The future of privacy: Applying distributed ledger technology for security and privacy in the cloud
Assessment Task 4: Final Report

Blog address: https://www.julio11706159capstone-project.delcorpdata.com/

Video file: https://youtu.be/FaO0-Xw63_0

Julio Del Cid (Student 11706159)

School of computing, mathematics, and engineering, Charles Sturt University

ITC571 Emerging Technologies and Innovation

Dr Mohsin Iftikhar

15 October, 2021

The future of privacy: Applying distributed ledger technology for security and privacy in the cloud

Julio Del Cid
School of computing, mathematics, and
engineering of ITC571 Emerging
Technologies and Innovation.
Charles Sturt University
Albury-Wodonga, Australia
julio@delcorpdata.com.au

***Abstract*— Lack of privacy and security of personal identifiable information (PII) in the cloud is fueling cybercrimes such as extortion where only a small number of global citizens have the right of online privacy via lawful means. Distributed ledger technology (DLT) has shown promise which may solve PII security and privacy issues. However, the application of this emerging technology is often incorrectly referred to as blockchain which, may lead to organisations applying the wrong DLT solution resulting in misconfigured software, breaches, and application of smart contracts, dumb ideas. This paper categorises popular DLT applications such as blockchain, digital rights, smart contracts, decentralised autonomous organisations (DAO) applied to real world use cases. This paper can be the commencement of a reference model for technical staff planning to apply DLT similar to the popular blockchain decision tree.**

Keywords—privacy and security in blockchain, cloud security, Hyperledger, distributed ledger technology (DLT), API driven privacy

I. INTRODUCTION

The use of blockchain technology and its current category being distributed ledger technologies will all be interchangeable terms. Although the original blockchain developed form the Satoshi Nakamoto's paper is now referred to blockchain version 1.0 we will refer to all blockchain technology and their derivatives as DLT.

This paper examines the use of DLT technologies in the cloud, meaning applications are applied to both private and public cloud providers with the distinction they all traverse the open web for peer-to-peer communications. This paper applies the use of many forms of DLT from private, public, hybrid and consensus DLT which simply means a converged DLT network.

Security situation and DLT benefits. The situation being the Covid-19 pandemic it is reported we have lost our privacy[1] faster than expected. This has led to reclaiming our privacy and strengthening security by the use of DLT, which is well-known for its strong encryption and anonymity features. The application of such a technology to preserve confidentiality, integrity, and availability (CIA) of information [2] is the aim of this report. However as implementors of such as technology, practitioners and managers need to be careful when implementing the technology as human error usually leads to vulnerabilities.

Ethical implications. The premise of this paper is about the lack of privacy and surveillance big tech firms have over its users. Surveillance has recently being used to profit and aid other motives such as capitalism, political influence, and many other crimes such as extortion over PII[3].

Data being sold by the big tech firm such as social media giants, is an immensely profitable business coined surveillance capitalism coined by Zuboff [4] which in the European Union has been regulated by the introduction of the General Data Privacy Regulation (GDRP) policy [5] should be managed by the data owners such as the users. This paper explores how DLT is enabling a new private and secure future built on DLT.

Lastly, a brief mention of what this paper is not. It does not explain the technology, how blockchain works in a technical manner as we assume you have an underlying knowledge of the main way blockchain technology works.

II. RESEARCH QUESTIONS & METHODOLOGY

A. Research Questions

What is the problem to be solved? The problem to be solved is bringing attention to the misapplication of blockchain technology [6] as an all-in-one solution to online security and privacy. Contraventions of Confidentiality, Integrity, and Accessibility (CIA) in information security is fuelling cybercrimes especially in the health sector where handling Personable Identifiable Information (PII) is commonly mismanaged [3].

Stakeholders who should care are the ones who are negatively impacted by breaches of sensitive information which if CIA is breached may cause harm to themselves. The secondary layer of stakeholders are the ones who may have contributed to the mishandling of any sensitive information. These stakeholders known as data owners have the legal responsibility to minimise harm with the added legal burden to notify the affected individuals else face legal consequences.

Existing research regarding the application of DLT is limited as the relatively new emergence of DLT is in its infancy. Limited amount of research has been conducted regarding the application of the appropriate DLT solution to a firms need. In terms of security there has been plenty of security frameworks used in industry such as the National Institute of Standards and Technology (NIST) cyber security framework, the Health Insurance Portability and Accountability Act (HIPAA) which directs healthcare professionals what needs to be protected. Chowdhury et al created a blockchain decision tree for anyone which is contemplating the use of a blockchain technology[7], Fig.1. which is used in this paper as an initial step. Following the initial decision to use blockchain for a solution, we guide the reader to other decisions such as the type of DLT software, the maturity level and finally the security and privacy applications.

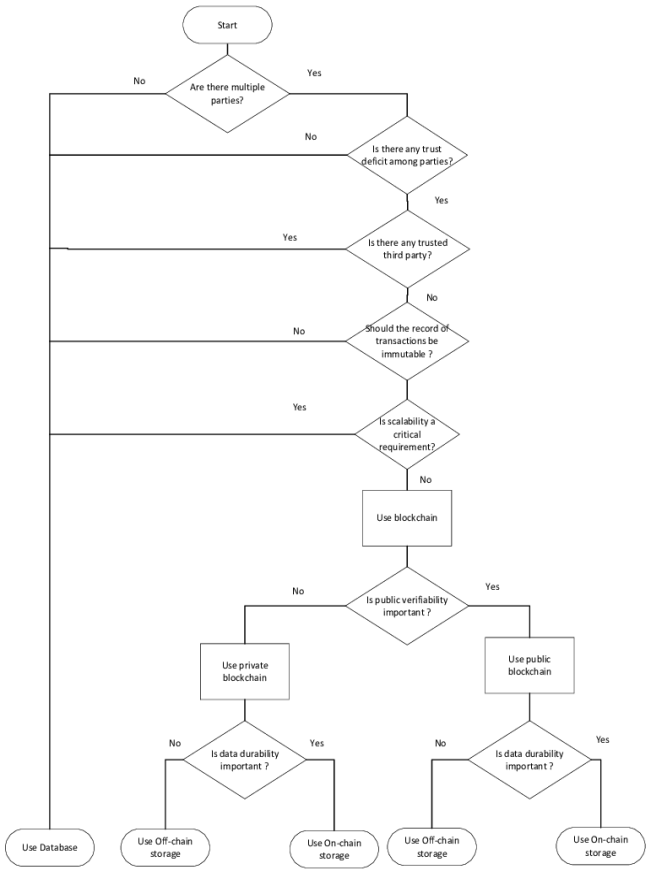

Fig. 1 Blockchain decision tree

The blockchain decision tree displays how this single DLT technology can be applied and which fails to consider other DLTs such as DAOs and smart contracts and makes no mention of how digital rights can be preserved.

Further problems with each of the methods above is that it is highly technical process and usually still requires highly skilled personnel with deep domain specific technical knowledge such as information security management, DLT, software engineering to name a few.

The solution proposed is to create a simple reference table which can be assessed by both technical and non-technical staff as an initial point of discussion to decide whether a DLT should be applied of would it be feasible to use existing well-known technology.

B. Theoretical Framework

Osterland and Rose [8] in their publication entitled From a Use Case Categorization Scheme Towards a Maturity Model for Engineering Distributed Ledgers outline a satisfactory comparison model of the different DLT technologies and categorises their findings within what they have observed. The shortcomings are the paper is very scientific out of practical reach for non-technical people who can at a glance explore a particular DLT. Their categorisation also seems to be one domain oriented which means they have one main use for blockchain in finance but fail to discuss growing areas of valid uses such as supply chain goods, medical goods and property documentation. Extraction of particular parts of the paper will be necessary such as the suggested categorisations of different DLTs.

The cyber decision tree by Chowdhury (2018) in Fig.1 simplifies the process of deciding if a blockchain technology is required. which Li et al [9] attempts to extend to include various DLT technologies. The problem with these decision trees it still does not suggest a particular DLT for a particular use, for example preserving digital rights is best handled by Non-Fungible Tokens (NFT), connecting both public and private blockchain interests are handled by the Hyper ledger project, and the list continues to grow on a daily basis. A proposed flow chart will be adopted to allow managers to make decision of the type of DLT and weigh up each benefit and advantage for their use case.

The conceptual framework suggested in this paper is one that categories the users implied needs for a DLT in to three categories. The DLT categories are permissionless, permissioned, and hybrid [10] and in 2021 Wegrzyn et al, [11] adds a fourth category which is a converged DLT referred to as a consensus DLT. Each category will have suggested latest novel solutions with risk and benefits of each technology. The conceptual framework suggested will follow a three step process asking. 1) Do you need a DLT solution? 2) If yes, what DLT technologies are suitable? And 3) What are the security and privacy considerations for a DLT solution.

The third stage being resources needed for each DLT solution may need to be further explored in a subsequent research paper.

C. Project Plan

The adoption of blockchain technology is growing every day, with eagerly first adopter applying blockchain technology incorrectly leaving security gaps open for exploitation. The main beneficiaries of this research are managers who have the decisive powers to apply certain technologies as their entities require which result in safer applications of appropriate DLT solutions to fitting use cases. The objective of this paper is to bring attention to different types of DLT and their uses which may foster further research and development in the DLT space.

III. METHODOLOGY

The research method applied is qualitative based on previous cases studies. Qualitative research method has been chosen due to a short timeline being ten weeks and no allocated budget. Majority of sources of information has been selected from peer-reviewed journals, reputable scientific and industry sources.

A. Prior work on distributed ledger technology

DLT has been popularised by its predecessor blockchain which was popularised by recent cryptocurrency trend made famous by a Bitcoin whitepaper explored further in this document. However DLT and blockchain technologies have been around since the fifties. Hashed chained tables also known as linked lists were first developed in 1956 [12] for the RAND corporation. Prior to this an IBM memorandum by Hans Peter Luhn [13] suggested storing text and numbers in hashed tables, whom can be credited with the latest hashing algorithm and linking information together. Another milestone in distributed computing came by the creation of IBMs virtual machines [14]. Campbells seminal piece created the pathways for Virtual Private Networks (VPNs) to be commonly accepted information technology (IT)

infrastructure and with the Sales Force offering a mass market customer relations management application over the internet which solidified distributed computing as an efficient way to perform business transactions.

B. Modern work on distributed ledger technology

We consider the term modern being the last twenty years since 2001 with many advancements made in cloud computing after the year 2000. A seminal piece to DLT is the work following a general distrust in financial institutions post global financial crisis is a whitepaper entitled Bitcoin: A Peer-to-Peer Electronic Cash System [15]. This highlighted a way to decentralise incorruptible information, which increased the integrity of information which grew into the latest blockchain movement with many citations related the term blockchain in a public ledger. Recently in 2016 the UK Government published Distributed Ledger Technology: beyond block chain (Distributed Ledger Technology: beyond block chain, 2016) [16] a report by the UK Government Chief Scientific Adviser looks beyond the capabilities of the blockchain and explores areas this paper will delve into.

The momentum is growing by industry, government and individuals.

IV. Results

The rise of all DLT related technologies continues to grow. The latest emergence is the ownership rights of artists with artists utilising Non-Fungible tokens (NFT) to verify and sell their unique work.

According to a publication by the Australian Government department of Department of Industry, Science, Energy and Resources (DISER) reported that blockchain related technology is forecasted to grow at yearly commercial value of over US$175 billion by 2025 and in excess of US$3 trillion by 2030 [17].

The pace of the growth in this technology is significant and with it comes speed to market actors which will prefer speed over security which opens vulnerabilities of the DLT.

Security breaches have risen on a month-by-month basis since the introduction of the mandatory data breach regulation introduced by the Government. Fig. 2 [18].

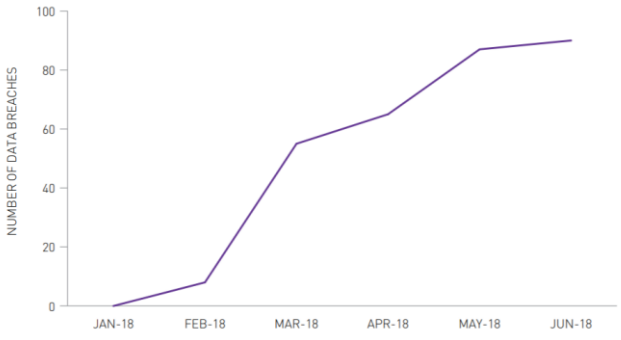

Fig 2. Initial reports by the Australian Computer Society shows data breaches in Australia show an upward trajectory.

The pace of the growth in this technology is significant and with it comes speed to market actors which will prefer speed over security which will undoubtedly face security vulnerabilities of the DLT.

V. Discussion

The research questions asked earlier are answered in the following sections entitled by the question.

A. Question one: Do you need a DLT solution?

To determine if you need a DLT solution, follow the blockchain decision tree in Fig 1, if the result ends in a yes proceed to question two.

B. Question two: What DLT options are suitable?

As of this writing there is a large emergence of new applications of the DLT, the main DLT options fall under four categories seen in Table 1.

TABLE 1.

TYPES OF DLT

Type #	Type Name	Description
1	Public or Permissionless	Public facing where anyone can join and access all data on the DL
2	Private or Permissioned	Private with permissions required to access some or all data on the DL
3	Hybrid	Combines the two above
4	Consortium	Is a collection of two or more permissioned DLs. The consortium refers to a group of members who manage the permissioned/private DL

Commercial applications of the DLTs are growing rapidly, Table 2. below notes the currently trending and established applications published by the Blockchain Council [19].

TABLE 2.

APPLICATION OF DLT

DLT	Use	Type name	Description	Year started
Crypto currency	Medium of exchange	Pub	Is a collection of binary data designed to be store of value such as traditional currency	1983
Corda	Smart contract	Pub	Is built on the Ethereum blockchain which connects other applications	2016
Blockchain	Protocol	Pri	Is a form of Merkle tree data structure	1992
Smart contract	Smart contract	Pri	Automatically execute, control or document events and data on the DLT	1990
Bitcoin	Medium of exchange	Pub	Is a peer-to-peer network of a digital decentralised currency	2009
Polygon framework	Smart contract	Cons	Is a multi-chain system built for the Ethereum network	

DeFi	Decentralised Finance	Cons	Smart contracts used to connect lender and borrower as an intermediary	2017
Non-Fungible Token	Ownership rights	Pub	Uses the Ethereum blockchain to store digital rights on a digital asset	2015
Ethereum	Blockchain protocol	Hyb	Is a decentralised blockchain protocol with smart contract functionality	2015
UniSwap	Decentralised Finance	Pub	Is a decentralised financial where banks are replaced with smart contracts	2018
Solidity	Programming language	NA	Is not a DFT, but a programming language derived from JavaScript, Python, and C++ to program Ethereum based contracts and applications	2014
Hyperledger	Blockchain protocol and smart contract	Hyb	Linux Foundation project with industry contributions by IBM, Intel, SAP Ariba designed to build a multi-purpose blockchain protocol to create smart contracts and applications	2015

Table abbreviations: Public as "Pub", private as "Pri", consensus as "Cons", hybrid as "Hyb", and not-applicable as "NA".

C. *Question three: What are the security and privacy considerations for a DLT solution?*

The cryptographic benefits of storing data in highly secure DLT is well documented as DLT is based on cryptographic asymmetric algorithms to encrypt data. To reverse or unlock the encrypted data with the original value is easy, however if someone does not have the original key value, they are forced to use a brute force approach to find all the possible values to break the algorithm. Searching for all possible combinations on a typical secured asset is known to have a time complexity of order factorial to the nth number O(n!)[20]. Just for context attempting to brute force attack on Secure hashed Algorithm shortened to SHA. A brute force attack on a SHA-256 bit will take millions of years to break, making the task unfeasible for any attacker.

Vulnerabilities in cryptography lay in the human errors such as misconfigured DLT applications, human error, business flaws, and coding errors in the DLT software.

D. *Security in the cloud*

It needs to be stated immediately what it means to be secure in the cloud by explaining the shared responsibility model. Figure 3 showing two separate areas, customer and vendor responsibilities. It is the customers responsibility which has the most vulnerabilities as the customer may lack the adequate training, skillset or other issues. Shared responsibilities seen in Fig. 3.

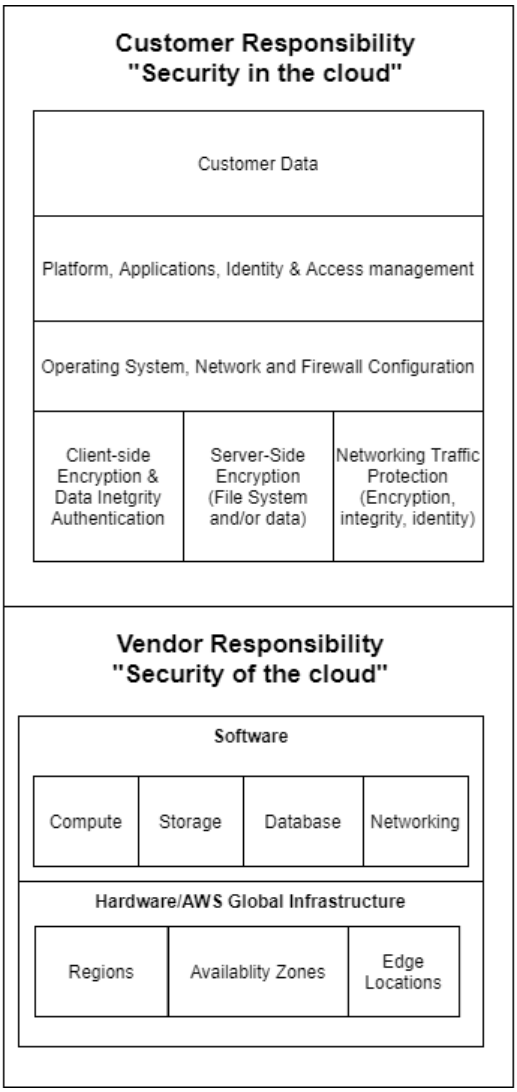

Fig 3. A common shared responsibility model used by cloud vendor providers.

E. *Security of the blockchain on cloud provider platforms*

Vendors will prescribe methods to secure the blockchain will be provided for by the cloud provider, with the main responsibility falling on the entities who implemented the DLT initiative on a chosen platform.

Many large vendor providers will provide their own prescriptive advice, usually based on certain security frameworks such as NIST, Payment Card Industry Data Security Standards (PCI-DSS), HIPPAA and other compliance frameworks depending on the industry.

An example of vendors applying security to a DLT platform is Amazon Web Services (AWS) who offer a blockchain platform-as-a-service in their infrastructure. The approach AWS takes is to advise their users to follow the well-architected framework in particular the security pillar [21].

F. *User responsibilities*

In an organisation there are many users, from directors to end-users. For this paper we define two types of users: technical and non-technical with distinct responsibilities.

TABLE 3.

TYPES OF USERS

User	Title	Department	Roles and responsibilities
Type 1: Non-Technical	DLT Administrator	Managerial	Non-technical and general user administrator controls such as allow people access to a DLT network
Type 2: Technical	DLT Systems Security Engineer	Engineering	Technical such as software engineering tasks, implement security controls, and development. Is responsible for applying security to the DLT.

Type 1 user: Non-technical. A non-technical user can be expected to take care of security mechanisms which are usually part of any corporate security policy. These general security policy guidelines cover the basics such disallowing passwords sharing, mandate two-factor authentication, password strength, and other controls. As a DLT administrator they are expected to follow the items below at a minimum to protect the Public Key Infrastructure (PKI). Fig 4. Shows the interaction between users.

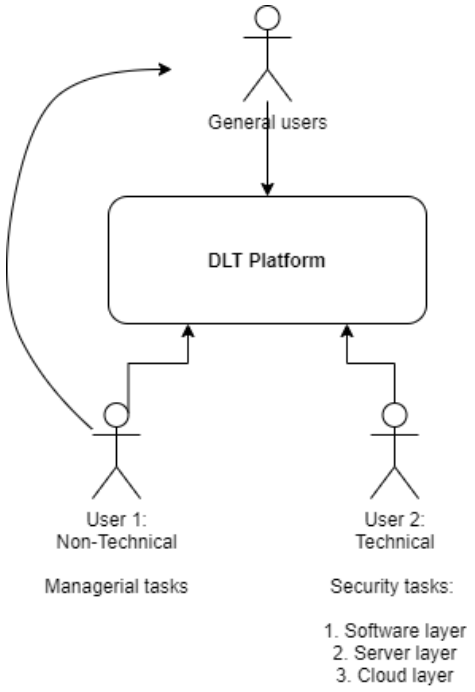

Fig 4. The two main users for an organisation to implement DLT are technical and non-technical administrative users.

TABLE 4.

USER TYPE 1: NON-TECHNICAL RESPONSIBILITIES

Security Measure	Risk
Check digital signatures	Check the authenticity of all incoming and outgoing certificates below allowing access
Securing private keys	Revealing private keys will mean someone can command control the entire DLT system, which is at the highest level of severity
Store physical devices safely	Two factor tokens, digital wallets, and anything else must be maintained physically safe
Knowing the exchanges	Exchanges are another way to say servers. Servers could be the weakest link, with outdated software, deprecated operating systems, unpatched systems and more. Noticing if there are web applications weaknesses is important such as using the OWASP Top 10 to determine the basic security of exchanges. Independent penetration testing is an important step to assess the security posture.
Non-technical security risks	The above risks need some form of security investment and managerial decisions could lead to applying security controls as a matter of urgency.
	Un-regulated environment, remember peer-to-peer networks such as the one DLT lives on are unregulated. Applying policies and security mechanisms can help, but when cross border peers do the wrong thing. This could be a problem very hard to eradicate.

Type 2 user: Technical. As seen from figure X. It is the users responsibilities to take care of the application in the cloud. The following security controls are applied in three layers, the ssoftware plane, server plane, and cloud vendor plane.

Software plane. The software development department has the best way to decrease any errors. These can be handled by using established secure software protocols as per the Carnegie Mellon University (CMU) [22] secure coding practices, see table 5.

TABLE 5.

SOFTWARE SECURITY METHODS

Practice	Description
Validate inputs	Validate inputs from all sources, trusted and untrusted. Eliminate Command Line Interface (CLI) instructions, network interfaces, and other instructions which may be executed in the operating system.
Heed computer warnings	Take actions of the errors raised in coding environments. Use software analysis tools such as Interactive Application Security Testing (IAST) as it tests dynamic and static components.
Architect and design for security policies	Plan the software at a high level with security in mind.
Keep it simple	Keep the design as simple as possible as complexity adds likelihood for extra bugs.
Default deny	Is another way of saying, zero trust. With a firewall approach, deny all unless explicitly allowed.
Apply principle of least privilege	All process should execute their tasks with the least resources to achieve the task.
Sanitise data before sending	Make sure systems talking to each other have sanitised data as subsystems may not know why certain calls are being made.
Practice defense in depth	Applying security in multiple layers will assist any shortcomings.
Use of effective quality assurance techniques	Test the robustness of the previous approaches by testing the application. Such tests include, fuzzing, pen-testing, and source code audits.

Adopt a secure coding standard	Develop a culture of securing your code as recommended by the language.
Define security requirement	Document bugs through a risk register and make sure they are handled before further iterations.
Model threats	Anticipate what attackers will do and the threats the application will be subjected to. Independent security companies can develop threat attacks and should provide ways to remedy the problem.

Although the Open Web Application Security Project (OWASP) security protocols are similar, we did not emphasises as much as the CMU as some applications are native which are coded in different languages such as Apples iOS mobile operating system and Google Android mobile platform to name some examples.

The server layer. All users need to download software or interact with a server at least once. The term servers and exchanges are interchangeable in this document, but in the practice they server different functions. The following security guidelines are provided by the Security Cloud Alliance (CSA)[23].

TABLE 5.

SERVER/EXCHANGE SECURITY METHODS

Security Control	Description
Apply Distributed Denial of Service attack protection	DDoS prevents accessibility to the DLT assets.
Apply Cross-Site-Scripting (XSS) protection	Websites which may be subjected to manipulation of data is an integrity attack.
Do not expose server information	Revealing server information is release of confidential information which usually leads to reconnaissance.
Apply web application firewalls	Protects web infrastructure from various attacks.
Database firewall	Centralised sources for DLT software, company information, and other log data is usually held in a centralised source.
Third-party components and patch	Supply chain attacks occur from installing external components with vulnerabilities.
HSTS (HTTP Strict-Transport-Security) and Secure Sockets Layer (SSL)	Applying a strict only HTTPS encrypts all traffic data
Apply machine learning for better protection	Assisting system operators with machine learning (ML) can help operators 24/7
HTTP Public key pinning	Basically dedicates only one IP for specific actions, such as accessing patch updates. Prevents man-in-the-middle (MIITM) attacks
Use hardware security module (HSM) enabled wallets	Similar to multifactor-authentication but uses microchips to reveal one-time-passwords (OTP) to the requesting DLT
Deploy a zero trust architecture	Applies a deny-all by default unless access is allowed
Error handling	Do not display errors to the users, as this can reveal server information
Apply two factor authentication (2FA)	Adding one extra layer of security increases the security posture
51% attack prevention	Miners who hold more than 51% of the assets can control the entire DLT ecosystem.
Cloud service security protection	Use the vendors recommended security practices

The cloud layer. Security of DLT in cloud providers is the same as taking care of other applications which reside in the vendors infrastructure. A sample of a leading cloud vendor is Amazon Web Services (AWS) security recommendations below.

TABLE 6.

VENDOR SECURITY METHODS

Security control	Description
Implement a strong identity	Implement a zero-trust posture
Enable traceability	Add the ability to monitor, audit and alerts
Apply security at all layers	Apply a defense in depth approach.
Automate security best practices	Automatically patching and detecting insecure mechanisms keeps your security posture strong.
Protect data in transit and at rest	Classification of data in tiers and pair with encryption, tokenisation, and access control for appropriate security
Keep people away from data	Keep a zero trust policy to avoid mishandling data both intentionally and unintentional
Prepare for security events	Incidents do happen and been prepared for breaches is a sound practice

G. Privacy and DLT

Suspicions of genuine privacy over a distributed ledger may arise suspicions but it not only immediately achievable but paves the way for the future of privacy. It all depending on the type of DLT and its configurations privacy is possible.

Privacy and DLT merge well with algorithms being the strongest point and anonymity being a strong point of bitcoin, a popular blockchain. Distinction between privacy and anonymity is that privacy is where an individual wishes to keep their documents private and can only be seen by authorised parties, where anonymity is where users are unknown. Depending on the design and requirements of entities, privacy can be applied in several ways. Below we present two methods.

Privacy method 1: Using a VPN in a hybrid DLT. Method 1 is for practical and immediate use for corporate settings, by the use of existing infrastructure such as Virtual Private Network (VPN).

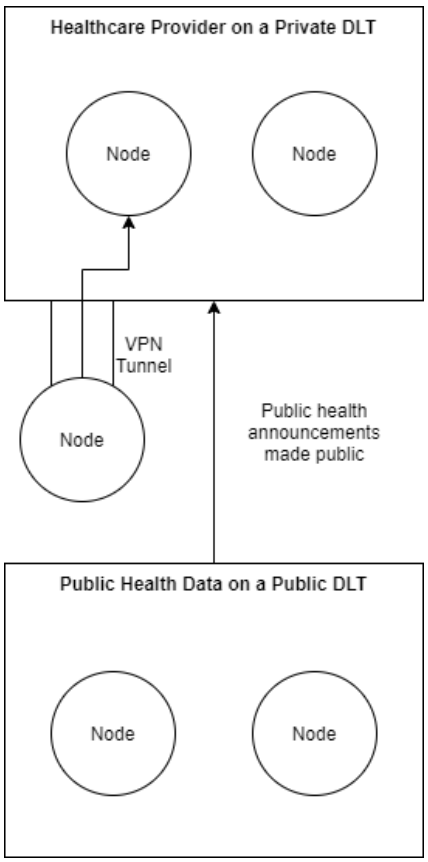

Fig 5. Example of a node accessing through a VPN.

This is applicable to hybrid blockchains as the VPN tunnel component will not conflict with the underlying DLT architecture.

Privacy method 2: Using a policy driven DLT and APIs. The second method is one driven by a user's policies and Application Programming Interfaces (APIs). This method gives the power to the user who owns their data to declare who has what files and can also revoke access at any given moment, which is showing great momentum.

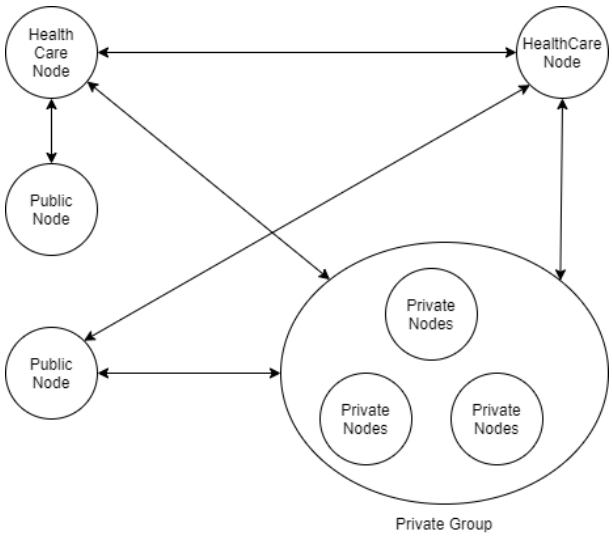

Fig 6. The diagram shows different entities sharing different information to different parties.

All modern applications are developed using APIs underwritten by policies written in well-known formats such JavaScript Object Notified (JSON).

Use of JSON Web Tokens. The use of JavaScript Object Notified (JSON) Web Tokens known as JWT are already in use in the industry to secure APIs. A sample of the JWT token call can be seen below:

Sample of a JWT token. JWT tokens have been used in the industry since 2015 [24] and offers security for APIs. Below is an example of a typical JWT call between two interfaces. Fig.7.

```
Encoded: 75734c21ea0d39fb7565e0f6a5611f8095e7211ea03a7e08d1ccb58a2dfa175a
Decoded:
Header: Algorithms and token type
{
        "alg": "SHA-256"
        "typ": "JWT"
}
Payload Data
{
        "full name": "Julio Del Cid"
        "record type": "Health record"
        "permission": "read only"
        "Entity": "Victoria Health Department"
        "Expiry": "UTC:12:00:00"
}
```

Fig 7. JSON Code of a JWT transaction.

CONCLUSION

The field of privacy is one that is highly contested, and to date there has not been a huge take-up of any privacy solutions offered without users relinquishing access to people favourite applications.

Security of the private and sensitive data in Australia needs to be a government issue as it is in the European Union with the General Data Protection Regulation (GDPR) regulation. It has been seen that as privacy currently sits corporations are taking advantage of users privacy referred to as surveillance capitalism.

Users should not wait for government intervention as this may never arrive, open privacy protocols which can allow users to genuinely own their data and not the other way. There are some exciting developments in the field of privacy and security mostly coming form joint efforts be the likes of the Linux Foundation with industry giants backers such as IBM, Intel and SAP Ariba with hybrid DLT technologies.

Further research required regarding the actual development of the DLT flowchart needs to be developed to mature levels[25]. Further developments outside of this papers scope are digital rights and privacy laws to accommodate DLTs, industry needs to develop open privacy protocols, and finally software development compatibility. Popular software development languages and frameworks to include DLT protocols to be compatible with DLT developments. In other words for this space to truly to grow, allow software developers to use their preferred languages.

REFERENCES

[1] Sharma, T. and Bashir, M., 2020. Use of apps in the COVID-19 response and the loss of privacy protection. Nature Medicine, 26(8), pp.1165-1167.

[2] Lundgren, B. and Möller, N., 2017. Defining Information Security. Science and Engineering Ethics, 25(2), pp.419-441.

[3] Ibarra, J., Jahankhani, H. and Kendzierskyj, S., (2019). Cyber-Physical Attacks and the Value of Healthcare Data: Facing an Era of Cyber Extortion and Organised Crime. Blockchain and Clinical Trial, pp.115-137. https://doi.org/10.1007/978-3-030-11289-9_5

[4] S, Zuboff. (2019). The age of surveillance capitalism. The fight for a human future at the new frontier of power. Profile books.

[5] Patil, V. and Shyamasundar, R., (2018). Efficacy of GDPR's Right-to-be-Forgotten on Facebook. Information Systems Security, pp.364-385. https://doi.org/10.1007/978-3-030-05171-6_19

[6] O'Hara, K., 2017. Smart Contracts - Dumb Idea. IEEE Explore. https://doi.org/10.1109/MIC.2017.48

[7] Chowdhury, M., Colman, A., Kabir, M., Han, J. and Sarda, P., 2018. Blockchain Versus Database: A Critical Analysis. IEEE Xplore. http://dx.doi.org/10.1109/TrustCom/BigDataSE.2018.00186

[8] Osterland, T. and Rose, T., 2020. From a Use Case Categorization Scheme Towards a Maturity Model for Engineering Distributed Ledgers. Progress in IS, pp.33-50.

[9] Li, J., Greenwood, D., & Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. Automation In Construction, 102, 288-307. https://doi.org/10.1016/j.autcon.2019.02.005

[10] Youm, H., & Hurwitz, S. (2021). Technical Report FG DLT D1.2 Distributed ledger technology overview, concepts, ecosystem. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf

[11] Wegrzyn, K. E., & Wang, E. (2021). Types of Blockchain: Public, Private, or Something in Between. Newstex.

[12] Bays, C., 1973. Some techniques for structuring chained hash tables. The Computer Journal, 16(2), pp.126-131.

[13] Stevens, H. (2018). Hans Peter Luhn and the Birth of the Hashing Algorithm. https://spectrum.ieee.org/hans-peter-luhn-and-the-birth-of-the-hashing-algorithm

[14] Campbell, G. (1976). Use of virtual-machine commands in digital simulation. SIMULATION, 26(6), 198-198. https://doi-org.ezproxy.csu.edu.au/10.1177/003754977602600607

[15] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved 20 August 2021, from https://bitcoin.org/bitcoin.pdf

[16] UK Government. (2016). Distributed Ledger Technology: beyond block chain. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[17] 2019. THE NATIONAL BLOCKCHAIN ROADMAP: Progressing towards a blockchain-empowered future. 1st ed. [ebook] Canberra: Australian Government. Available at: https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf .

[18] 2021. Blockchain 2030 A Look at the Future of Blockchain in Australia. 1st ed. [ebook] Australian Computer Society (ACS). Available at: https://www.acs.org.au/content/dam/acs/acs-publications/ACS-Data61-Blockchain-2030-Report.pdf

[19] Blockchain-council.org. 2021. Blockchain Certifications. [online] Available at: https://www.blockchain-council.org/blockchain-certification/

[20] 2021. the Big O Notation. 1st ed. [ebook] Massachusetts Institute of Technology (MIT), p.1. Available at: https://web.mit.edu/16.070/www/lecture/big_o.pdf

[21] Docs.aws.amazon.com. 2021. Security Pillar - AWS Well-Architected Framework - Security Pillar. [online] Available at: https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html .

[22] Wiki.sei.cmu.edu. 2021. Top 10 Secure Coding Practices - CERT Secure Coding - Confluence. [online] Available at: https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices

[23] 2021. Crypto-Asset Exchange Security Guidelines. 1st ed. [ebook] Available at: https://cloudsecurityalliance.org/artifacts/csa-crypto-asset-exchange-security-guidelines-abstract/

[24] Datatracker.ietf.org. 2021. rfc7519. [online] Available at: https://datatracker.ietf.org/doc/html/rfc7519 .

[25] Taylor, P., Dargahi, T., Dehghantanha, A., Parizi, R. and Choo, K., (2020). A systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2), pp.147-156. https://doi.org/10.1016/j.dcan.2019.01.005