Blockchain Challenges for Cloud Users

Yuan Zhao*,Bob Duncan†
Business School
University of Aberdeen, UK
Emails: *y.zhao@abdn.ac.uk,†robert.duncan@abdn.ac.uk

***Abstract*—Blockchain presents a new paradigm for delivering a very robust audit trail through the use of distributed ledger technology. There is the potential to provide a high level of security while keeping costs under control. There are, of course, many challenges, which are specific to cloud computing, and these must be identified and addressed before the right level of security can be achieved. Failure to achieve proper security will negate the benefits of the technology and also expose companies to massive potential fines. We investigate what these challenges are and suggest a means of ensuring how these challenges can be met in order to mitigate any potential exposure of cloud users. We address this in the context of a company who wishes to use a cloud based accounting system and must be compliant with the European Union General Data Protection Regulation.**

Keywords–Cloud forensic problem; GDPR; Blockchain/bitcoin technology.

I. Introduction

All computer systems are the subject of continuous attack, no matter to which market sector they might belong. No system is immune to attack. For traditional networked computer systems, this presents a serious challenge to ensure a high level of security and privacy can be maintained, but for cloud systems, these challenges increase exponentially, due to the increase in complexity in software, and the multiplicity of layers and actors involved in modern cloud ecosystems. There are many challenges to address in order to be able to ensure compliance can be achieved.

Yet, there remains one serious, and as yet unresolved challenge, namely the Cloud Forensic Problem [1], which is likely to prove a serious barrier to achieving any robust level of security and privacy for any company. When an attacker succeeds in gaining even a temporary foothold in a cloud based system, their primary goal will be to escalate privileges until they are able to eliminate the forensic trail, which logged their incursion into the system, thus, allowing them to bury themselves deep so as to become a more permanent intruder, lying undetected inside the victim's system. With cloud systems, there is nothing to prevent this from happening. The intruder is usually perfectly happy to remain hidden in the system, where they can carry on stealing information for as long as they wish with relative impunity. Formerly, the intruder was usually happy to get in and out quickly, but now, long term surveillance can be a far more lucrative proposition for them.

This presents a particularly problematic dilemma for companies who fall under the jurisdiction of, and, therefore, require to be compliant with, the European Union (EU) General Data Protection Regulation (GDPR) [2], and where they also use cloud. By default, those who use cloud will be unable to meet the stringent compliance requirements. With the maximum punitive level of possible fines for non-compliance being up to the greater of €20million or 4% of last year's global turnover [2], this will certainly have a considerable potential impact on those companies who are unable to meet the compliance requirements.

With the widespread convenience, instant access to resources, relatively low operating cost, and no requirement for capital expenditure, cloud systems provide companies with a huge incentive for cloud use. Many companies have already committed substantially to this paradigm, thus, exposing them to the impact of non-compliance. One option would be to convert back to conventional distributed network systems, but taking into account the long lead time needed, the massive costs involved, and the level of expertise that will be required to securely set up such systems, this move back to distributed network systems is unlikely to be either an economic or even a viable option. Equally, it is also not an option to do nothing.

Thus, it is imperative for all cloud users that an alternative solution be found in the meantime, as quickly as possible, and preferably one that might be as simple as possible to implement. In this paper, we look at the use case of a company trading throughout the EU, who wish to use a cloud based accounting software programme and will be subject to and required to comply with the GDPR. They will quite rightly be concerned about the implications of non-compliance this plan might have on their ability to comply with the GDPR.

We are interested in examining the potential offered by Blockchain - the underlying technology that provides the secure backbone of crypto-currencies. We start by examining the potential weaknesses in the use of blockchain in cloud environments in Section II. Next, we consider the potential impact of those weaknesses for cloud users in Section III. In Section IV, we consider how to resolve those cloud blockchain weaknesses, while in Section V, we consider how to set up a robust architecture to address the use case scenario we just introduced. In Section VI, we discuss our findings, and in Section VII, we present our conclusions.

II. Blockchain Weaknesses for Cloud Users

It is certainly the case that no computing system is immune to attack, with this being particularly relevant for cloud based systems. During recent years, some really good research from authors on accountability [3], compliance [4], privacy [5]–[8], risk [9], security [10]–[13], and trust [14]–[16], which has ensured that a far greater level of security and privacy has been achieved in cloud systems. Despite all these good efforts, no solution has yet been developed and implemented to properly address the cloud forensic problem.

Every attacker seeks to compromise a cloud system to gain even a small foothold. They will then attempt to escalate privileges to allow them to access forensic and audit trails,

to allow them to delete or modify such records as they need to hide their route into the system. At this point the attacker becomes an intruder, allowing them to remain hidden and lie undetected for long periods of time, free to help themselves to any data they choose. To achieve compliance with the GDPR, companies must be able to report a breach within 72 hours of discovery. The global average time for all companies between breach and discovery in 2012 was an average of 6 months [17] [18]. This had improved to some 4 weeks by 2016 [19] — still far short of what is needed to understand what has been going on with the intruders while they remained undiscovered.

It is obvious that the longer an intruder can remain hidden inside a company system, the more information they can acquire, or the greater the potential damage they can perpetrate. During 2017, following some serious lobbying, the GDPR was changed from "... within 72 hours of a breach occurring..." to a much less stringent "... within 72 hours of discovery ...", this rather misses the point that if a company cannot discover a breach within 72 hours of the breach occurring, how can they possibly discover it has arisen at all, let alone what data has been compromised after the intruder has deleted all forensic and audit trails? The reality of this backward step in the regulation, was that companies suddenly 'switched off' their attentions to improving cyber security, and this is evidenced by the fact that average times between breach and discovery had by the end of 2017, rather sadly returned to the levels of five years ago [20]. Unfortunately, many companies do not retain the access records that record which database records have been accessed, since many database configurations routinely turn off such functions by default in order to minimise the need for storage. This results in the situation whereby, once a breach occurs, the company will no longer have the means to be able to report which records have been accessed, copied, modified, deleted or ex-filtrated from their system. This means non-compliance with the GDPR, which in turn means exposure to potentially punitive levels of fines by the regulator.

Taking into account the high data volumes associated with cloud use, and in particular the Internet of Things (IoT), this raises the question of just how feasible complying with such a time threshold might be. For cloud users where the company is breached, and where it has made no special arrangements to ensure the safety of forensic and audit trail data, the 72 hour deadline becomes a moot point as it will have no means of knowing that it has been breached. Also, once discovery is made occur, there will be no realistic prospect of that company ever finding out just which records have been compromised. Once the forensic and audit trails are gone — they are gone forever.

A greater concern is likely to emerge where IoT is used, bringing a new range of problems to bear, not least being the general insecure level of devices, their small resource level, yet capable of generating high levels of data throughput. some of which may be lost in transit. Each device may be quite small, yet once the volume is scaled up with thousands of other devices, the impact they can create can rise exponentially. A good example of this is the mass Distributed Denial of Service (DDoS) attack perpetrated using surveillance cameras compromised by the Mirai virus [21][20]. The problem is not so much with the data lost from these IoT devices, rather than the fact that attackers can so easily compromise the devices, allowing them access via corporate networks to other more valuable devices in the system. Where a company does not take special measures to safeguard their forensic and audit trail data, they will be less likely to be able to discover the occurrence of the breach. If, by chance, they should manage to discover the breach, they would certainly be in a position to report it within 72 hours of discovery, but will simply struggle to be able to report what has been compromised, meaning they will be liable for some higher level of fine.

The general attitude by corporates now seems to be that they can forget about screening for the presence of intruders, and simply deal with the reporting once discovery takes place. Again they miss the point of the benefit that comes from rapid discovery - the longer the intruder remains inside the system, the more the damage they can do, and the greater the level of fine the regulator can levy. This means that non-compliance will necessarily become far more serious, thus, enlarging their exposure to the risk of much steeper fines.

While, under the GDPR there is no specific requirement to encrypt data, there is a very strong recommendation that this should take place, be carried out properly and completed within a reasonable time. Encryption and decryption keys should not be stored on the cloud instance. Failure to address these issues will certainly provide grounds for a much increased level of fines in the event of a breach. Thus, cloud use imposes the above weaknesses on the use of any cloud based system before considering any use of software.

As all firms involved in financial services are generally subject to a much greater level of attack than many other market sectors, it is worth taking a look at how they address security requirements. We believe there may be some merit in considering the approach taken with crypto-currencies, since as a new entrant to the market, there is more likelihood that their security approach, having security designed in from the beginning, might offer better prospects for success, as opposed to the approach taken by more traditional financial institutions.

Turning to crypto-currencies, vulnerabilities relating to crypto-currencies are mostly found in operator errors and security flaws. Equally, the Bitcoin platform also faces potential vulnerabilities from protocol designs. Moore and Christin addressed operational insecurity in [22], who suggest that fraudulence is an issue among crypto-currencies. Exchanges act as de facto banks, but almost half of them ceased operation due to the impact of security breaches, failing to reimburse their customers after shutting down. As an alternative approach, other users instead deposited their Bitcoins in a digital wallet. Naturally, these too became a target for cyber-criminals.

A small number of theoretical papers have been written by computer scientists, which address mining pool protocols and anonymity. Miners opted out of the pool in long rounds, where a potential block would be shared with large groups. Babaioff et al. [23], based on a peer-to-peer network layer, argued that the current Bitcoin protocols do not provide any incentive for nodes to broadcast transactions. This is problematic, since the whole system is based on the assumption that this incentive will form a core element. Eyal and Sirer [24], focus instead on the block mining protocol and demonstrate that mining is not incentive-compatible. They further suggest that so-called "selfish mining" can result in higher revenue for miners who collude against others. Houey [25] observed that larger blocks are not as likely to win a block race where new transactions are included into blocks.

Protection of online privacy and anonymity is an issue and both are addressed in the literature. Christin [26] examined anonymity in the online marketplace in crypto-currencies. Böhme et al. [27] examined Internet protocol adoption to see what could be learned from Bitcoin. Many of these studies analysed the public bitcoin transaction history. They were able to find a set of heuristics that can help to link a Bitcoin account with real word identities. Androulaki et al. [28] quantified anonymity in a simulated environment and found that almost half of the users can be identified by their transaction patterns. Using two examples, Bitcoin and Linden Dollars, their report focuses on the impact of digital currencies on the use of fiat money. Gans and Halaburda [29] analysed the economics of private digital currencies, but their explicit focus was on currencies issued by platforms like Facebook or Amazon (that retain full control), and not decentralized currencies like Bitcoin. Dwyer [30] provided institutional details about digital currency developments. The security, privacy and anonymity issue related to Bitcoin has been addressed by Krombholz et al. [31], in which they surveyed 990 Bitcoin users to determine Bitcoin management strategies and identifies how users deploy security measures to protect their keys and Bitcoins. They found that about 46% of participants use web-hosted solutions to manage Bitcoins, and over 50% use such solutions exclusively.

The denial-of-service attack is the one of the most prominent forms addressed by Böhme et al. [27], which entails the attacker swamping a target firm with messages and requests in such volume that either mining pools or exchanges become very slow and unusable. This type of attack is especially effective on the Bitcoin ecosystem because of its relative simplicity of monetising the attacks.

Karame, Androulaki and Capkun [32] looked at using Bitcoin for fast payments and after analysis, found that double-spending attacks on fast payments succeed with overwhelming probability and could be mounted at lower cost unless appropriate detection techniques were integrated in the current Bitcoin implementation. With regard to the double-spending and selfish mining attacks, Kogias et al. [33] proposed the use of ByzCoin as a novel protocol to optimise transaction commitment and verification under normal operation, while guaranteeing safety and liveness under Byzantine (it leveraged scalable collective signing to commit Bitcoin transactions irreversibly within seconds) faults.

There is also some attention from the literature focusing on the price dynamics and speculative bubbles in crypto-currency markets. Cheah and Fry [34] claimed that crypto-currencies are prone to substantial speculative bubbles, and they found that the fundamental value of Bitcoin is zero, by examining the daily clothing prices of Bitcoin from 2010 to 2014. A more recent study is conducted by Blau [35], which emphasised that high volatility of Bitcoin is not related to the speculative activities in this period. The volatility of Bitcoin has been analysed by Katsiampa [36]), Cheah and Fry [34], and many others.

There is no conclusive finding on whether Bitcoin is a speculative investment asset or a currency. Glaser et al. [37] suggest users treat Bitcoin as speculative assets rather than a type of currency. The diversification benefits offered by Bitcoin is also studied by Briére, Oosterlinck and Szafarz [38]. They found Bitcoin can offer diversification benefits after looking into the correlation between Bitcoin and other asset classes. Gandal and Halaburda [39] examined the exchange rates of different virtual currencies to observe the co-movement and identify the opportunities or triangular arbitrage. But they found little opportunity based on daily closing prices. Yermack [40] analysed changes in Bitcoin price against fiat currencies and concludes that its volatility undermines its usefulness as currency. To be qualified as a currency, Bitcoin needs to serve as an intermediary of exchange, as a unit of account and store value. Also, they have been proved not to be able to function as those by Bariviera et al. [41].

In [42]–[44], we considered the possible use of distributed ledger technology as a means of providing a robust mechanism for securing cloud applications. We examined the largest successful crypto-currency attacks and concluded that the link with crypto-currencies attracted greater attention from attackers than would otherwise be the case. In every case of these successful attacks, the inherent strength of the blockchain algorithm behind these companies was never in question. Rather, the success of the attacks came down to successful exploitation of mostly human weaknesses, poor decisions, poor management, neglect and sheer inexperience.

While not a blockchain specific risk, cloud operational weaknesses need to be considered, especially if we wish to include any element of cloud in our solution. We can consider these items in Table II:

TABLE I: CLOUD OPERATIONAL WEAKNESSES ©2019 ZHAO and DUNCAN

Item	Description
CSP	Using an inexperienced CSP can introduce unexpected weaknesses
Backup, Redundancy and Recovery	These issues should be at the core of any CSP decision
Internal Control Weaknesses	Proper internal control is vital to minimise access weaknesses
CSP Hardware & Environment	CSP needs to keep hardware up to date as well as software running on them
Tailored Cloud Deployment	Using "off the shelf" cloud solutions can leave weaknesses
Use of standard CSP offerings for Specilised industries such as Financial Services	Use of a standard cloud offering where the business is highly specialised presents a weakness

We cannot simply decide to use cloud in any solution without first examining their inherent weaknesses and addressing them properly.

We concluded that by removing the link to any crypto-currency, that the underlying blockchain technology could be a very robust way to secure cloud use through the provision of extremely robust audit trails. However, by removing the link to crypto-currencies, this also removes the incentive for "data miners" to spend time and resources on carrying out the necessary work to make the technology work. We suggested an alternative to this would be to create and utilise a 'paid service' to have this work carried out professionally to ensure the strength of the public distributed ledger is preserved.

There might also be an alternative to that solution, whereby a company in effect provides its own 'professional service' to maintain a secure record of the audit trail, and we will consider this as a possibility here. To conclude this section, it is clear that the weaknesses lie, not in the blockchain process, but in the use of cloud systems themselves, and we will consider what the impact of these weaknesses will be in the next section.

III. Impact of Weaknesses for Cloud Users

It is likely that by removing the crypto-currency element, leaving only the blockchain element, we can at one fell swoop eliminate the vast majority of weaknesses from the equation, and at the same time remove the attraction and incentive for attackers. This will leave us to address the cloud weaknesses that will need to be dealt with.

The Cloud Forensic Problem This is a huge potential problem unless special arrangements are in place, e.g., a secure forensic and audit trail is maintained. Failure to do this means there is nothing to prevent an attacker becoming a resident intruder, after which, they will have access to all data. This could lead to huge potential fines in the event of a breach.

The Internet of Things IoT devices used for any purpose by cloud users present a considerable risk, mainly due to the often cheaply made devices with little or no security, often vulnerable to the Mirai virus, which can allow attackers to gain access to systems and to further compromise the main PC and server network due to the porting of the Mirai virus to be able to attack Windows computers [20], [21]. This can expose many other systems to attack, leading to potentially huge fines.

The Need for Proper Monitoring Simple monitoring and analysis of system logs will go a long way to mitigate the well known exploits currently in active use by attackers. Failure to carry out this essential task can result in the company failing to spot attacks, leading to non-compliance and subsequent fines.

Not Using Encryption Under the EU GDPR, the use of encryption is not mandatory. That does not mean it is a good idea not to use it. In the event of a breach where any unencrypted data is leaked, the fine level will be very high. In addition, there is a requirement to notify every single data subject whose data has been compromised. For a large data leak, this could be very time consuming to do, and in the event that the company cannot determine what data details have been compromised, then a higher fine could apply.

Cloud Operational Weaknesses

Each of these cloud operational weaknesses, if not properly addressed, can lead to attackers gaining entry to important systems, leading to non-compliance and huge fines.

Thus, we can see that leaving these weaknesses unaddressed is not an option. In the next section, we consider how we might address these issues in a simple and straightforward way to substantially reduce the exploitation rise.

IV. How We Might Resolve These Weaknesses

There is no doubt that these weaknesses must be addressed, and we advocate doing so in as straightforward a manner as possible.

The Cloud Forensic Problem There has been some interest in addressing the cloud forensic problem [43]–[50], with some easy to implement and use suggestions. The key suggestions are the need for a solid and permanent audit trail and system logs through installing an off-cloud immutable database to store a tamperproof record of the required transactions.

The Internet of Things Great care will need to be taken if IoT devices are to be used. Strong authentication, and robust Intrusion Detection and Intrusion Protection systems should be installed. It would also be prudent to block access by default to all requests originating from the IoT devices and network.

The Need for Proper Monitoring A permanent monitoring system needs to be in place, which can carry out appropriate analytics to detect any anomalous behaviour that occurs on a day to day basis.

The Need to Use Encryption Encryption is a good thing to consider [51], but there are caveats – first, the encryption and de-cryption keys must not be kept on the cloud instance. The encryption should be carried out offline in the cloud users' own systems before being transferred to cloud. Done properly, this can provide serious mitigation to the new EU GDPR fine levels, because if an intruder does get into the cloud system, all they get is meaningless data. With strong levels of encryption, it becomes practically impossible to crack [52]. The regulator will not require data subjects to be notified where the data leak is in encrypted format.

Cloud Operational Weaknesses Resolution

TABLE II: CLOUD OPERATIONAL WEAKNESSES RESOLUTION ©2019 ZHAO and DUNCAN

Item	Description
CSP	Using a market-leading well established CSP who are familiar with legal and regulatory requirements for safeguarding customer data and other sensitive data
Backup, Redundancy and Recovery	Backup, redundancy, and recovery are at the core of the decision to use an outsourcing vendor with highly redundant and resilient data centres designed for mission-critical applications
Internal Control Weaknesses	Internal controls and security processes must ensure customer information is appropriately segregated and protected by industry-standard compliance policies
CSP Hardware & Environment	Leading cloud providers continuously improve their hardware environments to ensure the latest versions of operating systems are installed and use agile software development to deploy feature/function releases on an accelerated basis
Tailored Cloud Deployment	The use of tailored cloud deployment options to meet your specific needs including private clouds solely deployed on your behalf, or a hybrid cloud consisting of shared hardware but segregated data storage would be a prudent move
Use of standard CSP offerings for Specialised industries such as Financial Services	Providers with financial services domain expertise reduce complexity and risk for Financial Institutions with their extensive knowledge of global standards, communications protocols and file formats
CSP Global Support Centre	Cloud providers with global support centres can provide 24 x 7 support in multiple languages, ensuring your international clients and regional offices have access to the support resources required as problems arise

Outsourcing portions of your information technology infrastructure can free up internal IT resources to focus on strategic initiatives and new product development

Conventional Cloud weaknesses Naturally, conventional cloud weaknesses must not be forgotten. These revolve around the Business Architecture of a company, which comprises a combination of People, Process and Technology [17].

- **People Risk Mitigation** People are generally seen as the weakest link in any company, and are particularly prone to social engineering attacks. The company needs to keep abreast of these attacks and ensure all people in the company are regularly trained to understand the risks.

- **Process Risk Mitigation** Processes are often well documented, but also can be woefully out of date. Attackers know to exploit these areas, sometimes in conjunction with social engineering attacks. OWASP [53]are taking a more informed view of dealing with these kinds of attacks.
- **Technology Risk Mitigation** This is where companies are exposed to highly technical attacks. The CSA [54] has done some good work on identifying these risks, as well as offering good strategies to mitigate the risks.

It would certain be a prudent move to test the company cloud systems against the OWASP and CSA vulnerabilities to ensure all discovered vulnerabilities are patched. In the next section, we will look at how to address the resolution of the use case we introduced in the introduction.

V. Addressing the Use Case

Let us return to the use case we introduced at the beginning. The first requirement the company has is to properly secure their main cloud instance on which their cloud accounting system is to run, using all the recommendations we made in Section IV. That will set the scene for a robust environment in which to operate their main business. An essential part of this architecture will be to incorporate the recording of audit and forensic data in an off-cloud immutable database.

The next requirement is to decide on how many blockchain servers the company will seek for the purpose of redundancy. Each blockchain server should be set up in the same secure way as outlined for the main cloud server, but with the addition of the appropriate blockchain algorithms. The preference would be for each blockchain server to be hosted using a different CSP host, again following all the recommendations made in Section IV.

This architecture will provide the basic needs to run the accounting system software, together with an immutable audit and forensic trail. Each of the blockchain servers will have the same security and redundancy. Once the required number of blockchain servers have been set up, the whole system will offer an extremely high level of redundancy. The more robustness is required, it is simply a case of adding more blockchain servers. The more there are, the more challenging it becomes for an attacker to overturn the consensus between all the blockchain servers, and the more robust the system becomes.

VI. Discussion

Because of the major weakness posed by the cloud forensic problem, i.e., the potential to lose both the audit trail and the forensic trail means that recording the data we require to remain compliant with the GDPR becomes a vitally important task for us. The use of a distributed ledger holds great promise. The thinking behind the Blockchain approach affords us with huge redundancy, meaning that an attacker will have to compromise a great many of the distributed ledgers before they can have any impact on the ledger contents. Some would see this as too much redundancy. We would view this as just enough to provide the required assurance. This can therefore provide us with a very strong assurance that the consensus across the ledgers will deliver a high level of comfort as to the veracity of the contents. So, while this represents a big drawback for some, for us, it represents a major advantage.

Some would suggest that the huge volumes of processing generated by the Blockchain process as used in Bitcoin, would be too computationally expensive for our purposes. We disagree. Because it is a crypto-currency and highly volatile, Bitcoin is subject to transactional volumes measuring in multi-trillions per year. By stripping out the crypto-currency aspect from the equation, we also remove the need for such extreme volumes of transactional data, rendering the approach very manageable for any size of company.

VII. Conclusion

We have considered blockchain weaknesses for cloud users, and identified the fact that the major risks lie with the crypto-currencies attached to them. This risk can be eliminated by removing the crypto-currency from the equation. There are more risks attached to cloud use for users to contend with, and we have shown how to approach dealing with those risks.

Our proposal will be to use the underlying concept of a distributed ledger to ensure we are in a position to retain some element of both audit trail and forensic trail data to allow us to meet the compliance requirements of the GDPR, which would otherwise be impossible in the event of a breach. There will be a need to carry out some serious testing in order to find a satisfactory equilibrium between security, privacy, performance, reliability, accessibility and the accountability we require for GDPR compliance. However, it is clear that few current systems can offer anything close to this level of robustness.

References

[1] B. Duncan, "FAST-CFP: Finding a Solution To The Cloud Forensic Problem," in The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, 2018, p. 3.

[2] EU, "EU General Data Protection Regulation (GDPR)," 2017. [Online]. Available: http://www.eugdpr.org/ [Retrieved: March 2019]

[3] S. Pearson, "Towards Accountability in the Cloud," IEEE Internet Comput., vol. 15, no. 4, jul 2011, pp. 64–69.

[4] N. Papanikolaou, S. Pearson, M. C. Mont, and R. Ko, "A Toolkit for Automating Compliance in Cloud Computing Services," Int. J. Cloud Comput., vol. x, no. x, 2014, pp. 45–68.

[5] C. Millard, I. Walden, and W. K. Hon, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," Leg. Stud., vol. 27, no. 77, 2012, pp. 1–31.

[6] N. Papanikolaou, S. Pearson, and M. C. Mont, "Towards Natural-Language Understanding and Automated Enforcement of Privacy Rules and Regulations in the Cloud: Survey and Bibliography," Analysis, 2011, pp. 1–9.

[7] S. Pearson, "Taking account of privacy when designing cloud computing services," Proc. 2009 ICSE Work. Softw. Eng. Challenges Cloud Comput. CLOUD 2009, 2009, pp. 44–52.

[8] L. J. Sotto, B. C. Treacy, and M. L. Mclellan, "Privacy and Data Security Risks in Cloud Computing," World Commun. Regul. Rep., vol. 5, no. 2, 2010, p. 38.

[9] Y. Y. Haimes, B. M. Horowitz, Z. Guo, E. Andrijcic, and J. Bogdanor, "Assessing systemic risk to cloud-computing technology as complex interconnected systems of systems," Syst. Eng., vol. 18, no. 3, 2015, pp. 284–299.

[10] J. Bacon et al., "Information Flow Control for Secure Cloud Computing," IEEE Trans. Netw. Serv. Manag., vol. 11, no. 1, 2014, pp. 76–89.

[11] C. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," IEEE Trans. Serv. Comput., vol. 9, no. 1, 2016, pp. 138–151.

[12] D. Pym and M. Sadler, "Information Stewardship in Cloud Computing," Int. J. Serv. Sci. Manag. Eng. Technol., vol. 1, no. 1, 2010, pp. 50–67.

[13] T. Takahashi, Y. Kadobayashi, and H. Fujiwara, "Ontological Approach toward Cybersecurity in Cloud Computing Categories and Subject Descriptors," in Sci. Technol., 2010, pp. 100–109.

[14] R. K. L. Ko et al., "TrustCloud: A framework for accountability and trust in cloud computing," Proc. - 2011 IEEE World Congr. Serv. Serv. 2011, 2011, pp. 584–588.

[15] R. K. L. Ko, B. S. Lee, and S. Pearson, "Towards achieving accountability, auditability and trust in cloud computing," Commun. Comput. Inf. Sci., vol. 193 CCIS, no. PART 4, 2011, pp. 432–444.

[16] M. Felici, "Cyber Security and Privacy: Trust in the Digital World and Cyber Security and Privacy EU Forum 2013 Brussels, Belgium, April 18-19, 2013 Revised Selected Papers," in Commun. Comput. Inf. Sci. Springer International Publishing, 2013, vol. 182 CCIS, pp. 77–88.

[17] PWC, "UK Information Security Breaches Survey - Technical Report 2012," London, Tech. Rep. April, 2012. [Online]. Available: www.pwc.com www.bis.gov.uk [Retrieved: March 2019]

[18] Trustwave, "2012 Global Security Report," Tech. Rep., 2012. [Online]. Available: https://www.trustwave.com/Resources/Library/Documents/2012-Trustwave-Global-Security-Report/ [Retrieved: March 2019]

[19] Verizon, "2016 Verizon Data Breach Report," Tech. Rep., 2016. [Online]. Available: https://regmedia.co.uk/2016/05/12/dbir$_2$016.$pdf[Retrieved : March2019]$

[20] Verizon, "Verizon Security Breach Report 2017," Tech. Rep., 2017. [Online. Available: https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf [Retrieved: March 2019]

[21] B. Duncan and M. Whittington, "Cyber Security for Cloud and the Internet of Things: How Can it be Achieved?" Cybersecurity Inst. Eng. Technol., vol. Cybersecur, no. September, 2017, pp. 1–39.

[22] T. Moore and N. Christin, "Beware the middleman: Empirical analysis of Bitcoin-exchange risk," in International Conference on Financial Cryptography and Data Security. Springer, 2013, pp. 25–33.

[23] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, "On bitcoin and red balloons," in Proceedings of the 13th ACM conference on electronic commerce. ACM, 2012, pp. 56–73.

[24] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in International Conference on Financial Cryptography and Data Security. Springer, 2014, pp. 436–454.

[25] N. Houy, "The economics of Bitcoin transaction fees," GATE WP, vol. 1407, 2014.

[26] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in Proceedings of the 22nd international conference on World Wide Web. ACM, 2013, pp. 213–224.

[27] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," The Journal of Economic Perspectives, vol. 29, no. 2, 2015, pp. 213–238.

[28] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in International Conference on Financial Cryptography and Data Security. Springer, 2013, pp. 34–51.

[29] J. S. Gans and H. Halaburda, "Some economics of private digital currency," in Econ. Anal. Digit. Econ. University of Chicago Press, 2015, pp. 257–276.

[30] G. P. Dwyer, "The economics of Bitcoin and similar private digital currencies," J. Financ. Stab., vol. 17, 2015, pp. 81–91.

[31] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl, "The other side of the coin: User experiences with bitcoin security and privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2016, pp. 555–580.

[32] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012, pp. 906–917.

[33] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in 25th USENIX Security Symposium (USENIX Security 16). USENIX Association, 2016, pp. 279–296.

[34] E.-T. Cheah and J. Fry, "Speculative bubbles in bitcoin markets? an empirical investigation into the fundamental value of bitcoin," Economics Letters, vol. 130, 2015, pp. 32–36.

[35] B. M. Blau, "Price dynamics and speculative trading in bitcoin," Research in International Business and Finance, vol. 41, 2017, pp. 493–499.

[36] P. Katsiampa, "Volatility estimation for bitcoin: A comparison of garch models," Economics Letters, vol. 158, 2017, pp. 3–6.

[37] F. Glaser, K. Zimmermann, M. Haferkorn, M. C. Weber, and M. Siering, "Bitcoin-asset or currency? revealing users' hidden intentions," 2014.

[38] M. Brière, K. Oosterlinck, and A. Szafarz, "Virtual currency, tangible return: Portfolio diversification with bitcoin," Journal of Asset Management, vol. 16, no. 6, 2015, pp. 365–373.

[39] N. Gandal and H. Halaburda, "Can we predict the winner in a market with network effects? competition in cryptocurrency market," Games, vol. 7, no. 3, 2016, p. 16.

[40] D. Yermack, "Is Bitcoin a real currency? An economic appraisal," National Bureau of Economic Research, Tech. Rep., 2013.

[41] A. F. Bariviera, M. J. Basgall, W. Hasperué, and M. Naiouf, "Some stylized facts of the Bitcoin market," Phys. A Stat. Mech. its Appl., vol. 484, 2017, pp. 82–90.

[42] Y. Zhao and B. Duncan, "Could Block Chain Technology Help Resolve the Cloud Forensic Problem?" in Cloud Comput. 2018 Ninth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 39–44.

[43] Y. Zhao and B. Duncan, "Fixing the Cloud Forensic Problem with Blockchain," Int. J. Adv. Secur., vol. 11, no. 3&4, 2018, pp. 243–253.

[44] Y. Zhao and B. Duncan, "The Impact of Crypto-Currency Risks on the Use of Blockchain for Cloud Security and Privacy," in 7th Int. Work. Secur. Priv. Perform. Cloud Comput. (SPCLOUD 2018), 2018, p. 8.

[45] B. Duncan, M. Whittington, and V. Chang, "Enterprise security and privacy: Why adding IoT and big data makes it so much more difficult," in Proc. 2017 Int. Conf. Eng. Technol. ICET 2017, vol. 2018-Janua, 2018.

[46] B. Duncan, "Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?" in Cloud Comput. 2018 Ninth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 1–6.

[47] B. Duncan and M. Whittington, "Can Forensic Audit Help Address the Cloud Forensic Problem in Light of the Requirements of the Forthcoming European Union General Data Protection Regulation?" in Cloud Comput. 2018 Ninth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 84–89.

[48] B. Duncan and Y. Zhao, "Risk Management for Cloud Compliance with the EU General Data Protection Regulation," in 7th Int. Work. Secur. Priv. Perform. Cloud Comput. (SPCLOUD 2018), Orleans, France, 2018, p. 8.

[49] B. Duncan, A. Happe, and A. Bratterud, "Using Unikernels to Address the Cloud Forensic Problem and help Achieve EU GDPR Compliance."

[50] B. Duncan and M. Whittington, "The Complexities of Auditing and Securing Systems in the Cloud — is there a Solution and will the GDPR move it up the Corporate Agenda?" Int. J. Adv. Secur., vol. 11, no. 3&4, 2018, pp. 232–242.

[51] V. Chang, M. Ramachandran, Y. Yao, Y. H. Kuo, and C. S. Li, "A resiliency framework for an enterprise cloud," Int. J. Inf. Manage., vol. 36, no. 1, 2016, pp. 155–166.

[52] T. Pasquier, B. Shand, and J. Bacon, "Information Flow Control for a Medical Records Web Portal," Cl.Cam.Ac.Uk, 2013, pp. 1–8.

[53] OWASP, "Open Web Application Security Project," 2019. [Online]. Available: https://www.owasp.org/index.php/OWASP_Cloud_Security_Project Accessed: 28/03/2019

[54] CSA, "Cloud Security Alliance," 2019. [Online]. Available: https://cloudsecurityalliance.org/ [Retrieved: March 2019]