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

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

Julio Del Cid

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

ITC571 Emerging Technologies and Innovation

Dr Mohsin Iftikhar

07 September, 2021

Article #1

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

The article proposes an alternative financial system which is based on a decentralised peer-to-peer electronic cash system without the need of a centralised financial system. The proposed financial cash system is designed to be built on a hashing algorithms, designed to avoid possible problems such as double-spending by time stamping each transaction and publishing transactions on a public distributed ledger. **In particular**, these concepts include a node network with each node representing individuals with computer processing units (CPU) to be used to solve puzzles. **Moreover,** each node who solves these puzzles are rewarded with a piece of the bitcoin network. Finally the article concludes by mathematically proving the chances of an attacker on the network drops as the network grows which is a based on a computational complexity theory problem called nondeterministic polynomial-time complete which require vast CPU processing power which are energy dependent. The main limitations of article is the vague mention of the amount of energy required to solve a problem. **Therefore** although the vast energy required to attack the network is a security feature, the energy consumption is a real issue which has other environmental issues. (204 words)

Article #2

Treiblmaier, H., & Clohessy, T. (2020). Blockchain and Distributed Ledger Technology Use Cases (1st ed.). Springer Nature Switzerland AG 2020. https://doi.org/10.1007/978-3-030-44337-5

This work assesses the use of DLT and their use cases in several ways to categorise DLT technology. There are many ways to categorise DLT technology and their uses cases, the authors apply rationale to their categorisation choices and apply use cases applicable in four main domains; cryptocurrencies, healthcare applications, Internet of things (IoT) and other. **In particular** the authors offer other ways to categorise DLTS such as the DLT software's engineering maturity, stating that the older the more scrutiny hardens software issues and preference over open-source technology which is transparent to

scrutiny offers the best DLT software. The work is intended for academics and DLT practitioners who are about to embark the DLT journey who need some clarification of what kinds of DLT exists and their practical uses cases. The **limitations** are apparent with the shortcomings in offering a general framework to guide new DLT entrants such as Non-Fungible Tokens (NFT) and other new categories or sub-categories of DLT such as how future versions of Distributed Autonomous Organisations (DAO) may fit in the current DLT landscape. **Therefore** this text will be used to form the basis of the final piece in which the categories suggested here will be considered but will be customised for a broader scope and practical use. (211 words)

Article #3

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

A paper which questions the hype of blockchain and creates a decision to tree to argue against the use of a new technology over a the use of established databases. The authors di recognise the strength of a cryptographic data structure to store data and protect its integrity, however they do question the indiscriminate application of the technology without considering the strengths and weaknesses of the DLT technology. In particular, the article raises the question of how a popular DLT, blockchain is applied and not what applications entities can leverage, such as databases as many recent articles about the hype of blockchain they discuss the how to apply. The authors proposed a decision tree to allow blockchain enthusiasts determine for themselves if their use case requires a blockchain application or a database. In particular the authors focus on a supply chain management (SCM) use case database with a blockchain. The decision tree is a set of different questions which is designed to tackle issues such as trust, data confidentiality, fault tolerance, performance, redundancy, and security. Each question asked in the decision tree leads to a binary outcome to use a database or blockchain. The main limitations is that the binary outcome is blockchain based, and not the wider use of DLT technologies such as smart contracts, and DAO applications. Therefore, while the article is a

fundamental article to highlight the use of blockchain may not be worth all the hype the limitations will need some adaption to encompass smart contracts and DAOs. (253 words)

Article #4

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

The article examines how smart contracts have been and can be applied to normal situations which result in sub-optimal outcomes, referred to as dumb ideas. Users and developers of distributed ledger technology (DLT) usually have an optimistic view that software and technology can solve many issues, however when decisions cannot all be binary outcomes we have some ethical issues. Smart contracts are agreements between two parties, however in the rule of law contracts have eight elements which need to be satisfied for a valid agreement to be acceptable in the eyes of the law. **In particular** when smart contracts are in use, they are void of sound legal principles and smart contracts can be used to take advantage of unsuspecting users who may agree to unfair terms. The smart in smart contract simply denotes there is some autonomy and network connectivity to developers and users of the contract which despite a smart contracts ethics or inbuilt biases users of smart contracts trust in the DLT technology. The author further explores smart contract shortcomings when efficient breaches are performed and all within legal and smart contract terms the outcomes benefit only a few. **The main limitation** of the article is the author fails to define what is deemed to be legal contracts, as the term used in the DLT 'smart contract' assumes the contracts are legally enforceable. Therefore while the article shines light on a seldomly spoken issue which is the applicability of smart contracts, the base idea of a smart contract, dumb idea will be used as a main idea to demonstrate that not all blockchain technology solutions are one-size-fits all.

Article #5

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

This report is about the ability of DLT to store vast amounts of information under categories of smart contracts, digital signatures and an array of ways to refactor DLT. Distributed ledgers potentially allow governments to collect taxes, manage passports, land ownership, enforce supply chain of goods, deliver other benefits but overall ensure the integrity of government records and services. The article highlights the current issues faced by the IT legacy information technology (IT) systems have such as security and the security of DLT with the decentralisation of data. The second large issue the UK government face is the bewildering array of terminology in technology and wishes to use DLT as a way for the public to take part of its design to develop a better future government. A better future for the government is one that DLT can assist in reducing fraud, corruption, errors and automate business processing. The author makes recommendations for the government to focus on seven key areas; vision, technology, governance, privacy and security, disruptive potential applications and global potential. This main **limitation** is the article focuses on the technology's potential and fails to highlight the risks factors such as trust in code can lead to many issues such as code vulnerability and unethical use of DLTs, a second limitation is there is no research method rather an observation method of how DLT can transform the UK government. **Therefore**, the article is very useful for what a future government can be and a proponent for DLT. (249 words)

Article #6

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

The article standardises DLT its use, concepts, ecosystems and attempts to clarify technical terminology, the types which exist and fundamental four elements of what a makes a DLT. The author clearly states there are three types of DLT, permissionless, permissioned, and hybrid. Permission is a

public DLT, where a permission is a private and a hybrid is a combination of both private and public. The authors have noticed all DLTs must have four essential elements to function hardware such as a wallet, software development to develop the DLT in question, the protocols a software developer must implement and finally the business application of the DLT. Moreover the authors remain quite neutral of the use of DLT where they point to the factual use of a DLT which is to append new information, the data be immutable, the data be shared between two or more nodes which is to be distributed. Its main limitation of this article is that DLT terminology changes so often that other words will be added to the DLT landscape such as Non-Fungible Tokens (NFTs) which are not mentioned. **Therefore** the article is useful given the authority of the publisher and the baseline standards the report intends to apply to the greater DLT community. (208 words)

Article #7

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

The European Union (EU) has enacted a law the General Data Protection Regulation (GDPR) which regulates how collection and processing of personal data occurs. One of the core principles of this law is the right-to-be-forgotten (RTBF) which protects EU citizens to privacy by the amount of information their personal data is used by organisation which are usually used to sell targeted advertisements upon users. **In particular** the GDPR is designed to have a deterrent approach for the online social networks (OSN) which are discouraged by large fines for breaches of the GDPR laws. Data is equivalent to gold, which the OSNs gather data in the following methods; applications, content providers such as the users, advertisers, and analytic services. **Moreover** When the RTBF action is triggered, that is when a user's requests a provider to delete the users data from their databases however the authors show have not been followed due to the complexity of data structures and place of processing such as third party applications available on OSNs. The problems faced by regulators by enforcing the RTBF is that the service providers are the data processor and the

controller. Moreover if the rules are not followed the exercise to find breaches could an expensive exercise, so the laws in place have shown to be not enough of a deterrent. **The limitations** of the article do not explain the ineffectiveness if breaches are held, nor did they explain the amount of breaches found. **Therefore** the article will be used to showcase that even the law is not enough of a deterrent to dispel GDPR cheats. (263 words)

Article #8

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

This article shines light on a rapidly growing cybercrime industry for electronics health records (EHR) sold on the dark web. The value of each record ranges from $15 and $22 dollars and in some cases they spike to hundreds, or thousands of dollars. **In particular** the authors highlight that blockchain amongst bio-telemetry, virtual reality, and big data are suitable for the hospitals of the future. The authors highlight the benefits of cloud computing which are streamlined collaboration, saving on data storage, data analytics, clinical research, telemedicine capabilities and EHR creation and management. **Moreover** the authors state the exposed public health DLT is susceptible to online attacks which is true as the DLT is made public. The article continues to present the benefits of blockchain technology with focus on the NP-Hard complete algorithmic problem, which simply states the harder the mathematical problem is to solve the more of a deterrent it is for cyber criminals to breach a hospitals information systems. The articles limits are that it encourages browsing the dark web, which is in itself a risky proposition and they also fail to highlight virtualisation and private DLTs as a form of security. **Therefore** the article will be used to highlight the burgeoning thirst for HER on the dark web. (212 words)

Article #9

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

This article researches the most popular DLT technology for cyber security purposes by citing peer reviewed research. This work focuses on privacy, security, integrity, and accountability of data. **In particular** the article focuses on securing the following technologies from highest to smallest; IoT, data storage and sharing, networks, data privacy, public key infrastructure, DNS, web, wi-fi and malware. **Moreover** the authors dive deeper into the technology stacks and discuss very little on industry or use cases. The limitations of the work is that the authors cite only one way to solve the algorithmic puzzles called proof-of-work (PoW) another limitation are the keywords they used which included twenty three keywords which did not include the term DLT, which upon my own research did show multiple articles with DLT exclusively in their titles and keywords. **Therefore,** the article did provide great literature gaps, the article will be used for the broad based approach of applying blockchain to the specific technologies mentioned. (160 words)

Article #10

Hasanova, H., Baek, U., Shin, M., Cho, K., & Kim, M. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal Of Network Management, 29(2), e2060. https://doi.org/10.1002/nem.2060

This article conducts a survey on the weaknesses and vulnerabilities on different types of DLT applications. The authors categorise DLT in three categories being blockchain 1.0, being simple cryptocurrency transactions, blockchain 2.0 being smart contracts for economic and financial market and blockchain 3.0 for other things than the previous two which include government use, health, science, literacy and more. **Moreover,** the authors rightly highlight the amount of research and the lack of research regarding blockchain vulnerabilities. DLT only append information to an existing

data structure with the first blockchain 1.0 and 2.0 focus on PoW and Proof-of-Stake (PoS) which increase risks of double spending. **In particular** the authors highlight each blockchain technology from 1.0 to 3.0 with vulnerabilities in each. Vulnerabilities identified in blockchain 1.0 were twenty seven, blockchain 2.0 were twenty-four and blockchain 3.0 fifth teen. The **limitations** of the article is that a significant drop in vulnerabilities exist in mature models of blockchain which the authors did not state if they were due to the relatively recent development of blockchain 3.0 and or perhaps vulnerabilities are yet to be found. Therefore, the article is a great research piece which will be used for countermeasures against the most common attacks at each DLT. (205 words)

Article #11

Islam, M., & Kundu, S. (2020). IoT Security, Privacy and Trust in Home-Sharing Economy via Blockchain. Advances In Information Security, 33-50. https://doi.org/10.1007/978-3-030-38181-3_3

This article researches trust and privacy in the home-sharing economy and blockchain technology. The authors rightly place the spotlight in the seldom researched topic of privacy in the blockchain. The reason it is rarely research as distributed ledgers the information is inherently made public which counter the privacy aspect. The article starts with the threats which exist in home with appliances connected to the internet, internet of things (IoT). In particular the article addresses the most pressing matter IoT faces, protection of trust, privacy, and IoT security. The authors propose a physical unclonable function (PUF) which involves the manufacturer enrolling the IoT device similar to a MAC address, where a device connected to the home network is registered and if any unregistered devices are added to the network requests are dropped. The **limitations** of the paper is the invention of a new protocol which may add additional load to manufacturers. A second limitations is that the proposed private smart contract is coded in Etherium rather than a software framework using other languages such as C, C++, python, and other well established languages. **Therefore**, the article will

be used for a potential hardware solution to a common problem where IoT is one of the most vulnerable areas of the modern internet. (212 words)

Article #12

Palma, S., Pareschi, R., & Zappone, F. (2021). What is your Distributed (Hyper)Ledger?. 2021 IEEE/ACM 4Th International Workshop On Emerging Trends In Software Engineering For Blockchain (WETSEB). https://doi.org/10.1109/wetseb52558.2021.00011

The article discusses a hybrid blockchain technology called a hyper ledger, with many facets of security, privacy, security, and cryptography are present in the hyper ledger. The hyper ledger uses the well known proof of work (PoW) and introduces Proof-of-Assignment (PoA) which assigns certain permissions. The hyper ledger is designed to be used in multiple ways, with a consortium environment. The article describes two types of hyper ledgers, the Besu and Fabric. The Besu version is a Etherium based decentralised application (Dapp), Fabric which is the most popular of the list with uses in multiple industries with modularity which can be used for specific business uses. The article continues with other version with names such as Indy, identity based, Iroha a role based ledger, Sawtooth smart contracts with business autonomy, and Burrow with virtual machine functionality. **Moreover** the article over some real world use cases with examples of the hyper ledger written in eleven different programming languages and one relational database language called rich queries. Admittedly the authors cite their **limitations** with the lack of a software development kit (SDK) and require the software developers to research on their own. **Therefore** the article and hyper ledger in general presents several favourable uses for many industries for many use cases. (210 words)