and value of the IoT

YEAR	2007	2017	2027
Estimated number of connected devices.	560 million	12.32 billion	270 billion
Increased value measured as an increase in the functionality of the network from 2007.			
According to Metcalfe’s Law the value of a network is the square of the number of its nodes (devices).		15,178%	7,290,000%

Sources: Exponential growth estimates using data from Howard (2015), Proffitt (2013), Evans (2011), Intel (n.d.), Gartner (2013, 2014, 2015), Machina Research (2013), Soderbery (2013), ABI Research (2013), Navigant Research (2013), IDC (2014), Lucero (2016), Cisco (2016), Danova (2013), Lund et al (2014), Business Insider (2016), Ericsson (2011)

This rate of adoption for the IoT presents a significant amount of potential value. The challenge to capturing and protecting this value is the necessity to ensure the security of these devices, the safety of their users, and the integrity of the data they capture. Distributed ledgers could provide this by ensuring:

- the integrity of the configuration of devices connected to the internet, and the updates they download and apply,
- the identity of the device — sometimes referred to as know your thing (KYT), or know your device (KYD), and
- the data recorded from multiple sensors are corroborated and stored as a trusted fact.

This impending tsunami of data is threatening to swamp society. The challenge is to create data provenance in a world swimming in data and devices. Distributed ledgers could act as oracles that ensure the integrity of the hardware, software and information.

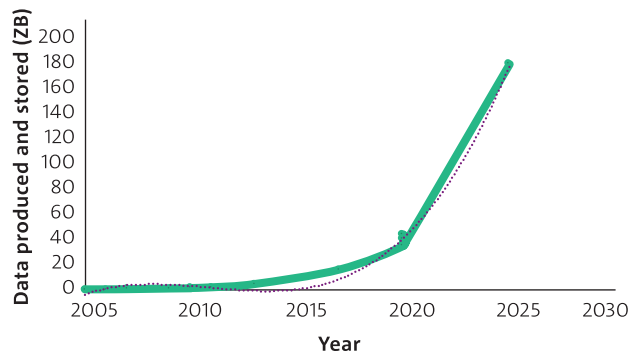
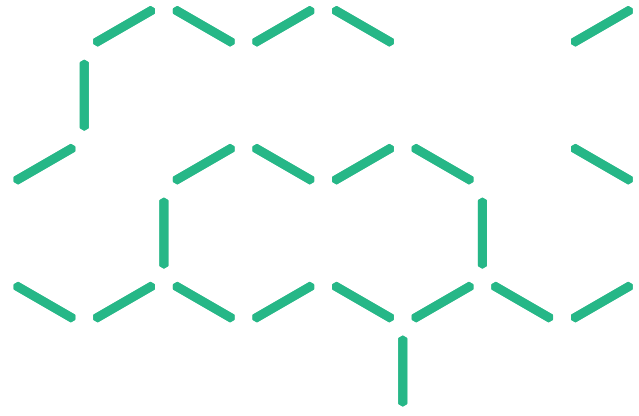


Figure 10: Big data prediction curve

Data source: IDC Digital Universe Study (2007, 2010, 2011, 2012, 2014), IDC Infographic (2011, 2013), Kanellos (2016)

The challenge is to create data provenance in a world swimming in data and devices.



A DAY IN THE LIFE OF 2030 – THE SHERRIFF ON THE DIGITAL SUPERHIGHWAY

Dan was looking forward to his trip. The several hours he would spend in his driverless car, on the way to see his grandkids, would be spent sleeping, catching up on episodes of his favourite shows and managing his investments. His mobility and freedom were certainly increased with both his driverless car and his mobility exo-skeleton. Even if it were legal, Dan would not feel comfortable driving himself anymore. Industry standards for safety and security have enabled interoperability between compliant IoT devices and distributed ledger platforms manage their safety and security by validating configurations and software/firmware/security updates.

Between the IoT devices in his car, on his mobility suit and in his medical implants, his family and medical staff know exactly how he is, and are able to even predict what he needs before he does. Distributed ledgers ensure the security of all of these devices, and ensure that only authenticated and trusted users access his information and settings.

Dan's car is a pool vehicle, shared in a partnership between several retirees. The vehicle's every move is recorded on a distributed ledger that logs where it went, how fast it went and stores sensor data about road conditions and the surrounding traffic. This information is used as a record to ensure the partners adhere to the agreed conditions of use and in case of accident or emergency. The evidentiary nature of the ledger has saved more than one partner from paying for an insurance claim. All these sensors allow the vehicle to verify the service and repair actions taken by mechanics, which is usually preventative maintenance the vehicle has self-diagnosed.

On the drive, Dan's car makes decisions on the most efficient method of recharging based upon pricing signals and recharging points along the way. Dan's car uses programmable money and autonomous contract tools in order to be able to autonomously make purchasing decisions, which it often does as Dan naps. Government taxes and carbon credits are managed automatically via distributed ledger enabled financial and automated compliance platforms with continuous auditing, fraud controls, automated tax-filing and real-time settlement.

During the trip Dan looks in on his investments. Dan is participating in a Decentralised Autonomous Organisation (DAO) that manages the import and export of retail goods. Dan's user interface has a highly sophisticated IoT enabled situational awareness functionality. IoT devices in cargo containers, at ports and with transport and logistics companies all feed trusted real-time data to the distributed ledger enabled oversight system. Dan likes to play with the system and see where the shipments are at, and what conditions the cargo is in. He believes he has found a shortcut via Singapore for several of his supply chains, which provides him with a competitive edge. The system, like several others, plays a significant role in stimulating global trade. Reduced barriers to entry, lowered risk and automated, and trustworthy, insurance schemes have made trade finance an attractive option for retirees, with sufficient capital, who wish to remain active.

Dan is not worried that the regulators have not provided an official position on their view of the DAO he has invested in. He is, however, somewhat cautious about the use of so-called 'smart contracts' given the uncertainty of their standing and quality in certain jurisdictions. Dan trusts the autonomous contract tools made by the company that runs his DAO, however, as he trusts their brand, and has not had a problem with any of his transactions through their verified suppliers and alliance partners.

COMMENTARY

In this scenario the safety and security of the IoT is a fundamental issue — from the smart meters ensuring the safe and secure transfer of energy in exchange for money, to the tracing and tracking of consignments in global supply chains, to the personal automation and medical devices. CSIRO and Energy Networks Australia suggest the development of sound operational practices, including new techniques for the operations of distribution systems will be key for the deployment of Distributed Energy Resources (DER), like those in the scenario.¹³² By 2027 this market could be worth \$AUD1.1 billion per year.¹³³ Innovators will be motivated by this opportunity and blockchain enabled smart meters, and other IoT devices could be part of these systems and practices. Furthermore, peer-to-peer or many-to-many systems lead to the innovation of new DER energy products, which again could be blockchain enabled.

132 CSIRO and Energy Networks Australia, 2017







133 Ibid

Walmart is currently exploring the potential for blockchain to provide food provenance in the wake of many years of costly recalls from around the world. By providing this visibility of the supply chain, it is hoped to reduce the time of the recall action and the significant disruption to the underlying industry.

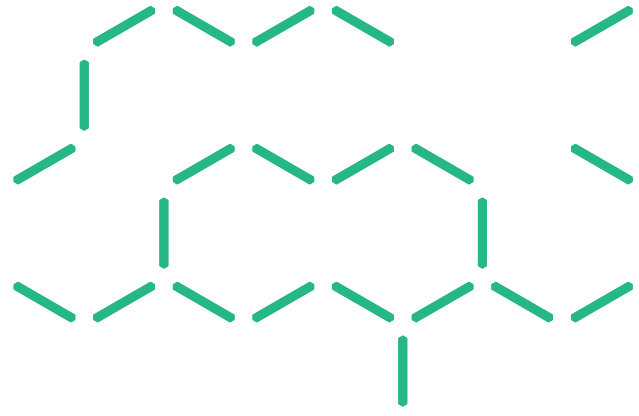
Programmable money, for the driverless vehicle, DAO and supply chains, offers significant utility for the distributed ledgers involved in this scenario, regardless of the existence of a fiat digital currency.

Key questions:

- How should the private sector generate trust for the digital transactions and economic activity of the future?
- How should the private sector maximise the potential of the IoT?

<p>LEGAL</p> 	<p>In order to establish certainty in the marketplace, in the absence of clear direction and leadership from regulators, industry has taken responsibility for establishing codes of conduct, guidelines, and standard terms for transacting. Specifically these address the matter of who is responsible for what in the event of a failure or dispute. Given the potential for multiple technologies, business processes, suppliers and vendors to be involved in any given transaction, it provides comfort to the market that there are clear channels for raising complaints and seeking resolution of disputes.</p>
<p>INNOVATION</p> 	<p>Clearly an industry-accepted security architectural model is required for the emerging IoT phenomenon. Vast amounts of sensor data will be created, and will be required to be processed, analysed and relied upon. Being able to identify where this data came from and also to trust its source is of significant importance. Industry-led data provenance standards¹³⁴ underpin this scenario. Partnerships between industry and academia increased research and development of approaches to distributed ledger innovation.</p>
<p>QUALITY</p> 	<p>Peak bodies and professional membership organisations establish certification and training programs. The barrier to entry is low, but once certified an ongoing requirement for professional education hours keeps practitioners ‘returning to the well’ where industry can refresh them on best practice and update them on opportunities, risks, regulation and technology.</p>
<p>USER ADOPTION</p> 	<p>By leveraging visualisation tools, which have been repurposed from network and audit log analysis, intuitive and powerful user interfaces have been created that enable powerful and insightful analytics to be run on data with high integrity. This step alone brought the power of the distributed ledger to the board room, where info graphics and statistics influence key decision makers.</p>
<p>INTEGRATION</p> 	<p>Research and training on handling commercial confidentiality with distributed ledgers provides the confidence and capability to integrate information exchange across diverse industries, as well as improve supply chain quality, and facilitate the provenance of branded goods.</p>
<p>DIGITAL CURRENCY</p> 	<p>The capability to generate sound financial transaction platforms that meet the integrity requirements of both regulators and users has lowered the barrier to entry, and reduced market asymmetries across the banking and finance sectors.</p>

134 OECD, 2015



5.4 New equilibrium scenario: A bumpy ride

DRIVERS FOR CHANGE	TECHNOLOGICAL DEVELOPMENT	USER ADOPTION	REGULATORY ENVIRONMENT
Direction of change	▲	◀▶	◀▶
<p>'It will be a challenge to let markets figure out how to best use this technology while ensuring consumer safety and efficiency.'¹³⁵</p>			
<p>KEY QUESTION:</p> <p>How may the market behave if left to its own devices?</p> <p>In this scenario, we imagine a future Australia, where the innovative potential of distributed ledgers is being explored in the absence of regulatory guidelines. Speed bumps on the road to innovation produce trust gaps with users who are wary of a technology with a trail of pot holes in its recent past.</p>			

THE WORLD OF 2030

Innovation tends to be valued more highly than security¹³⁶, consequently innovation travels ahead of considerations and lived experiences, with respect to risk and security. Policy, regulation and legislation tend to have long lifecycles and understandably take some time to catch-up to innovative developments. In part this is also because the courts, and generally governments, use the 'mischief rule'. In this approach, their intent is to avoid stifling innovation and the freedoms of the market, and only to impose restrictions when the system has clearly failed to support the principles and values of society.

In this future, regulators have left the market to its own devices with respect to distributed ledgers. Painful lessons have been learned, and trust with users has been eroded, although not entirely lost, due to leaps of faith with the technology that did not perform as advertised.

In any creative period of evolution, many new ideas are born, and Darwinian processes determine the ideas that thrive. As the better-performing ideas survive, there tends to be a die-off of competitors, especially as standardisation occurs. This downturn in the overall number of ideas may lead some to believe that the concept is on the decline, whereas the truth is much different.

One of the areas where this creative energy flows into is existing services and products. In the latter half of the 19th century sailing ships were under competition from the new steam ships. This pressure invoked a renaissance in sailing ships' (long stagnant) design and innovation, with better sails and sleeker hulls. The steam ship was, however, eventually triumphant. This is known as the 'sailing ship effect'.

Where distributed ledgers challenge an established intermediary, or present a better service or product, the incumbent is likely to seek efficiencies and new functionalities in order to be competitive. For example, the New Payments Platform¹³⁷ offers functionality that rivals the peer-to-peer capabilities of digital currencies with the added value of providing a regulatory framework in the event of a dispute, which differs from Bitcoin where you are on your own when you have a problem with your transaction, or wallet. Remittance is a high value and disruptive use case for distributed ledgers. This use case drives a sailing ship effect on the banking and finance industry in this future.

¹³⁵ Koepl & Kronick, 2016

¹³⁶ Rice, 2007

¹³⁷ Australian Payments Clearing Association, 2015

Distributed ledgers are highly likely to cause a sailing ship effect in services and products that involve the requirement for trust, transparency, provenance or verification. Distributed ledgers appear to already be, at least in part, the driver for various banking and finance services being developed and deployed.¹³⁸ Distributed ledgers do not even need to be able to provide a viable offering in order to stimulate investment in sailing-ship-style research and development.

Areas in which distributed ledgers (potentially in concert with other emerging technologies) may cause the sailing ship effect include:

- Banking and finance
 - Remittance
 - Trade finance
 - Core banking services
- Professional Services
 - Accounting
 - Audit
 - Legal
 - Risk management and assurance
- Agribusiness
 - Food provenance
 - Supply chain management
- Intellectual Property
 - Software
 - Copyright
 - Management of IP rights.

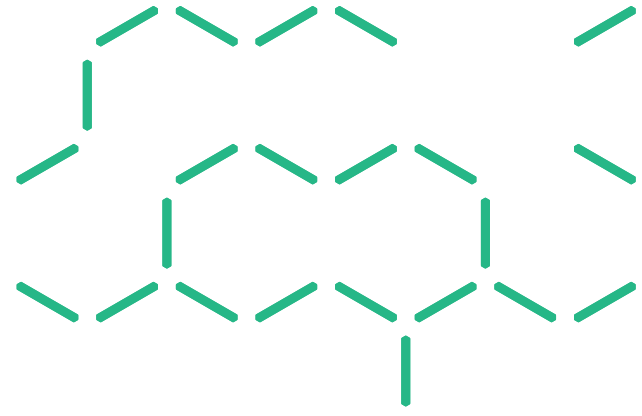
A DAY IN THE LIFE OF 2030 – A BUMPY ROAD

Kaisu is reading the news on her new phone. As a logical extension to the National Broadband Network (NBN), and in acknowledgment of internet access being recognised as a basic human right, Kaisu received a basic hand-set from the government, along with anyone else who asks. The program is called the Universal Basic Telephone (UBT) service (sometimes pronounced ‘you bewt’). Initially these handsets were basic retro-feature phones from the pre-smartphone era, but the internet of things has made anything that basic almost impossible to buy. The government is able to always contact you, and deliver services to you through the phone.

Underpinning the concept of government service delivery via the internet is the task of authenticating the user. Successive state and federal governments had tried to mount identity platforms with the intent of creating efficiencies and economies of scale. The taint of the dark web on Bitcoin left the concept of distributed ledgers on the back burner for many years.

The spark came from innovations in the private sector, which were able to establish secure and high integrity identity platforms, using sim cards. The sim cards, which utilised distributed ledger technology as a component of the overall system, were able to run on the older-feature phones the government had first started issuing just prior to 2020. With the fuse lit, it was not long before government service delivery was explosively transformed.

138 ANZ and Wells Fargo, 2016



Kaisu uses her phone for the administration of most of the services in her life, including banking. There is virtually no such thing as ‘the unbanked’¹³⁹ anymore. Benefits, entitlements and other payments can all be made through and stored on the UBT. Kaisu was disappointed in the number of digital currencies she had stored in various accounts and wallets. She felt ripped off. Kaisu had just read an article talking about how ‘complementary currencies’ like digital currencies, or even loyalty reward points,¹⁴⁰ generally lost value over time and tended to become more and more regulated, and shifted towards a central authority until they either joined the official fiat currency or collapsed.¹⁴¹

The article went on to discuss how until the mid-19th century banks were able to issue their own bank notes. Unscrupulous individuals would sometimes pay debts in currencies that were hard to exchange or redeem, and unsavoury employers would sometimes pay employees in vouchers that were only redeemable through their cartels that had inflated prices for staple goods and services.

Kaisu thought about the similar situation that happened when a big company overseas came out with a digital currency and paid its workers with it. She wondered why the article did not mention it, but then she noticed it had focused instead on the foreign ‘smart contract’ scandal where cartels were inflating their digital assets and altering the performance of the ‘smart contracts’ programmable-code in, often technically legal, but unethical ways. The article drew comparison to the ‘wild cat’ banks on the American frontier that would leave bank vaults slyly open with the deceiving appearance of being overflowing with riches, but they were in fact empty.

COMMENTARY

In this scenario the mixture of competing banking and finance services and products presents a bewildering array to the consuming public. The lack of a supportive regulatory regime has produced uncertainty amongst users and ambiguity to industry. Technological advancements are not producing the productivity gains they otherwise could, and the pathway is much longer than it otherwise could have been.

Key question:

- How may public and private sector organisations provide leadership and direction to the market in order to balance risk and optimise rewards? Particularly where innovation occurs offshore and Australia is in a position where it would need to accelerate research and development in order to remain competitive.









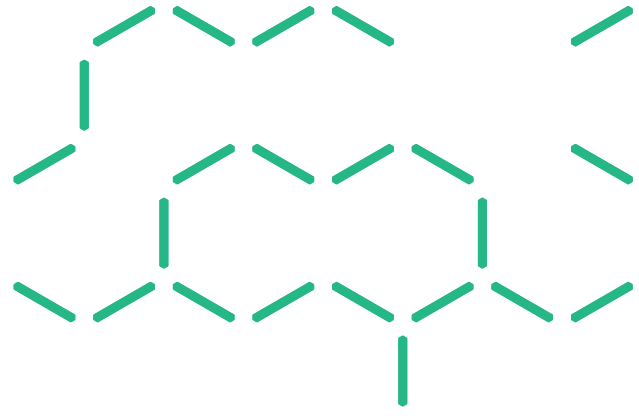
How may public and private sector organisations provide leadership and direction to the market in order to balance risk and optimise rewards?

¹³⁹ Individuals who are without bank accounts or access to a financial institution are considered ‘unbanked’.

¹⁴⁰ Deloitte, Centre for the Edge, 2015

¹⁴¹ Ibid

<p>LEGAL</p> 	<p>As innovations spread into new sectors and either disrupt them or are simply adopted by them, there is an adjustment period. The customary law, and industry standards required to set norms for trading and exchange, take a while to adapt to changes, and even longer for emerging and brand new markets.</p> <p>In this future, innovators, the market, and individuals in the community suffer from a lack of certainty with respect to various aspects of distributed ledgers. This uncertainty has a negative impact on their respective levels of confidence.</p>
<p>INNOVATION</p> 	<p>In this scenario the sailing ship effect soaks up a lot of effort and resources for research and development until significant break-throughs and clear advantages define tipping points in technology directions.</p>
<p>QUALITY</p> 	<p>Uneven quality has a dampening effect on the market. Poor performance inhibits the diffusion of innovation.</p>
<p>USER ADOPTION</p> 	<p>Misplaced trust in products and services that prove to be sub-standard or suboptimal, impacts the adoption of all similar technologies. Clear differentiation of brands and products is required to ignite recognition and loyalty.</p>
<p>INTEROPERABILITY</p> 	<p>Interoperability is key to the transition towards the adoption of a beneficial product or service, from a mistrusting market. The more integrated and seamless the integration, the less friction to use there is. When assessing distributed ledger products and service, regulators and other assurance providers will assess risk in the design of the whole system. These security and risk assessments will evaluate all the other components providing user interfaces, cryptographic key management, and off-chain databases, communications, and processing.</p>
<p>DIGITAL CURRENCY</p> 	<p>There is a history of complementary currencies being regulated either into alignment with centrally issued fiat currencies, or into extinction.</p> <p>Inter-currency exchange rates naturally emerge as markets in environments with multiple tokens for value exchange.</p>



5.5 Collapse scenario: A slippery slope

DRIVERS FOR CHANGE	TECHNOLOGICAL DEVELOPMENT	USER ADOPTION	REGULATORY ENVIRONMENT
Direction of change	▼	▼	▼
<p>‘Blockchain technology represents an alternative approach to the safe storage of information of value such as trade execution, clearing and settlement and custody. It can provide for secure, transparent and immediate confirmation of information that can then be distributed to all interested parties without the need for a central record-keeping authority. While this new alternative approach has many advantages, it also presents new challenges related to data privacy, defect corrections, and trust in decentralised financial servicing.’¹⁴²</p>			
<p>KEY QUESTION:</p> <p>Why may institutions and users become averse to the use of Distributed Ledger Technology?</p> <p>In this scenario, we imagine a future Australia with a regulatory environment and user-base hostile to distributed ledgers through broken trust. Some technological innovations had occurred but their implementations were not aligned with the appetites or expectations of investors and users. Once this foundation of trust was eroded, it was a slippery slope to distrust and contempt. Although trust may be granted, it usually takes a long time to build, and may collapse in an instant.</p>			

THE WORLD OF 2030

This future is a stark reality for distributed ledgers. Rampant innovation has brought distributed ledgers to many areas of the economy and society. The expectations set, however, were not met. The expectations of those few it did meet, were unfortunately criminally minded, and who used a vacuum of regulation and understanding to succeed in making significant proceeds of crime.

As the shine comes off the distributed ledger euphoria, cracks start to appear on the platforms and applications that have been rapidly adopted in this era of cloud computing and everything-as-a-service. Oracles established to administer insurance claims were discovered to be misconfigured by insurers in order to alter the outcomes of claims, and increase premiums, as are the ‘smart contracts’ offered by the insurers to, ‘save you time and give you peace of mind’. Several Decentralised Autonomous Organisation (DAOs) are discovered to be Ponzi schemes, but the litigation takes years as there remains a question at law to determine what the DAO is, if it can actually be sued, and which laws would be enforced if it could be.

As distrust for anything related to distributed ledgers becomes systemic, bank runs on digital currencies occur. Bank runs have historically occurred because of a concern by account holders that there will not enough cash left for them to withdraw their deposits before the bank fails. Currencies only hold their value because of the shared belief in this value. It has been decades since bank notes were tied to a gold standard, or any other physical asset. Digital currencies are the same. The global financial crisis of the early 21st century demonstrated how rumours and speculation were able to result in the collapse of significant institutions.

With an irrational and emotional loss of faith in the underpinning architecture of digital currencies, many of them suffer significant devaluations, and many completely collapse. For a series of reasons the government of the day decides it is in Australia’s interest to prohibit this technology and the use of any non-fiat digital currencies.

¹⁴² Financial Conduct Authority, 2016

INVASION OF PRIVACY – WHEN YOU CANNOT HELP BUT WEAR YOUR HEART ON YOUR SLEEVE...

As the IoT, coupled with other emerging technologies, becomes capable of assessing the emotional state of individuals, it becomes capable of recording very personal and intimate details that we may wish to keep private. Measurements such as eye tracking, body warmth, voice patterns and sentiment analysis are providing a window into the soul. Should this data be captured and stored in distributed ledgers, this could be a privacy cause for concern itself.

The matter becomes more salient when we start to consider the highly plausible potential for the rich context around an emotional state to be captured. This could include metadata, proximity to other individuals and stimuli, and potentially even what was read or heard at the time. Although there is apparently great potential for the commercial deployment of distributed ledgers for the purposes of ensuring a high amount of integrity in transactions, some transactions may present significant privacy issues. Scope creep, unintended consequences and a lack of foresight may result in personal, deeply private and intimate data being recorded on permanent and persistent ledgers. How does the ‘right to privacy’ factor into transactions on a distributed ledger? What remedies are available for violations of privacy, when transactions cannot be removed, ‘as if it had never occurred’?

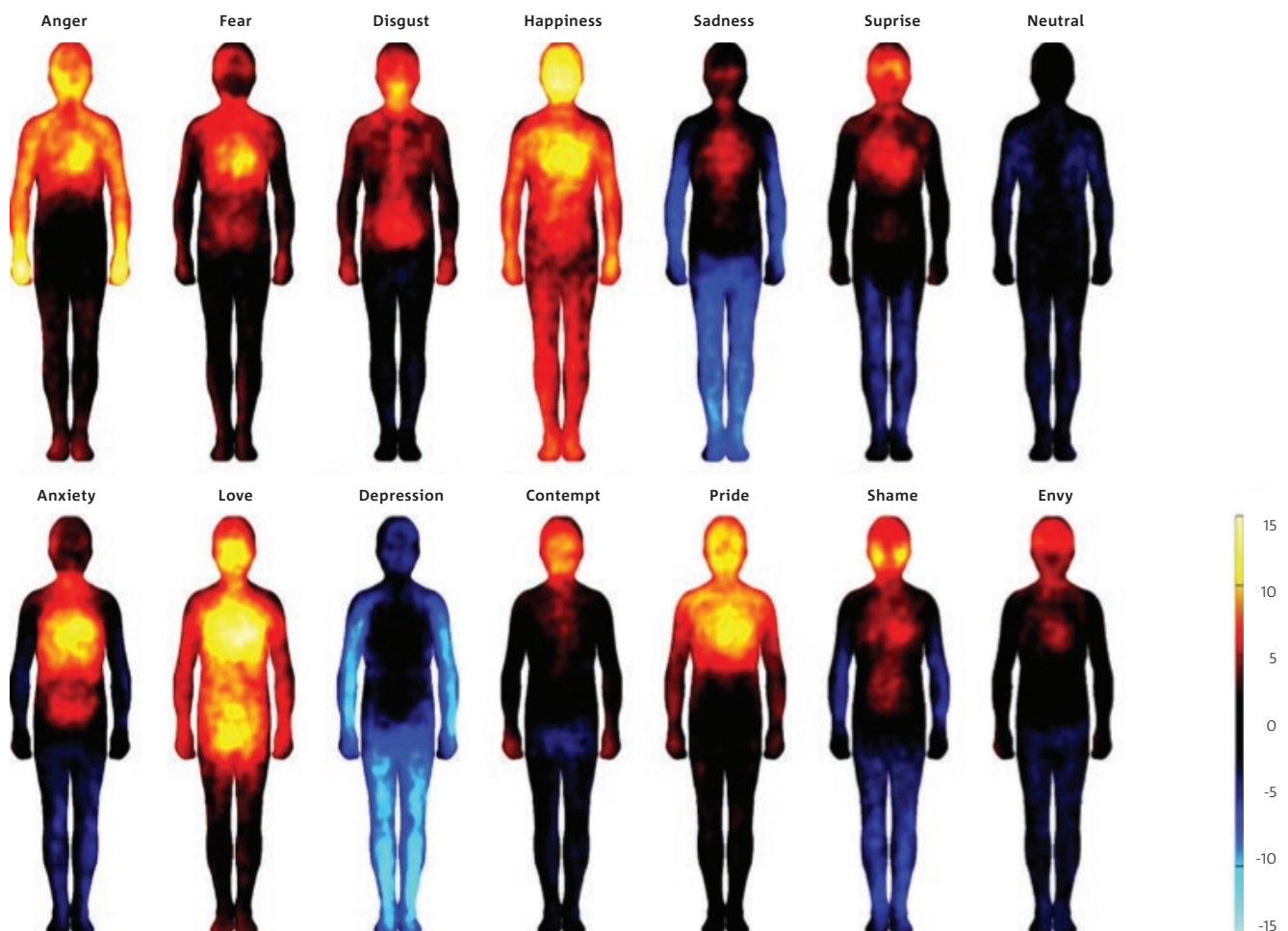
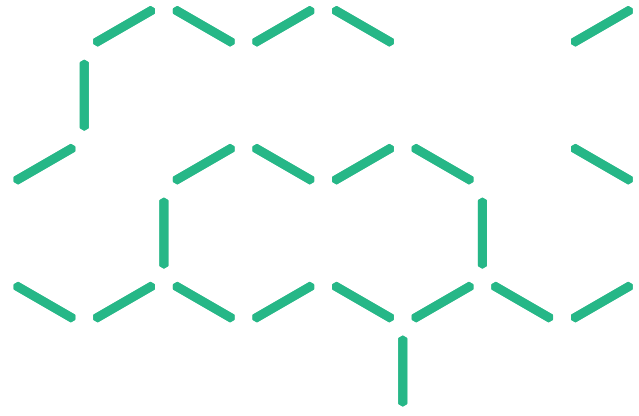


Figure 11: Body map of human emotion showing regions of increased activation (warm colours) and decreased (cool colours) for each type

Source: Nummenmaa, Glerean, Hari & Hietanen, 2013



A DAY IN THE LIFE OF 2030 – A SLIPPERY SLOPE

The only trusted aspect of blockchain in 2030 is the blockchain-enabled news. Through the use of blockchains and cognitive computing (artificial intelligence), trusted and reliable facts are able to be cross-checked by natural-language processors scanning text and decoding the spoken word. Politicians, announcers and journalists are fact checked in real-time. The common term for this end to ‘fake news’, which is built on ‘baked in facts’, is Bake In Fake Out, or BIFO. Interviewees initially take some time to adjust to this hard-hitting reality.

Media headlines are littered with a litany of blockchain and distributed ledger technology issues including:

- Gold-plated supply-chain provenance systems promoted as insurance for Australia’s export markets are discovered to be over-hyped and not respected by the relevant export markets.
- A DAO is involved in making supply chain decisions and performs an illegal act. The mum and dad investors involved in the transaction are investigated by law enforcement and are prosecuted as criminals, in part because the DAO is not recognised as a legal entity.
- Insurance oracles¹⁴³ specified in the ‘smart contracts’ are found to have been rigged against claims, as had the ‘smart contracts’ themselves.
- Public distributed ledgers have sensitive and deeply personal information registered on them with no way of restoring the victims’ privacy or retrieving and retracting the information. These include:
 - Government-held health records, where the patient has the legal and ethical right to redact details of actual events and facts, but cannot.
 - Criminal records that were meant to have been legally exonerated, expunged or spent are still visible in systems, and to users, that they should not be.

- The restructuring and reformatting of an older blockchain to meet new regulatory requirements, changing customer demands, and technological updates meant rewriting the whole blockchain in order to allow it to be accessible in the new system. Data integrity issues corrupt older entries, but this issue is not identified until months after the transition, putting later transactions under uncertainty.
- A blockchain enabled voting system, which was thought to provide voter anonymity was discovered by researchers to be re-identifiable. The researchers make the data public, which discloses how everyone voted.

The blockchain brand becomes so tainted that there is a loss of trust and faith in the institutions that are seen to use them.

In this scenario, the blockchain brand becomes so tainted that there is a loss of trust and faith in the institutions that are seen to use them.

¹⁴³ Oracles know something (for example about some event or activity, perhaps the location of a shipment) and always speak the truth (or in other words, provide correct and reliable answers when asked).

COMMENTARY

Examples of emerging ‘fact checking’ and ‘evidence-based journalism’ news platforms are arising as a countertrend to ‘fake news’. Wikitribune,¹⁴⁴ from the founder of Wikipedia, is a news platform that intends to link sources and references to news articles. It is plausible to conceive a blockchain performing the role of an oracle for facts and providing identity services for journalists and for verifying the provenance of news articles.


In this scenario emerging and future use cases are discussed in order to foreshadow issues before they arise. The World Economic Forum recently rated blockchain technology as a high risk and low benefit emerging technology, third most likely to significantly exacerbate global economic risks, and fourth in need of better governance.¹⁴⁵ Some indications of risks and issues with blockchains and distributed ledgers have already occurred, such as the incident with the DAO. There are, however, many questions that may be asked of technologies deployed today, which may also forearm decision makers against emerging risks:

- Are distributed ledgers admissible as evidence? If so, under what circumstances, and in which jurisdictions?
- What encryption, or other technologies, are considered a defence asset, and subject to export controls?¹⁴⁶
- Are ‘Smart Contracts’ contracts?
- What is a Decentralised Autonomous Organisation? Is it a legal entity against which legal action can be taken?

The engagement of professionals and subject-matter experts from the various disciplines and domains involved will assist in the identification and mitigation of risks.

Key questions:

- How should the public and private sector ensure the relevant engagement and interaction of professionals and practitioners, from the various domains involved, in order to avoid the failures listed here, and discover the ones that are not?
- How should both sectors provide certainty to investors and innovators operating new technologies and business models?

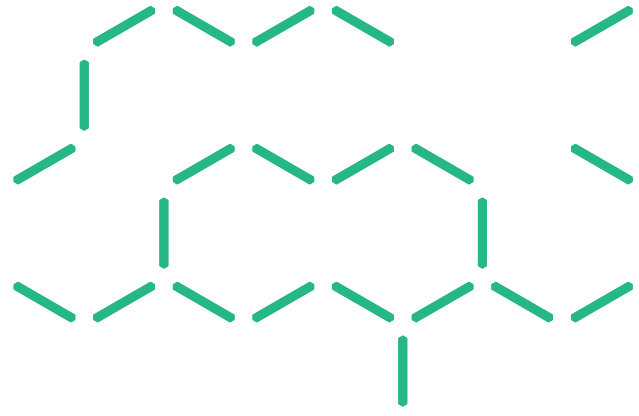








The engagement of professionals and subject-matter experts from the various disciplines and domains involved will assist in the identification and mitigation of risks.

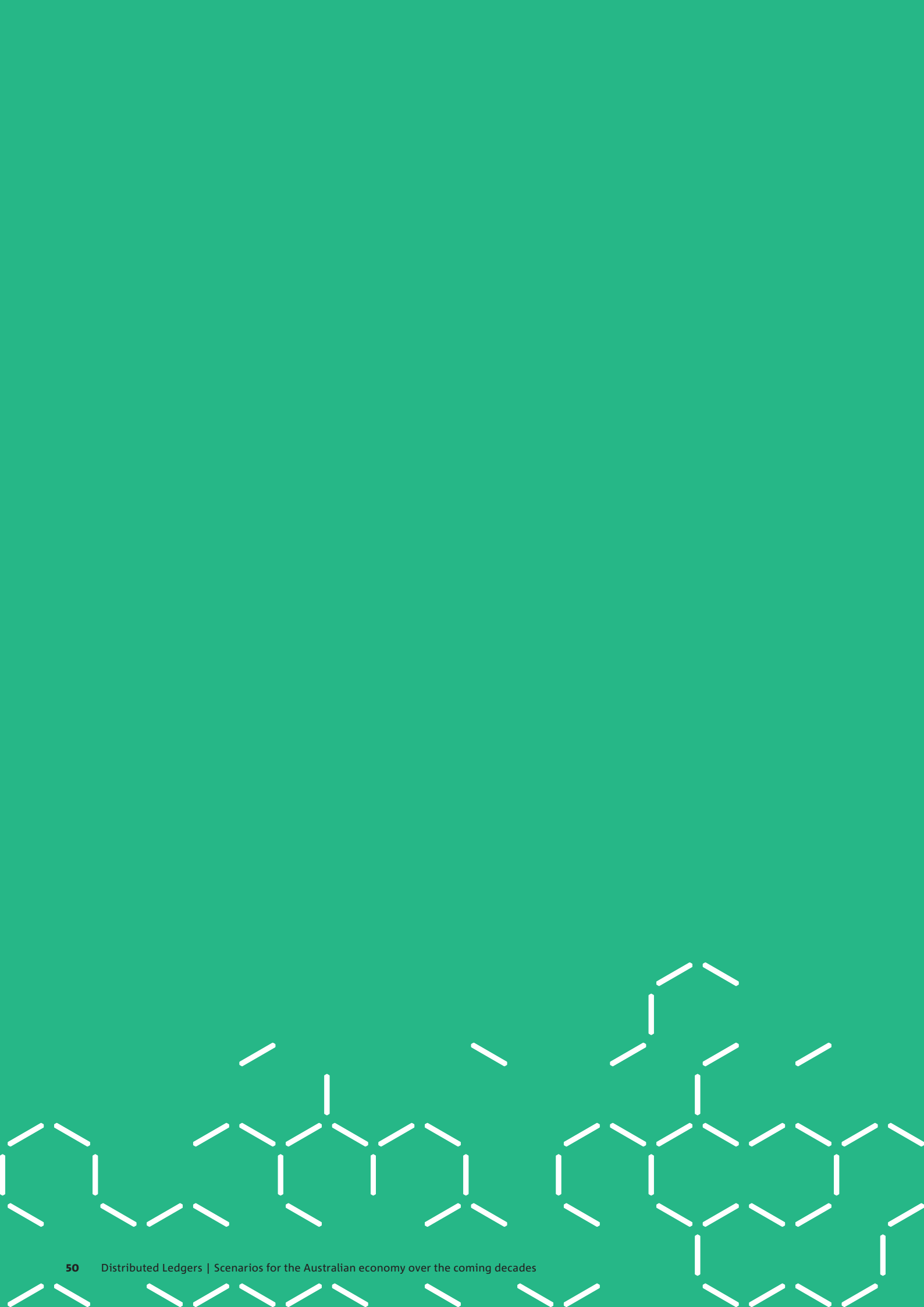
¹⁴⁴ www.wikitribune.com

¹⁴⁵ World Economic Forum, 2017

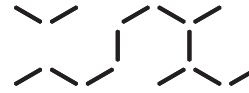
¹⁴⁶ Department of Defence, 2017



<p>LEGAL</p> 	<p>Without clear guidance and direction from regulators as a deterrent, scandals of unethical business practices and outright criminality with ‘smart contracts’ and Distributed Autonomous Organisations (DAOs) occur. Mum and dad investors lose millions. The schemes are standard pump and dump investment frauds and Ponzi schemes, although the use of technology makes it newsworthy. The protracted legal debate over the question at law of what a DAO is, and the lack of dispute and resolution services able to handle the complexity of the ‘smart contracts’ generates bad publicity that demonises the sector.</p>
<p>INNOVATION</p> 	<p>To paraphrase Machiavelli, organised crime is the continuation of business by other means. Technology is neither good nor evil, it is how it is used that should be judged.</p> <p>Trans-national serious and organised criminals find distributed ledgers highly beneficial in running their empires. Underground services and dark websites enable crime gangs to establish trust between each other in ways that were not previously possible. These relationships are further enhanced with the use of real-time language translators from cross-cultural interactions, and IoT sensors with a shared understanding or when the drugs were intercepted by the police, or if the shipment was ripped off by a gang member. Their use of the technology tarnishes its reputation in the mind of the public, and becomes politically unpalatable.</p> <p>Businesses also operate as cartels, using distributed ledgers to increase barriers to entry by keeping information and processes locked in permissioned ledgers and away from competitors and new market entrants.</p>
<p>QUALITY</p> 	<p>Without testing for failure, it is possible for products and services to reach a significant user base before a material issue becomes apparent.</p> <p>In this scenario a trusted oracle, used by millions of users every day is discovered to be untrustworthy.</p> <p>Without a logical or governance mechanism to deal with the toxic data placed on it, a distributed ledger with the records of millions of dollars of digitised assets is seized by law enforcement as they investigate the origins of the illegal content and the associated criminality.</p>
<p>USER ADOPTION</p> 	<p>After being sold too much snake oil, users no longer trust the brand of distributed ledgers, or blockchains.</p>
<p>INTEROPERABILITY</p> 	<p>Without relevant standards referring to how fraud controls should interoperate with the entire system, distributed ledgers marketed as fraud controls are found to be insufficient, and trust in their capabilities is eroded.</p>
<p>DIGITAL CURRENCY</p> 	<p>After banning the use of non-fiat digital currencies, and postponing the development of any distributed ledger based financial services platforms, a foreign jurisdiction launches a fiat digital currency that is rapidly adopted as a unit of value and exchange. There are concerns on how the use of this foreign fiat digital currency will impact Australian monetary and fiscal policy levers.</p>



6 METHODOLOGY



‘We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten. Don’t let yourself be lulled into inaction.’

Bill Gates, The Road Ahead

6.1 Our research

Data61’s research is focused on the methods and tools organisations can use to (a) explore plausible futures and (b) make wise choices; both within a digitally enabled economy context. This research broadly falls under the fields of decision theory, management science, operations research and applies human factors, including social science domains such as geography, economics, and organisational psychology, to digital technology issues.

When considering the future, the further forward we look, the more possibilities and potential there is. The relatively small zone of uncertainty of the present rapidly expands over time. We use the futures cone to frame our examination of the emerging environment. There is a natural tendency to discount scenarios on the edge of the cone, and not to question linear projections of the present – towards the centre. We question the assumptions and challenge orthodoxies with evidence and research, and we check the plausible viability of ideas at the edge. This is done in order to identify potential blind spots, and uncover emerging opportunities and risks, in order to assist decision makers in finding pathways to preferable futures. These preferable futures may exist anywhere across the base of the cone, which faces the future.

We use the futures cone to frame our examination of the emerging environment.

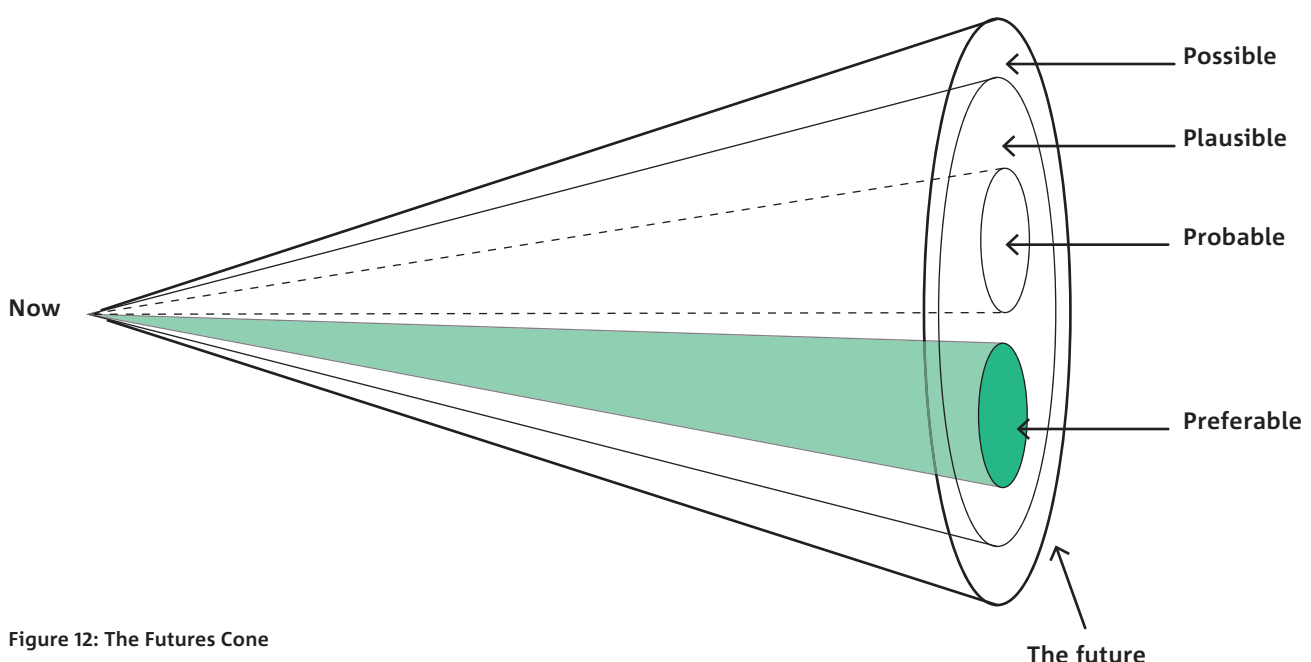


Figure 12: The Futures Cone

Source: Voros, 2003

6.2 CSIRO strategic foresight methodology

CSIRO has defined a process for conducting strategic foresight research.

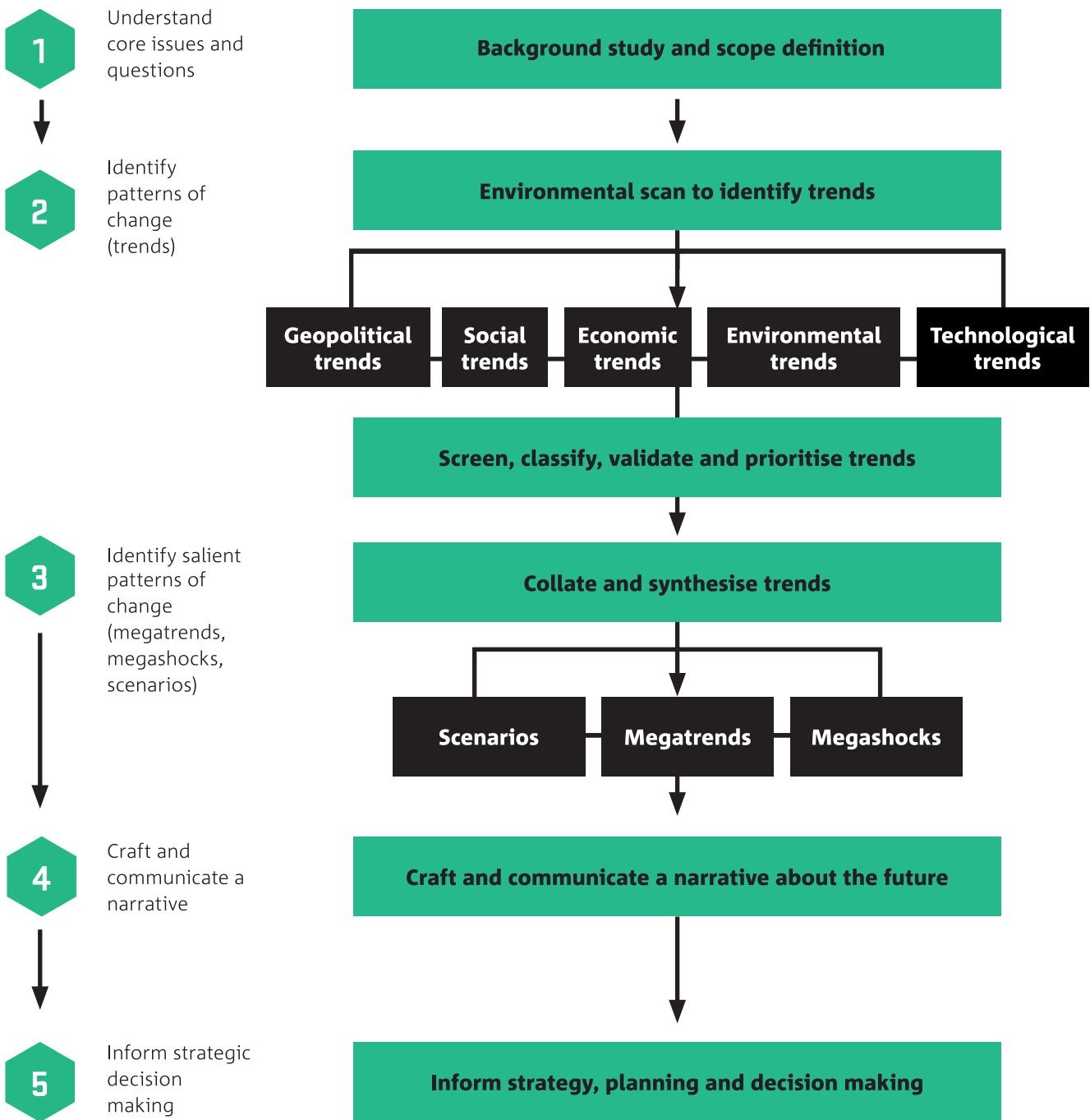
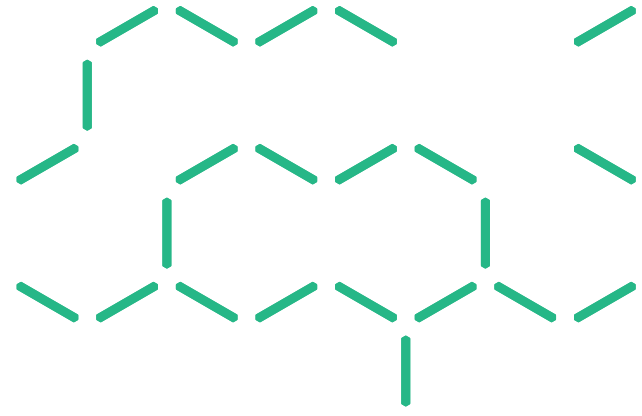


Figure 13: CSIRO's strategic foresight methodology



The approach for the research used for this report followed the CSIRO strategic foresight methodology. A literature review, and subject-matter expert engagement were used in order to understand the core issues and questions, and also to identify the patterns of change. Over 100 subject-matter experts were engaged, primarily through the course of four consultative workshops and one panel discussion, namely:

- A panel discussion on the impact of blockchain on the future of audit (and other professional services)
- A workshop on the impact of privacy and identity
- A workshop on the impact of law (especially ‘smart contracts’)
- A workshop on draft scenarios
- A workshop on the use of distributed ledgers in the future of the electricity grid.

An interim report was released at the end of 2016, containing initial findings and an exploration of emerging and high impact use cases.

This research was conducted in parallel with, and informed by, the research conducted by Dr Mark Staples into the risks and opportunities for systems using blockchain and smart contracts.

6.3 Scenario design

‘Morphological analysis is simply an ordered way of looking at things.’¹⁴⁷

The scenarios have been designed by combining the complementary methodologies of Zwicky’s¹⁴⁸ General morphology¹⁴⁹ and Dator’s four archetypes of the future.¹⁵⁰ They have also been stratified by their technological maturity.¹⁵¹ The four archetypes have been adjusted, using the Houston method¹⁵², to explore aspirational, transformative, new equilibrium, and collapse scenarios.

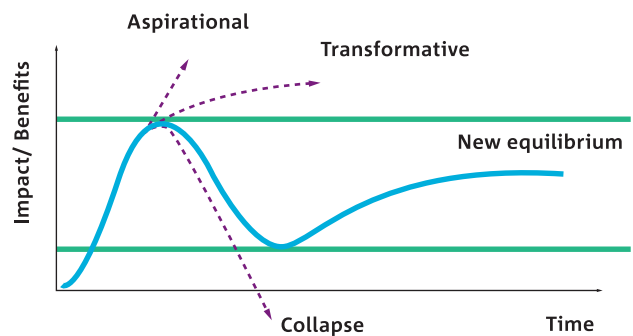


Figure 14: Four archetypes of the future

Scenarios typically explore the intersection between technology, human behaviour and regulation. Each scenario explores a three-element morphology: technology development, user adoption and the regulatory environment.

¹⁴⁷ Zwicky, 1948

¹⁴⁸ Fritz Zwicky (1898–1974) was a Swiss astronomer who worked most of his life at the California Institute of Technology.

¹⁴⁹ A method for systematically identifying the total set of possible configurations contained in a multi-dimensional, non-quantified complex problem. Parameters of the problem are identified, assigned values, and set against each other in a morphological ‘Zwicky box’.

¹⁵⁰ Continued growth; collapse/decline; conserver/disciplined society; and high tech transformation.

¹⁵¹ Wardley n.d.

¹⁵² This method replaces the continuation scenario with an aspirational scenario, and is generally considered to add more value to the scenario set.

TECHNOLOGICAL DEVELOPMENT

There are questions over the scalability of blockchain, and the suitability of other trust methods for distributed ledger technologies. A positive outcome would result in greater levels of trust and value in information systems, whereas a neutral result would indicate continuation of current circumstances, and a negative result indicates a situation where misplaced trust has been given to information systems with adverse consequences.

USER ADOPTION

Users adopt technology based upon their positive perception of the technology and the influence of others in their peer-group. The literature¹⁵³ demonstrates that adoption is shaped by emotional perceptions over rational cost benefit analysis. A positive outcome in a scenario indicates a movement of, or a trend towards, adoption encouraged by successful uses (and use cases), which have built an experience-base that the new user is willing to trust. A neutral outcome indicates no wide-scale adoption, whereas a negative outcome indicates either a lack of positive examples and/or significant negative examples that have damaged the brand of the technology.

REGULATORY ENVIRONMENT


The importance of the regulatory environment in supporting distributed ledger technology cannot be overstated. The core role of 'the state' is protection. This protection can take several forms, from security (in all its dimensions), to ensuring there is a reasonable sense of certainty with respect to contracts and negotiations. In an environment where regulators have taken notice of emerging distributed ledger technologies and have provided the results of their analysis through guidance and regulation, there is anticipated to be a greater sense of certainty and confidence in the marketplace. The same is true with respect to cyber security. A neutral outcome indicates no further developments by the regulators, which will include a continuation of certain ambiguities and uncertainties. A negative outcome indicates a hostile regulatory environment.

TECHNOLOGICAL MATURITY

Activities, practices and models evolve along a progression pathway from a genesis to a commoditised utility.¹⁵⁴ These states are defined as follows:

Table 4: Technological evolutionary maturity

EVOLUTIONARY STAGE	STATE	DESCRIPTION OF THE TECHNOLOGY
Genesis	Chaotic	Rare, poorly understood, used as a market differentiator, considered a competitive advantage, has a high unit value, is constantly changing, has an undefined market.
Custom Built Product	Transitional	High profitability, high total value, high total variation, responsive to customers.
Commodity	Linear	Commonplace, well understood, efficient operations, considered a cost of doing business, standardised, has a defined market.



Users adopt technology based upon their positive perception of the technology and the influence of others in their peer-group.

153 Ventakesh, 2000; Straub, 2009; Rodger & Gonzalez, 2013; Swerdlhoff, 2016

154 Wardley n.d.

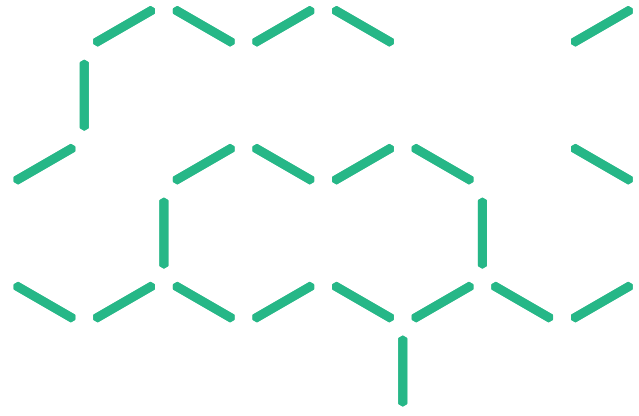
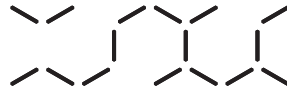


Table 5: Morphology of the scenarios

SCENARIO	TECHNOLOGICAL DEVELOPMENT	USER ADOPTION	REGULATORY ENVIRONMENT
LINEAR STATE			
Regulation on rails (ASPIRATIONAL)	▲	▲	▲
LINEAR STATE			
The sheriff on the digital superhighway (TRANSFORMATIVE)	▲	▲	◀▶
TRANSITION STATE			
A bumpy ride (NEW EQUILIBRIUM)	▲	◀▶	◀▶
CHAOTIC STATE			
A slippery slope (COLLAPSE)	▼	▼	▼

Legend: Positive outcome ▲ Neutral outcome ◀▶ Negative outcome ▼

REFERENCES



Abbate, J. (1999). Cold war and white heat: The origins and meanings of packet switching. In D. MacKenzie, & J. Wajcman, *The Social Shaping of Technology* (pp. 351 - 371). Buckingham: Open University Press.

ABI Research. (2013, May 9). *More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020*. Retrieved from ABI Research: <https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/>

ADCCA. (2016). *Aus.ID Collaboration*. Australian Digital Currency Commerce Association.

ANZ and Wells Fargo. (2016, September). *Distributed Ledger Technology and Opportunities in Correspondent Banking*. Retrieved from https://bluenotes.anz.com/media/1002/ANZ_WellsFargo_DLT_Paper_HIRES.pdf

Association of Certified Fraud Examiners. (2016). *Report to the Nations on Occupational Fraud and Abuse*. Austin: Association of Certified Fraud Examiners.

Australian Computer Society. (2016). *Cybersecurity: Threats, Challenges, Opportunities*. Australian Computer Society. Retrieved from https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

Australian Cyber Security Centre. (2016). *ACSC 2016 Threat Report*. Australian Government. Retrieved from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

Australian Law Reform Commission. (2008, August 12). *The meaning of privacy*. Retrieved from Australian Law Reform Commission : <http://www.alrc.gov.au/publications/1.%20Introduction%20to%20the%20Inquiry/meaning-privacy>

Australian Payments Clearing Association. (2015). *New Payments Platform*. Retrieved from APCA: <http://www.apca.com.au/about-payments/future-of-payments/new-payments-platform-phases-1-2>

Bank for International Settlements Committee on Payments and Market Infrastructures. (2017). *Distributed ledger technology in payment, clearing and settlement: An analytical framework*. Bank for International Settlements.

Bates, C. L. (2016). *Bitland Global: White Paper*. Brave New Coin. Retrieved from <https://bravenewcoin.com/assets/Whitepapers/Bitland-Whitepaper.pdf>

Benson, B. L. (2007, June 29). *The Enterprise of Customary Law*. Retrieved from Mises Institute: <https://mises.org/library/enterprise-customary-law>

Bitcoin Mining. (2017). *Bitcoin Mining Pool Hash Rate Distribution*. Retrieved from Bitcoin Mining: <https://www.bitcoinmining.com/bitcoin-mining-pools/>

BitFury. (2016, February 7). *The BitFury Group and Government of Republic of Georgia Expand Historic Blockchain Land-Titling Project*. Retrieved from Medium: <https://medium.com/@BitFuryGroup/the-bitfury-group-and-government-of-republic-of-georgia-expand-historic-blockchain-land-titling-4c507a073f6b>

Blockchain.info. (2017). *Blockchain Size*. Retrieved from Blockchain.info: <https://blockchain.info/charts/blocks-size?timespan=all>

Brave New Coin. (2016). *Venture Capital*. Retrieved from Brave New Coin: Digital Currency Insights: <https://bravenewcoin.com/industry-resources/bitcoin-venture-capital-investments/2016/>

Business Insider. (2016, June 9). *There will be 24 billion IoT devices installed on Earth by 2020*. Retrieved from Business Insider: <http://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5/?r=AU&IR=T>

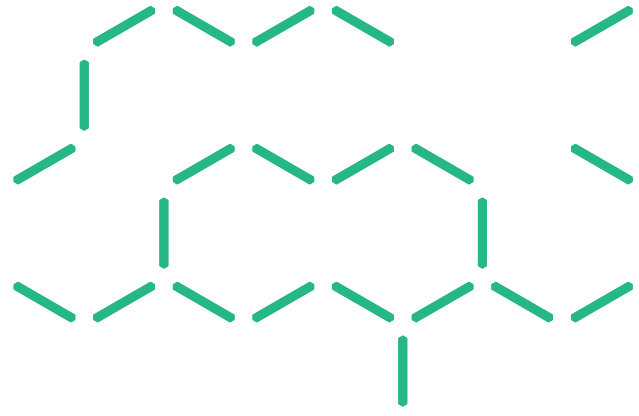
Buterin, V. (2013, March 12). *Bitcoin Network Shaken by Blockchain Fork*. Retrieved from Bitcoin Magazine: <https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/>

Center for Long-Term Cybersecurity. (2016). *Cybersecurity Futures 2020*. Retrieved from <https://cltc.berkeley.edu/scenarios/>

Chakrabarti, A., & Manimaran, G. (2002). Internet infrastructure security: a taxonomy. *IEEE Network*, 13 - 21.

Christie, A. (2016). *When is a Smart Contract (or other Blockchain/Distributed Ledger Application) not so Smart?* EY.

Cisco. (2016, June 7). *Cisco Visual Networking Index Predicts Near-Tripling of IP Traffic by 2020*. Retrieved from Cisco - The Network: <https://newsroom.cisco.com/press-release-content?type=press-release&articleId=1771211>



Clark, J., & Whitbourne, K. (2009, September 8). *How much actual money is there in the world?* Retrieved from HowStuffWorks.com: <http://money.howstuffworks.com/how-much-money-is-in-the-world.html>

Cressey, D. R. (1973). *Other People's Money*. Montclair: Patterson Smith. CSIRO and Energy Networks Australia. (2017). *Electricity Network Transformation Roadmap: future market platforms and network optimisation synthesis report 2017-27*.

CSIRO and Energy Networks Australia. (2017). *Electricity Network Transformation Roadmap: future market platforms and network optimisation synthesis report 2017-27*.

Data61. (2017). *Digital Legislation*. Retrieved from Digital Legislation: <https://digital-legislation.net/>

Davidson, S., & Potts, J. (2017). The Stationary Bandit Model of Intellectual Property. *Cato Journal*, 37(1), 69 - 88.

Deloitte Centre for the Edge. (2015). *The Future of Exchanging Value: Cryptocurrencies and the trust economy*. Melbourne: Deloitte.

Department of Broadband, Communications and the Digital Economy. (2013). *Advancing Australia as a Digital Economy*. Canberra: Australian Government. Retrieved from <http://apo.org.au/files/Resource/Advancing-Australia-as-a-Digital-Economy-BOOK-WEB.pdf>

Department of Defence. (2017). *Overview of Cryptography and the Defence Trade Controls Act 2012*. Retrieved from Defence Export Controls: <http://www.defence.gov.au/ExportControls/Cryptography.asp>

Department of Infrastructure and Regional Development. (2014). *Transport Security Outlook to 2025*. Canberra: Commonwealth of Australia.

Diamond, J. (2005). *Collapse: How Societies Choose to Fail or Survive*. London: Penguin Books.

Digiconomist. (2017). *Digiconomist*. Retrieved from Bitcoin Energy Consumption Index: <http://digiconomist.net/bitcoin-energy-consumption>

Dodd, T. (2017, April 30). *University of Melbourne first in Australia to use blockchain for student records*. Retrieved from Australian Financial Review: <http://www.afr.com/leadership/university-of-melbourne-first-in-australia-to-use-blockchain-for-student-records-20170427-gvubid>

Ericsson. (2011). *Ericsson White Paper: More Than 50 Billion Connected Devices*. Ericsson. Retrieved from http://www.akos-rs.si/files/Telekomunikacije/Digitalna_agenda/Internetni_protokol_ipv6/More-than-50-billion-connected-devices.pdf

Evans, D. (2011). *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*. CISCO. Retrieved from http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Evans-Greenwood, P. (2016, May 5). *Blockchain performance might always suck, but that's not a problem*. Retrieved from Deloitte Blogs: <http://blog.deloitte.com.au/greendot/2016/05/05/blockchain-performance-sucks-not-problem/>

Everledger. (2017). *Welcome to the digital vault of the future*. Retrieved from Everledger: <https://www.everledger.io/>

Eversheds Sunderland. (2016). *Blockchain - considering the regulatory horizon*. Retrieved from http://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/Financial_institutions/Blockchain_-_considering_the_regulatory_horizon

Ferrara, E., Varol, O., David, C., Menczer, F., & Flammini, A. (2015). The Rise of Social Bots. *Communications of the ACM*, 96 - 104.

Financial Conduct Authority. (2016). *Business Plan 2016/17*. London: Financial Conduct Authority.

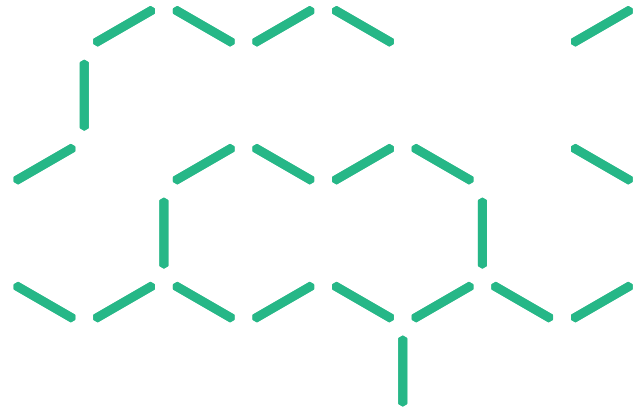
Flowers, S. (1996). *Software failure: management failure: amazing stories and cautionary tales*. New York: John Wiley & Sons.

Gartner. (2013, December 12). *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020*. Retrieved from Gartner Newsroom: <http://www.gartner.com/newsroom/id/2636073>

Gartner. (2014, November 11). *Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015*. Retrieved from Gartner Newsroom: <http://www.gartner.com/newsroom/id/2905717>

Gartner. (2015, November 10). *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*. Retrieved from Gartner Newsroom: <https://www.gartner.com/newsroom/id/3165317>

- Government of Canada. (2011, March 6). *Federating Identity Management in the Government of Canada: A Backgrounder*. Retrieved from Government of Canada: <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/federating-identity-management-government-canada-backgrounder.html>
- Greverie, F., Buvat, J., Nambiar, R., Appell, D., & Bisht, A. (2014). *Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT*. Capgemini Consulting .
- Grimaldi, M., & Barrière, F. (2004). Trust and Fiducie. In A. Hartkamp, M. Hesselink, E. Hondius, C. Joustra, E. du Perron, & M. Veldman, *Towards a European Civil Code: Third Fully Revised and Expanded Edition* (pp. 787 - 806). Kluwer Law International.
- Hajkowicz, S., Reeson, A., Rudd, L., Bratanova, A., Hodgers, L., Mason, C., & Boughen, N. (2016, January). *Tomorrow's Digitally Enabled Workforce: megatrends and scenarios for jobs and employment in Australia over the coming twenty years*. Retrieved from <http://www.data61.csiro.au/en/Our-expertise/Expertise-Strategic-insight/Tomorrows-Digitally-Enabled-Workforce>
- Harkness, A. (2016, January 22). *ASX Selects Digital Asset Holdings, LLC*. Retrieved from ASX: <http://www.asx.com.au/documents/asx-news/ASXSelectsDigitalAssetHoldingsLLC.pdf>
- Hawley, K. (2012). *Trust: A Very Short Introduction*. Oxford: Oxford University Press .
- Hertig, A. (2016, September 2016). *A Controversial Bitcoin Alternative is Seeking a Comeback*. Retrieved from CoinDesk: <http://www.coindesk.com/controversial-bitcoin-alternative-seeking-comeback/>
- Hertig, A. (2017, March 14). *CoinDesk Explainer: The Bitcoin Unlimited Debate*. Retrieved from CoinDesk: <http://www.coindesk.com/coindesk-explainer-bitcoin-unlimited-debate/>
- Howard, P. N. (2015, June 9). *Sketching out the Internet of Things trendline*. Retrieved from Brookings: <https://www.brookings.edu/blog/techtank/2015/06/09/sketching-out-the-internet-of-things-trendline/>
- HSBC, Bank of America Merrill Lynch, IDA Singapore. (2016, August 10). *BofAML, HSBC, IDA Singapore Build Pioneering Blockchain Trade Finance App*. Retrieved from HSBC: www.about.hsbc.com.sg/~media/singapore/.../160810-blockchain-letter-of-credit.pdf
- IDC. (2007). *The Expanding Digital Universe*. EMC. Retrieved from https://www.tobb.org.tr/BilgiHizmetleri/Documents/Raporlar/Expanding_Digital_Universe_IDC_WhitePaper_022507.pdf
- IDC. (2010). *The Digital Universe Decade - Are You Ready?* EMC. Retrieved from <https://www.emc.com/collateral/analyst-reports/idc-digital-universe-are-you-ready.pdf>
- IDC. (2011). *The 2011 IDC Digital Universe Study*. EMC. Retrieved from <https://www.emc.com/collateral/about/news/idc-emc-digital-universe-2011-infographic.pdf>
- IDC. (2011). *The Diverse & Exploding Digital Universe*. EMC. Retrieved from <https://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf>
- IDC. (2012). *The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East*. EMC. Retrieved from <https://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf>
- IDC. (2013). *Where in the World is Storage: Byte Density Across the Globe*. Retrieved from IDC: http://www.idc.com/downloads/where_is_storage_infographic_243338.pdf
- IDC. (2014). *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*. EMC. Retrieved from <https://www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities-vernon-turner.htm>
- Intel. (n.d.). *A Guide to the Internet of Things*. Retrieved from Intel: <http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html>
- Kang, K. (2017). *Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of the Blockchain Technology*. OECD Global Anti-Corruption & Integrity Forum.
- Koepl, T. V., & Kronick, J. (2017). *Blockchain Technology - What's in Store for Canada's Economy and Financial Markets? C.D. Howe Institute Commentary, 468*.



Lantmäteriet, Telia & ChromaWay. (2017). *The Land Registry in the blockchain - testbed*. Stockholm: ChromaWay. Retrieved from https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Lucero, S. (2016). *IoT Platforms: Enabling the Internet of Things*. IHS Technology. Retrieved from <https://cdn.ihs.com/www/pdf/enabling-IOT.pdf>

Ma, W. W. (2014, September 9). *Why Created in China is the new Made in China*. Retrieved from World Economic Forum: <https://www.weforum.org/agenda/2014/09/created-china-new-made-china/>

Machina Research. (2013, December 20). *Press Release - Machine-to-Machine Connections to Hit 18 Billion in 2022, Generating USD1.3 Trillion Revenue*. Retrieved from Machina Research: <https://machinaresearch.com/news/press-release-machine-to-machine-connections-to-hit-18-billion-in-2022-generating-usd13-trillion-revenue/>

Manyika, J., & Roxburgh, C. (2011). *The great transformer: The impact of the Internet on economic growth and prosperity*. McKinsey Global Institute.

McCullagh, A. (1998). *E-commerce - A Matter of Trust*. ACS Information Industry Outlook Conference. ACS.

Micali, S. (2016). *Algorand: The Efficient Public Ledger*. Retrieved from <https://arxiv.org/pdf/1607.01341.pdf>

Microsoft News Centre. (2016, November 8). *Webjet and Microsoft build first-of-a-kind travel industry blockchain solution*. Retrieved from Microsoft: <https://news.microsoft.com/en-au/2016/11/08/webjet-and-microsoft-build-first-of-a-kind-travel-industry-blockchain-solution/#sm.001eikwke148zdg9qy82jbgcatwpz#4GMujfpBMzizy2hd.97>

Morrison & Foerster LLP. (2017, March 21). *Delaware Paves the Way for the Use of Blockchain Technology*. Retrieved from JD Supra: <http://www.jdsupra.com/legalnews/delaware-paves-the-way-for-the-use-of-89667/>

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved April 21, 2017, from <https://bitcoin.org/bitcoin.pdf>

National Institute of Standards and Technology, Computer Security Division, Computer Security Resource Centre. (2014, July 30). *Cryptographic Toolkit*. Retrieved from CSRC: <http://csrc.nist.gov/groups/ST/toolkit/index.html>

Navigant Research. (2013, November 11). *The Installed Base of Smart Meters Will Surpass 1 Billion by 2022*. Retrieved from Navigant Research Newsroom: <http://www.navigantresearch.com/newsroom/the-installed-base-of-smart-meters-will-surpass-1-billion-by-2022>

Nummenmaa, L., Glerean, E., Hari, R., & Hietanen, J. K. (2013). *Bodily maps of emotions*. *Proceedings of the National Academy of Sciences of the United States of America*, 111(2), 646 - 651.

OECD. (2015). *OECD Digital Economy Outlook 2015*. Paris: OECD Publishing.

Office of the Australian Information Commissioner. (2017). *Australian Privacy Principles*. Retrieved from Office of the Australian Information Commissioner: <https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles>

Overstock. (2016, March 16). *Overstock.com Announces Historic Blockchain Public Offering*. Retrieved from Overstock.com: <http://investors.overstock.com/phoenix.zhtml?c=131091&p=irol-newsArticle&ID=2148979>

PricewaterhouseCoopers. (2016). *Global Economic Crime Survey 2016 / Australian Report*. PwC.

Proffitt, B. (2013, September 30). *How Big the Internet of Things Could Become*. Retrieved from ReadWrite: <http://readwrite.com/2013/09/30/how-big-the-internet-of-things-could-become/>

Redman, J. (2017, February 23). *Bitcoin's Transaction Queue Sets a New Record*. Retrieved from Bitcoin: <https://news.bitcoin.com/bitcoins-transaction-queue-sets-a-new-record/>

Reis, D. (2016). *Cybersecurity: Issues of Today, A Path for Tomorrow*. Bloomington: Archway Publishing.

Rice, D. (2007). *Geekonomics: The Real Cost of Insecure Software*. Boston: Pearson Education, Inc.

Rodger, J. A., & Gonzalez, S. P. (2013). *Emotion and Memory in Technology Adoption and Diffusion*. *Proceedings of the Nineteenth Americas Conference on Information Systems*, (pp. 1 - 13). Chicago.

Rogoff, K. S. (2016). *The Curse of Cash*. Princeton: Princeton University Press.

- Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., & Schwartz, A. (2003). *Information Technology Security Handbook*. Washington: The World Bank.
- Soderbery, R. (2013, January 7). *How Many Things Are Currently Connected to the "Internet of Things" (IoT)?* Retrieved from Forbes: <https://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/#3a3a2fddb2d>
- Standards Australia. (2017). *The Role of Standards and Innovation for Driving APEC's Silver Economy: an issues paper for the 2017 APEC workshop on standards and innovation*. Sydney: Standards Australia.
- Staples, M., & Zhu, L. (2017). *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*. Canberra: CSIRO.
- Steiner, J. (2015, June 19). *Op-Ed: Blockchain Can Bring Transparency to Supply Chains*. Retrieved from Business of Fashion: <https://www.businessoffashion.com/community/voices/discussions/does-made-in-matter/op-ed-blockchain-can-bring-transparency-to-supply-chains>
- Straub, E. T. (2009). Understanding Technology Adoption: Theory and Future Directions for Informal Learning. *Review of Educational Research*, 79(2), 625 - 649.
- Swerdloff, M. (2016). Online Learning, Multimedia, and Emotions. In S. Y. Tettegah, & M. P. McCreery, *Emotions, Technology, and Learning* (pp. 155 - 174). London: Elsevier.
- The Conference Board. (2015, September). *Growth Accounting and Total Factor Productivity, 1995 - 2014*. Retrieved from Total Economy Database: <https://www.conference-board.org/data/economydatabase/index.cfm?id=27762>
- The Economist. (2015, October 31). The trust machine. *The Economist*.
- Timberg, C. (2015, May 30). A Flaw in the Design. *Washington Post*. Retrieved from http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?utm_term=.e7e945718ed7
- Transparency International. (2015). *Corruption Perception Index 2015*. Retrieved from Transparency.org: <https://www.transparency.org/cpi2015/>
- UK Government Chief Scientific Adviser. (2016). *Distributed Ledger Technology: Beyond Blockchain*. London: Government Office for Science.
- United Nations General Assembly. (2016, June 27). The promotion, protection and enjoyment of human rights on the Internet. *Human Rights Council*.
- University of Nicosia. (2017). *UNIC Blockchain Initiative*. Retrieved from University of Nicosia: <http://digitalcurrency.unic.ac.cy/>
- Ventakesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research*, 11(4), 342 - 365.
- von Weizsacker, J. (2016). *Draft Report on Virtual Currencies*. European Parliament (Committee on Economic and Monetary Affairs).
- Voros, J. (2003). A generic foresight process framework. *Foresight*, 5(3), 10 - 21.
- Wardley, S. (2017). *Future *is* predictable*. Retrieved April 4, 2017, from <http://www.wardleymaps.com/uploads/9/5/9/6/9596026/future-is-predictable-v12.pdf>
- Williams, E. F. (2015). *Green Giants: How Smart Companies Turn Sustainability into Billion-Dollar Businesses*. New York: AMACOM.
- Woo, W. (2017, March 15). *BY Critical Bug 'Damage Would Have Been in the Millions' During Fork*. Retrieved from Bitcoinist: <http://bitcoinist.com/bu-critical-bug-millions-fork/>
- World Bank. (2015). *GDP per capita, PPP (current international \$)*. Retrieved from The World Bank: <http://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?locations=AF>
- World Economic Forum . (2016). *The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services*. World Economic Forum.
- World Economic Forum. (2017, January 11). *What new technologies carry the biggest risks?* Retrieved from World Economic Forum: <https://www.weforum.org/agenda/2017/01/what-emerging-technologies-have-the-biggest-negative-consequences/>
- Zwicky, F. (1948). Morphological Astronomy. *The Observatory*, 68(845).

GLOSSARY

Anti Money Laundering and Counter Terrorism Financing

Anti-Money Laundering and Counter Terrorism Financing (AML/CTF) legislation and regulation aims to prevent money laundering and the financing of terrorism by imposing a number of obligations on the financial sector, gambling sector, remittance (money transfer) services, bullion dealers and other professionals or businesses that provide particular regulated services.

Application Programming Interface

An Application Programming Interface (API) is a technical interface to a web service or programming language library that exposes functions or methods in the interface to be able to be invoked by clients using a programming language.

Banking-as-a-Service

Banking-as-a-Service (BaaS) is an on-demand end-to-end process ensuring the overall execution of a financial service provided over the internet, often through the use of APIs.

Bitcoin

Bitcoin is a peer-to-peer payment system invented by an unidentified programmer, or group of programmers, under the name of Satoshi Nakamoto.

Block

A block in a blockchain is the container of transactions. Each block contains a timestamp and a link to the previous block.

BFT Consensus

Byzantine-Fault-Tolerant (BFT) Consensus: a mechanism for achieving fault-tolerant consensus. It has stronger consistency guarantees than Nakamoto consensus, but requires a known and smaller maximum number of participants.

Consensus

The belief held by the majority of those in the group.

Decentralised Autonomous Organisation

A Decentralised Autonomous Organisation (DAO) is a special kind of Smart Contract. A DAO is code that operates as a decentralised autonomous business model for organising both commercial and non-profit enterprises (generally in a financial way), and is designed not to have a conventional management structure or board of directors. A DAO could be considered an unincorporated association with the possibility that the curators will be held accountable for the code in the event of its failure. A specific DAO called 'The DAO' ran as an investment vehicle on Ethereum in 2016, but failed because of poorly understood smart contract code.

Digital currency

Digital currency is an Internet-based form of currency or medium of exchange distinct from physical (such as banknotes and coins) that exhibits properties similar to physical currencies, but allows for instantaneous transactions and borderless transfer-of-ownership.

Distributed ledger

A distributed ledger (also sometimes referred to as a shared ledger) is a consensus of replicated, shared, and synchronised data geographically spread across multiple parties who may be in different sites, institutions, or countries. There is no central administrator or centralised data storage. A blockchain is one type of a distributed ledger design.

Ethereum

Ethereum is a public blockchain-based distributed computing platform, featuring smart contract functionality. It provides a decentralised virtual machine, the Ethereum Virtual Machine (EVM), which can execute peer-to-peer contracts using a token called ether.

Forking

Accidental forking occurs when two blocks are generated at exactly the same moment, creating two simultaneous links in the chain. Forking is possible in the Nakamoto consensus method used in Bitcoin and Ethereum. Usually, this is resolved relatively quickly when miners converge on one block and discard the other, which becomes an 'orphaned block'.

A 'hard fork' occurs when nodes split into two or more camps, each running different software. Nodes running one version of the software cannot validate blocks created by nodes running the other version. This causes the blockchain to fork into two separate chains of transactions.

Functional requirement

In software engineering and systems engineering, a functional requirement defines the observable input/output behaviour of a system or its components, for example, calculations, technical details, data manipulation and processing and other specific functionalities that define what a system is supposed to accomplish.

Gas

As smart contracts execute, they use computational resources in many participating nodes. To limit resource utilisation and compensate for the use of these resources, some blockchains such as Ethereum charge 'gas' for the execution of smart contracts. Gas is usually paid for with the blockchain's digital currency. More-demanding smart contracts use more gas, and blockchains may impose a limit on the amount of gas that can be used per transaction or per block.

Hash

A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

Immutable

Not able to be changed. Although sometimes called immutable, distributed ledgers and blockchains are better called 'tamper evident' because attempts to enter fraudulent data change it in one location will be interpreted as an attack on integrity by other participants, and will be rejected.

Information security

Security is a collection of Non-Functional Properties, which classically include Confidentiality, Integrity, and Availability. The requirements for the security of sensitive information, as outlined in the Australian Commonwealth *Privacy Act 1988*, is covered under 1 of the 13 Australian Privacy Principles.

Internet of Things

The internet of things (IoT) refers to devices, sensors, motors, and other electronics connected to the internet. The rising rate of computational power in parallel with their falling cost foreshadows a potentially significant and increasing trend of adoption, with many billions of devices expected to be deployed in the coming years.

Know Your Customer

Know your customer (KYC) is the process of a business identifying and verifying the identity of its clients. The term is also used to refer to the bank regulation which governs these activities.

Know Your Customer's Customer

Know your customer's customer (KYCC) takes these requirements to the next level in exploring who your clients are doing business with, their source(s) of funds and its legitimacy, and the risk that these third parties are laundering money or financing terrorism.

Know Your Device Thing

Know Your Device (or Know Your Thing) refers to the process of identifying individual mobile devices, and confirming the integrity of its configuration state, through their unique attributes.

Miner

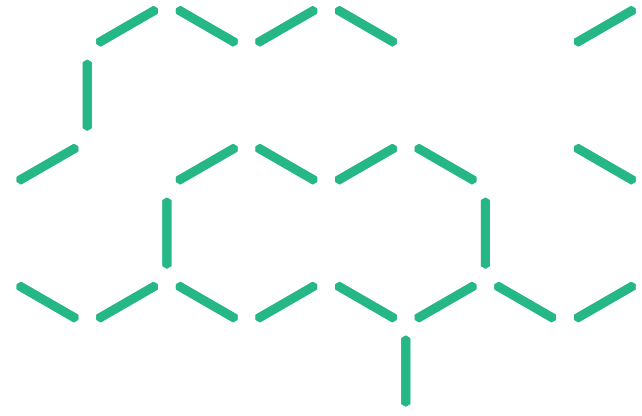
In a proof-of-work blockchain, the processing nodes which collectively operate the blockchain are known as miners.

Nakamoto Consensus

The Nakamoto Consensus mechanism is used in Bitcoin and other blockchain systems. When there are multiple alternative versions of the blockchain ledger, the Nakamoto Consensus mechanism favours the longest chain.

Non-Functional Property

Non-Functional Properties are criteria that can be used to judge the performance of a system, and include performance, scalability and security.



Non-Functional Requirement

In systems engineering and requirements engineering, a non-functional requirement is a requirement for a Non-Functional Property. These requirements specify criteria about the performance of a system. They are contrasted with functional requirements.

Non-Repudiation

The inability to deny a previous claim. On a blockchain, the immutability of historical transactions which are cryptographically signed means that there is always strong evidence that those transactions were performed by someone with control over those cryptographic keys.

Nostro/Vostro accounts

Conventionally, a bank does not have a ledger jointly shared with another bank. Instead they create internal accounts intended to mirror the accounts held at the other bank. The other bank holds dual sets of accounts, and these 'nostro/vostro' accounts can be periodically reconciled to check and maintain consistency between the two banks. A jointly shared distributed ledger, perhaps implemented using a blockchain, is an alternative to this conventional approach.

On chain off chain

An on-chain transaction is simply a blockchain transaction. An off-chain transaction is the movement of value or information outside of the blockchain – for instance, the third-party website Coinbase enables off-chain Bitcoin transactions between user accounts. Consequently these off-chain transactions do not incur mining fees, and avoid the verification waiting times associated with on-chain transactions. Off-chain transactions are sometimes suggested to improve performance for system limitations. These claims should be investigated on a case-by-case basis.

Oracle

Oracles know something (for example about some event or activity, perhaps the location of a shipment) and always speak the truth (or in other words, provide correct and reliable answers when asked). In terms of a distributed ledger, an oracle could be a trusted source that provides data recorded on the ledger (and potentially used in the execution of smart contracts).

Privacy

Privacy can be divided into a number of separate, but related, concepts:¹⁵⁵

- **Information privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as 'data protection'.
- **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches
- **Privacy of communications**, which covers the security and privacy of mail, telephones, e-mail and other forms of communication
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

The Australian Privacy Principles in the Australian Commonwealth *Privacy Act 1988* refer to the protection of sensitive information, which is a type of personal information and includes information about an individual's:¹⁵⁶

- health (including predictive genetic information)
- racial or ethnic origin
- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal record
- biometric information that is to be used for certain purposes
- biometric templates.

155 Australian Law Reform Commission, 2008

156 Office of the Australian Information Commissioner, 2017

Proof of Concept

Proof of concept (PoC) is a realisation of a certain method or idea in order to demonstrate its feasibility or a demonstration in principle with the aim of verifying that some concept or theory has practical potential.

Proof of Stake

A proof-of-stake (PoS) is a type of consensus protocol used by blockchain systems, where the probability of mining a block is dependent on how much digital currency is controlled by the miners.

Proof of Work

Proof-of-work (PoW) is a type of consensus protocol used by blockchain systems, where the probability of mining a block is dependent on how much work is done by the miners.

Private Key

See Public Key.

Public Key

In cryptography a public key is a published number which is used as a parameter in an encryption function, to encrypt and check signed messages. Public keys are paired with secret private keys, which are used to decrypt and sign messages.

Regtech

RegTech is the use of technology to more effectively and efficiently manage regulatory monitoring, reporting, and compliance. The four key characteristics of RegTech are: agility, speed, integration and analytics.

Scenario

Scenarios are a tool for arranging arguments for alternative future environments that will be influenced by decisions made today. They are evidence-based stories about the future with implications for present-day decision making.

Sharding

Sharding is a technique of breaking apart a database into separate independent pieces. If the pieces are truly independent, they can be processed concurrently, which can significantly increase the throughput of the overall system, although performance gains for blockchains are sublinear at best.

Smart contract (blockchain)

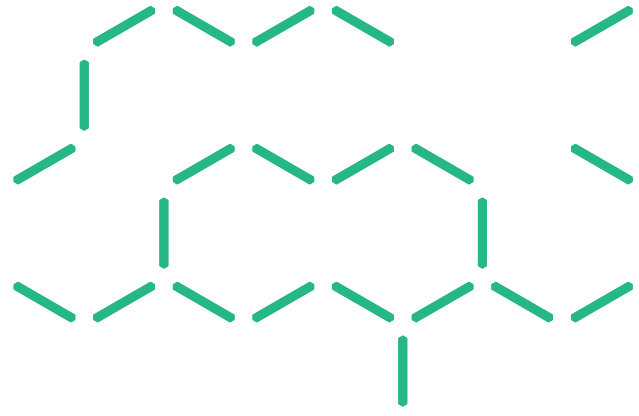
In blockchain technology, a smart contract is computer code stored on the blockchain ledger and able to execute as part of a transaction's validation on the blockchain. Usually this would be to enter its own transaction recording the occurrence, or non-occurrence, of an event, essentially monitoring the performance of a contract. In addition to executing the logic encoded in the program, smart contracts can carry digital currency or control access to other digital assets or tokens recorded on the blockchain. Some blockchains allow smart contracts to be arbitrary Turing Complete programs, while other blockchains only allow more limited programs

Smart contract (legal informatics)

Smart contracts are computer programs that facilitate, verify, or enforce the negotiation or performance of a legal contract. They are not necessarily recognised at law as legal contracts.

State channels

State channels are a design pattern for the use of smart contracts to adjudicate on the completion of an off-chain protocol. Participants first jointly commit to this smart contract. Then they exchange a series of messages off-chain which may be too confidential or rapid or large to perform on the blockchain. The final state of the off-chain exchange is submitted back to the smart contract, which resolves final exchange of assets on the blockchain

**Trusted**

In dependable systems, being trusted means being relied upon to achieve some purpose.

Trustworthy

In dependable systems, being trustworthy is the quality of having good evidence for being dependable.

Turing complete

In computability theory, an instruction set or a programming language is said to be Turing Complete or computationally universal if it can simulate a Turing machine. The Church-Turing thesis is that all such languages have equivalent computational power.

Use case

In software and systems engineering, a use case is a list of actions or event steps, typically defining the interactions between a role (or actor) and a system, to achieve a goal.

Zero knowledge proofs

Zero knowledge proofs or methods prove to one party (the verifier) that a given statement about another party (the prover) is true, without conveying any additional information other than that the fact is indeed true.

CONTACT US

t 1300 363 400
+61 3 9545 2176
e csiropenquiries@csiro.au
w www.data61.csiro.au

WE DO THE EXTRAORDINARY EVERY DAY

We innovate for tomorrow and help
improve today – for our customers,
all Australians and the world.

WE IMAGINE
WE COLLABORATE
WE INNOVATE

FOR FURTHER INFORMATION

Rob Hanson MA MSc BBus CISA CISM CRISC CRMA
Senior Research Consultant
t +61 2 6216 7028
e rob.hanson@data61.csiro.au
w www.data61.csiro.au

