The Impact of Crypto-Currency Risks on the Use of Blockchain for Cloud Security and Privacy

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

***Abstract*—A great many cloud users face a difficult challenge in respect of the forthcoming EU General Data Protection Regulation, which comes into effect on 25th May, 2018. While all computer systems are continuously under attack, those who operate conventional distributed network systems stand a far greater chance of being able to demonstrate compliance than those who use cloud based systems. The main reason for this discrepancy between the two approaches is down to the as yet unsolved cloud forensic problem, meaning many cloud users will be completely unable to demonstrate compliance with the new regulation, thus exposing themselves to potentially massive fines after 25th May. We consider the possible use of a crypto-currency based mechanism to address the as yet unsolved cloud forensic problem. Crypto-currencies are becoming a global phenomenon, gaining more attention from media, venture capitalists, financial and government institutions. We focus on the operational risk and the market risk related to crypto-currencies, especially the dominating Bitcoin. Operational risk encompasses the actions that undermine the technological infrastructure and security assumptions of crypto-currencies. We discuss how blockchain technology could improve the efficiency of financial infrastructures, as well as the inevitable vulnerabilities of operational risk of software, open-source governance, and code maintenance. We summarise the literature findings on the co-movement of crypto-currencies with different currencies, indices, and commodities, to show the role of crypto-currency as a commodity, currency, or a speculative investment under portfolio diversification theory. Particularly now that we have seen successful attacks on crypto-currencies in action, it is important to understand where these weaknesses lie, and to endeavour to find out to what extent the use of such technology might expose companies using this technology for GDPR compliance. In the light of the robustness of this approach, we consider whether the underlying blockchain technology could, in turn, be practically applied to addressing the cloud forensic problem. This paper looks at the pros and cons of the blockchain/bitcoin approach, seeking to identify weaknesses, potential benefits offered versus the additional resource costs/latency involved, and considers whether such an approach might be used to secure cloud forensic trails.**

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

I. INTRODUCTION

Every computer system is the subject of continuous attack, no matter to which market sector they belong. No system is immune. For traditional networked computer systems, this presents a serious challenge to ensure a high level of security and privacy can be maintained. 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.

But there remains one serious, yet unresolved challenge, namely the cloud forensic problem, 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 any cloud based system, their primary goal is to escalate privileges until they are able to eliminate the forensic trail which logged their incursion into the system, thus allowing them 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.

This is particularly problematic for companies who are liable to fall under the jurisdiction of, and therefore require to be compliant with, the forthcoming EU General Data Protection Regulation (GDPR) [1], 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, 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 on cloud systems providing a huge incentive for cloud use, many companies will have already committed substantially to this paradigm. 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. 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 latest global phenomenon of crypto-currencies, and the technologies they use to ensure security. An added concern is the rise in hacking exploits that seek to usurp Cloud infrastructures for illicit mining of such currencies.

Security for all financial systems needs an unusually robust approach due to the value of cash at risk, especially for financial companies. The range of risks they face is massive, and we believe it may be worthwhile looking at the operational risks

which encompass the actions that undermine the technological infrastructure and security assumptions of crypto-currencies, as well as the market risk related to crypto-currencies, particularly now that we have started to see successful breaches of these systems. We can analyse these attacks to determine where the weaknesses lie, and learn from our discoveries how to adapt the technology to assist cloud users to better comply with the GDPR.

We examine the cloud forensic problem to understand why it is so much more of a challenge for cloud users than for traditional distributed system users to become compliant with the GDPR in Section II. Next, we turn to crypto-currencies and consider the operational risk in such systems in Section III. In Section IV, we consider the implications of market risk, while in Section IV-A, we look at the co-movement of crypto-currencies with different currencies, indices, and commodities, to show the role of crypto-currency as a commodity, currency, or a speculative investment under portfolio diversification theory, followed by the empirical tests, results and analyses. In Section V, we review a number of successful attacks on crypto-currencies to try to understand what sort of weaknesses have been exploited. In Section VI, we consider the robustness of this approach for dealing with security issues. In Section VII, we discuss our findings, and in Section VIII, we present our conclusions and consider possible future work in this area.

II. The Cloud Forensic Problem and GDPR Compliance

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 Pearson and Charlesworth; Pearson and Benameur; Sotto, Treacy and Mclellan; Ko et al.; Pym and Sadler; Bacon et al.; Papniko;aou et al.; and Chang and Ramachandran [2]–[9], 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.

Once an attacker compromises a cloud system, gaining even a small foothold, they will attempt to escalate privileges to the point where they can access forensic and audit trails, in the process deleting or modifying such records as are necessary to hide their route into and presence in the system, at which point the attacker becomes an intruder. This permits 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 [10] [11]. This had improved to some 4 weeks by 2016 [12] — 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. Last year, 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, is that companies have suddenly 'switched off' their attentions to improving cyber security, and this is evidenced by the fact that average times between breach and discovery have by the end of 2017, have rather sadly returned to the levels of five years ago [13]. Unfortunately, a great many companies do not retain the access records which 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 means that 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.

Considering the high 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. Where a company uses cloud, the company is breached and 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. However, once discovery does 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 DDoS attack perpetrated using surveillance cameras compromised by the Mirai virus [13], [14]. 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. 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. In the next section, we consider the operational risk associated with crypto-currencies.

III. Operational Risk of Crypto-Currencies

Operational risk refers to the actions that undermine the technical infrastructure and security assumptions relating to crypto-currencies. The vulnerabilities related to crypto-currencies can be found in operator errors and security flaws. And most importantly, the Bitcoin platform also faces potential vulnerabilities from protocol designs. Moore and Christin addressed operational insecurity in [15], who suggest that fraudulence is an issue among crypto-currencies. Exchanges act as de facto banks, but almost half of them have ceased operation due to the impact of security breaches, and these exchanges failed to reimburse their customers after shutting down. Taking an alternative approach, other users instead deposited their Bitcoins in a digital wallet. Of course, these too have become a target for cyber-criminals.

Computer scientists have written a small number of theoretical papers which address mining pool protocols and anonymity. Miners opted out of the pool in long rounds, where a potential block will be shared with large groups. Babaioff et al. [16], based on a peer-to-peer network layer, argue that the current Bitcoin protocols do not provide any incentive for nodes to broadcast transactions. This is problematic, since the system is based on the assumption that there will be such an incentive. Instead, Eyal and Sirer [17], focus on 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 [18] observed that larger blocks are not as likely to win a block race where new transactions are included into blocks.

The protection of online privacy and anonymity arises and are both addressed in the literature. Christin [19] examined the anonymous online marketplace in crypto-currencies. Böhme et al. [20] examined what can be learned from Bitcoin regarding Internet protocol adoption. Many studies analysed the public bitcoin transaction history and found a set of heuristics that help to link a Bitcoin account with real word identities. Androulaki et al. [21] quantified the 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, the report focuses on the impact of digital currencies on the use of fiat money. Gans and Halaburda [22] analysed the economics of private digital currencies, but they explicitly focus on currencies issued by platforms like Facebook or Amazon (that retain full control), and not decentralized currencies like Bitcoin. Dwyer [23] provided institutional details about digital currency developments. The security, privacy and anonymity issue related to Bitcoin has been addressed by Krombholz et al. [24], 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.

Among all the potential causes for operational risk, the denial-of-service attack is the prominent form by Böhme et al. [20], which entails 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 [25] analysed the security of using Bitcoin for fast payments, and found that double-spending attacks on fast payments succeed with overwhelming probability and can be mounted at lower cost unless appropriate detection techniques are integrated in the current Bitcoin implementation. Regarding the double-spending and selfish mining attacks, Kogias et al. [26] proposed the usage of Byz-Coin 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. In the next section, we look at the market risk of crypto-currencies.

IV. Market Risk of Crypto-Currencies, the Empirical Tests, Results and Analysis

There are also some attentions from the literature focusing on the price dynamics and speculative bubbles in the crypto-currency markets. Cheah and Fry [27] claimed that the crypto-currencies are prone to substantial speculative bubbles, and they found that the fundamental value of Bitcoin is zero, by examining the daily closing prices of Bitcoin from 2010 to 2014. A more recent study is conducted by Blau [28], 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 [29]), Cheah and Fry [27], and many others.

There is no conclusive finding on whether the Bitcoin is a speculative investment asset or a currency. Glaser et al. [30] 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 [31]. They found Bitcoin can offer diversification benefits after looking into the correlation between Bitcoin and other asset classes. Gandal and Halaburda [32] 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 [33] 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. [34].

These risks are inherent in Bitcoin/blockchain technology, but only because of their use for currencies. Removing the

currency aspect would effectively eliminate much of the market risk from the currency impact, thus potentially providing better security for cloud security and privacy.

A. Co-movement of Crypto-Currencies and Portfolio Theory

Despite extensive studies on the economics aspects of cryptocurrencies, there are relatively fewer studies conducted on analysing the inter-linkage of cryptocurrencies with other financial assets. A number of papers have analysed the ability of cryptocurrencies, usually Bitcoin, to act as safe havens or hedges mentioned by a series of papers such as [35]–[37]. Dyhrberg [35] analysed the hedge properties of Bitcoin using a selection of explanatory variables such as gold (cash and future), the dollar-euro and dollar-pound exchange rates and the the Financial Times Stock Exchange 100 (FTSE 100) Index. The results of the GARCH model [38] showed that Bitcoin can be used in hedging against the dollar and the UK stock market, showing similar hedging capabilities to gold.

Bouri, Azzi and Dyhrberg [37] used a quantile regression approach to analyse the relationships between the Bitcoin and global uncertainty. The findings demonstrate that at the longer frequencies VIX have strong negative impact on Bitcoin returns, while at the shorter frequencies uncertainty does have positive and significant impacts only on high quantiles. This implies that Bitcoin can hedge against global uncertainty at short investment horizons and in the bull regime only. Another study by them in 2017 investigated interrelationships between Bitcoin and the world equity indices, bonds, oil, gold, the general commodity index and the US dollar index using the bivariate DCC model by Engle [39]. The results show limited evidence of hedging and safe haven properties of the Bitcoin; however, Bitcoin still can be an effective diversifier.

In this paper, we will analyse the market risk of Bitcoin and also the co-movement of a few key crypto-currencies to investigate the diversification benefit, and resilience in the condition of financial turmoil, by carrying out some empirical research on the volatility and causality tests using the three largest crypto-currencies, Bitcoin, Ethereum and Ripple.

Figure 1 shows the market capitalisation of the largest three cryptocurrencies, including Bitcoin, Etherum, and Ripple.

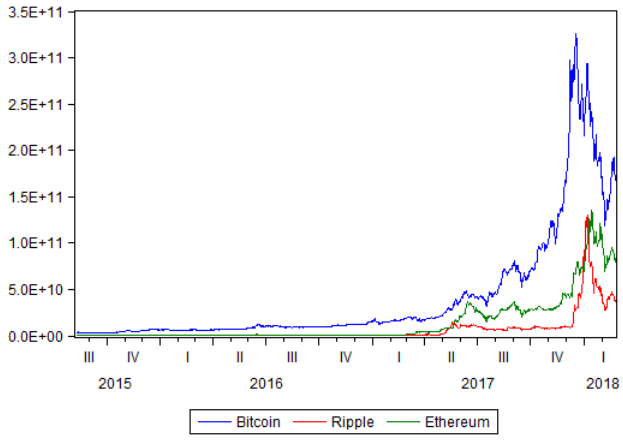

Figure 1: A Comparison of largest three cryptocurrencies [40].

TABLE I: Descriptive statistics and unit root test of Bitcoin returns

Descriptive stats	
Mean	0.002435
Median	0.002045
Maximum	0.3575
Minimum	-0.2662
Std. Dev.	0.04503
Skewness	-0.1917
Kurtosis	11.0549
Jarque-Bera	4776.9130
Observations	1763
Unit root test	
ADF test	-41.6905
PP test	-41.8247
KPSS test	0.2537

B. Bitcoin volatility

In this section, we carry out some empirical tests on forecasting the volatility of the largest crypto-currencies - Bitcoin.

Firstly, we have compared different volatility models which have been proposed in the literature. We examine the natural logarithm of the closing price ratio of consecutive days from 28 April 2013 to 24 Feb 2018 from coindesk website. The daily return of Bitcoin index is 0.2435% with standard deviation of 0.04503. The returns are negative skewed and leptokurtosis. The p-value of Jarqu-Bera test indicates that the returns deviates from normal distribution. We also test there is significant ARCH effect in the returns of Bitcoin returns, suggesting the ARCH family models as the more appropriate specification to model. The unit root test from ADF, PP and KPSS test shows the return series from Bitcoin is stationary. The descriptive statistics and unit root tests are presented as follows:

We follow similar approach in Katsiampa (2017), and conduct the likelihood ratio test on the GARCH model specifications, including AR(1)-GARCH(1,1), AR(1)-EGARCH(1,1), AR(1)-TGARCH(1,1), AR(1)-APARCH, AR(1)-CGARCH(1,1). And we find that the AR(1)-EGARCH(1,1) is the best specification. We forecast the conditional volatility from this specification and present it in Figure 2. Figure 2 shows the persistence and asymmetry in Bitcoin return volatility, especially around late 2013, beginning of 2015, and the end of 2017.

C. Comovement of crypto-currencies

The contagion of spillover effects of multiple cryptocurrencies have been examined by implementing the trivariant GARCH model. The following figure 3 exhibits the covariance of each pair of cryptocurrencies. And there are distinct correlation among these three.

We implement the Granger block causality test to examine the causal relationship of different cryptocurrencies. Under the condition of economic shock, Ripple has a significant causal impact on the returns of Bitcoin. And Etherum has a causal relationship with Ripple. This indicates the resilience in these two currencies in the event of financial structural break.

V. An Analysis of Some of the Largest Successful Crypto-Currency Attacks

In this section, we take a look at some of the largest crypto-currency breaches in recent years, in order to understand how

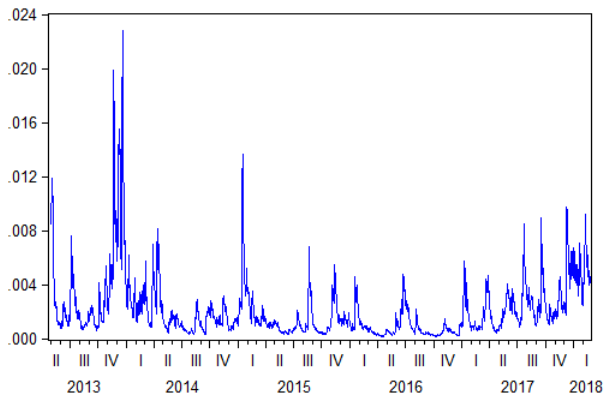

Figure 2: Conditional volatility of Bitcoin returns, from [40].

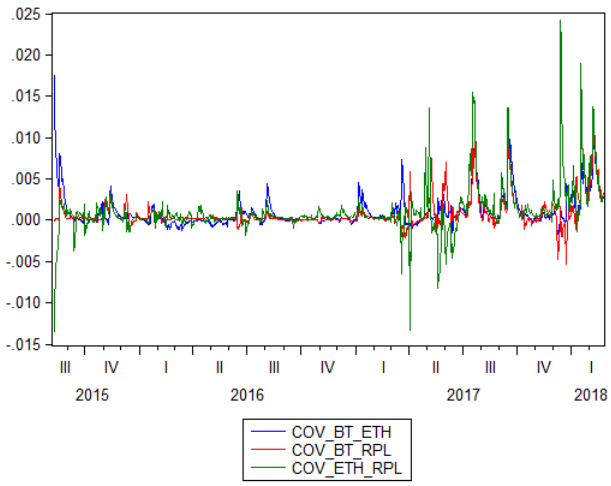

Figure 3: A Comparison of largest three cryptocurrencies [40].

the breaches arose.

Jan 2018 - Tokyo based Coincheck [41] suffered a $530 million loss of crypto currency due to being hacked. Investigations showed that this breach arose due to the Coincheck exchange not using secure networks.

The 2014 Tokyo based Mt Gox [42] lost $460 million following a hack which was successful due to a combination of poor management, neglect and inexperience. This was the second, and fatal, hack for the business, having already lost $8.75 in June of 2011 [43]. This second hack resulted in bankruptcy for the company and arrest for the CEO of the company.

In 2016, Bitfinex [44], another of the world's largest bitcoin exchanges was hacked and lost $72 million. The company had used a different authorisation mechanism in an attempt to make the system more robust, but did not realise their approach had an exploitable weakness, which hackers duly discovered and exploited.

Also in 2016, the Decentralized Autonomous Organization

TABLE II: Granger causality test of the largest three cryptocurrencies

Descriptive stats		
Dependent variable: Bitcoin		
Excluded	Chi-sq	Prob.
Etherum	1.119537	0.5713
Ripple	10.46673	0.0053
All	12.08829	0.0167
Dependent variable: Etherum		
Excluded	Chi-sq	Prob.
Bitcoin	0.188579	0.91
Ripple	2.356285	0.3079
All	2.653052	0.6175
Dependent variable: Ripple		
Excluded	Chi-sq	Prob.
Bitcoin	1.130565	0.5682
Etherum	5.116094	0.0775
All	5.351787	0.2531

(DAO) which was created to operate like a venture capital fund for decentralized crypto-currency projects, built on a smart contract on the Ethereum blockchain, were hacked [45]. A hacker drained $70 million within a few hours by exploiting a flaw that allowed the DAO smart contract to return Ether multiple times before it updated its internal balance. The company coders failed to realise the possibility that anyone would use a recursive function to take advantage of this weakness. The hack resulted in the hard fork of the Ethereum protocol that resulted the creation of Ethereum Classic (ETC).

In 2012, Bitcoinica [46], another large bitcoin trading platform were hacked, losing 46,703 bitcoins. It subsequently transpired that Bitcoinica stored large amounts of digital currency online, as opposed to offline in secure servers. Just a few months later, a second hack resulted in a further loss of another 18,547 bitcoin.

In every case of the above 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 inexperience.

VI. The Robustness of this Approach for Security Issues

The design of Bitcoin presents distinctive risks that differ from other payment methods and thus pose security issues related to operational risk, market risk, and contagion risks with other crypto-currencies. Operational risk occurs when certain actions undermine the technical infrastructure and security assumption of crypto-currencies, including fraudulence of exchanges, mining pool inefficiency, double spending attacks, and online anonymity. Market risk lies in the unpredictable fluctuations in the price of Bitcoin and other cryptocurrencies. As an agent for the storage of value and price goods, the sharp movement of exchange rate of Bitcoin will also cause liquidity issues.

The contagion risk arises when the co-movement of price of a bundle of crypto-currencies becomes inevitable. This will cause potential issues for portfolio diversification, despite their innovations and efficiencies. For instance, the Litecoin confirms transactions four time faster than Bitcoin, which is more useful for the retail use and other time-sensitive transactions.

NXT [47] reduces the electronic and computational burden of Bitcoin mining by replacing the proof-of-work mining with proof-of-stake, assigning blockchain duties in proportion to coin holdings. Zerocash [48], which is not yet operational, will seek to improve privacy protections by concealing identifiers in the public transaction history. Peercoin [49] allows a perpetual 1% annual increase in the money supply.

We can see from what we have looked at, that from a security perspective, in principal, Blockchain technology provides a potentially robust approach to solving this problem. However, in looking at a number of real world instances, we can see that there are potential issues that must be considered. Attacks, such as Denial of Service (DOS) attacks, can prove lethal to both functionality and performance, although Tripathi et al. [50] have suggested a workaround to mitigate this particular issue.

The majority of successful attacks are perpetrated against the storage and containment technology in use, often utilising social engineering or in a recent case, holding of BitCoin owners to ransom until their BitCoins are transferred to the criminal perpetrators. There are clear core strengths contained in Blockchain technology, but there are practical concerns to be considered. The lack of a clear economic methodology to pay for the use of the technology presents a major concern, as does the volatility of the crypto-currencies inextricably linked to it.

However, if we strip away the currency component, and focus only on the Blockchain technology, putting the financing of processing distributed ledger transactions onto a solid financial basis, with sufficient distributed resources to ensure a robust enough environment can be built to sustain the whole process, there might be a way to move forward.

There needs to be a sufficient incentive for distributed ledger providers to provide a highly secure, robust and low latency mechanism to deliver the means to record irrefutable transactional data rapidly enough to provide a high performing system. It is certainly the case that the use of some Blockchain based mechanism to protect cloud instances could prove a very useful means of doing so. However, it is also obvious that if the Blockchain ledgers are run within the same cloud instance as the system they are trying to protect, then we would be asking for trouble.

The obvious solution to this issue would be to truly distribute the Blockchain instances to a sufficiently diverse number of locations, such as to make it difficult for an attacker to compromise all, or a sufficiently large number of the ledgers to be able to force a permanent illicit change to their own advantage. On the other hand, while the increased number of distributed ledgers can significantly increase the security, it will also increase the cost and the latency of processing transactions.

It is certainly the case that while the Blockchain technology is very robust, everything surrounding this technology must also be set up in a similarly robust manner, otherwise the efforts to produce a secure system will be wasted.

VII. Discussion

Because of the major weakness posed by the cloud forensic problem, 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.

There are those who would express concerns at the impact of selfish miners. We take the view that by removing the need for mining from the equation, instead having the processing carried out by credible parties for economic cost, this will remove any incentive to try to mess with the system in this way. All processors would be paid at the same rate for the job they perform, so there would be no means available to them, nor any incentive, to try to improve on that.

Yet others point to the dangers of Distributed Denial of Service (DDoS) attacks. Given that there will be no direct financial advantage to be gained by attacking these Blockchain ledgers, the volume of attacks will likely be lower. For a large attack to be financially viable, there has to be a huge financial incentive before it becomes worthwhile to spend the kind of money it takes to perpetrate such an attack. In the case of using this approach for GDPR compliance, there is no obviously monetizable item for the attacker to steal. This means with a significantly reduced incentive to attack the system, there is likely to be a much higher safety level for our purposes.

VIII. Conclusion and Future Work

It is clear that for any company using cloud, it will prove virtually impossible to achieve compliance with the GDPR in the event of a security breach due to the, as yet unresolved, Cloud Forensic Problem. For those who have yet to realise this as a problem, discovering this fact after a cyber breach will not be grounds for mitigation from the regulator. Thus, cloud users who require to be compliant with the GDPR must take steps now to be thoroughly prepared ahead of time.

We have looked at the Operational Risk and the Market Risk of crypto-currencies as well as considering the co-movement of crypto-currencies in the light of portfolio theory. Many of these risks arise through the perceived mass value attributable to these crypto-currencies and the mass transactional processing volumes implicit in their operation. Clearly, by removing the currency aspect from the equation, we can eliminate a huge portion of the risk. We accept that all risk will not be removed, but there will be a significant reduction in risk levels involved.

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.

To this end, as part of our future work, we plan to conduct a pilot case study on how the technical aspects might be implemented in order to meet all the required goals to ensure compliance can be achieved. This will be tested running on a miniature cloud system, offering both cloud-based and non-cloud based ledgers to assess what the optimum configuration might be.

REFERENCES

[1] EU, "EU General Data Protection Regulation (GDPR)," 2017. [Online]. Available: http://www.eugdpr.org/ Last accessed: 5 May 2018

[2] S. Pearson and A. Charlesworth, "Accountability as a way forward for privacy protection in the cloud," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 5931 LNCS, no. December, 2009, pp. 131–144.

[3] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in 2010 IEEE Second International Conference on Cloud Computing Technology and Science, no. December. IEEE, nov 2010, pp. 693–702.

[4] L. J. Sotto, B. C. Treacy, and M. L. Mclellan, "Privacy and Data Security Risks in Cloud Computing," World Communications Regulation Report, vol. 5, no. 2, 2010, p. 38.

[5] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "TrustCloud: A framework for accountability and trust in cloud computing," Proceedings - 2011 IEEE World Congress on Services, SERVICES 2011, 2011, pp. 584–588.

[6] D. Pym and M. Sadler, "Information Stewardship in Cloud Computing," International Journal of Service Science, Management, Engineering, and Technology, vol. 1, no. 1, 2010, pp. 50–67.

[7] J. Bacon, D. Eyers, T. F. J.-M. Pasquier, J. Singh, I. Papagiannis, and P. Pietzuch, "Information Flow Control for Secure Cloud Computing," IEEE Transactions on Network and Service Management, vol. 11, no. 1, 2014, pp. 76–89.

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

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

[10] PWC, "UK Information Security Breaches Survey - Technical Report 2012," London, Tech. Rep. April, 2012. [Online]. Available: www.pwc.com www.bis.gov.uk Last accessed: 5 May 2018

[11] Trustwave, "2012 Global Security Report," Tech. Rep., 2012. [Online]. Available: https://www.trustwave.com/Resources/Library/Documents/2012-Trustwave-Global-Security-Report/ Last accessed: 5 May 2018

[12] Verizon, "2016 Verizon Data Breach Report," Tech. Rep., 2016. [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf Last accessed: 5 May 2018

[13] Verizon, "Verizon Security Breach Report 2017," Tech. Rep., 2017. [Online]. Available: https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/ Last accessed: 5 May 2018

[14] B. Duncan and M. Whittington, "Cyber Security for Cloud and the Internet of Things: How Can it be Achieved?" Cybersecurity: The Institution of Engineering and Technology, vol. Cybersecur, no. September, 2017, pp. 1–39.

[15] 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.

[16] 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.

[17] 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.

[18] N. Houy, "The economics of Bitcoin transaction fees," 2014.

[19] 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.

[20] 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.

[21] 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.

[22] J. S. Gans and H. Halaburda, "Some economics of private digital currency," in Economic Analysis of the Digital Economy. University of Chicago Press, 2015, pp. 257–276.

[23] G. P. Dwyer, "The economics of Bitcoin and similar private digital currencies," Journal of Financial Stability, vol. 17, 2015, pp. 81–91.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

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

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

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

[31] 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.

[32] 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.

[33] D. Yermack, "Is Bitcoin a real currency? An economic appraisal," In Handbook of digital currency (pp. 31-43).

[34] A. F. Bariviera, M. J. Basgall, W. Hasperué, and M. Naiouf, "Some stylized facts of the Bitcoin market," Physica A: Statistical Mechanics and its Applications, vol. 484, 2017, pp. 82–90.

[35] A. H. Dyhrberg, "Bitcoin, gold and the dollar–a garch volatility analysis," Finance Research Letters, vol. 16, 2016, pp. 85–92.

[36] A. H. Dyhrberg, "Hedging capabilities of bitcoin. is it the virtual gold?" Finance Research Letters, vol. 16, 2016, pp. 139–144.

[37] E. Bouri, G. Azzi, and A. H. Dyhrberg, "On the return-volatility relationship in the bitcoin market around the price crash of 2013," 2016.

[38] T. Bollerslev, "Generalized autoregressive conditional heteroskedasticity," Journal of econometrics, vol. 31, no. 3, 1986, pp. 307–327.

[39] R. Engle, "Dynamic conditional correlation: A simple class of multivariate generalized autoregressive conditional heteroskedasticity models," Journal of Business & Economic Statistics, vol. 20, no. 3, 2002, pp. 339–350.

[40] Coindesk, "Coindesk," 2017. [Online]. Available: https://www.coindesk.com/ Last accessed: 5 May 2018

[41] BBC, "Coincheck: World's biggest ever digital currency 'theft'," 2018. [Online]. Available: http://www.bbc.co.uk/news/world-asia-42845505 Last accessed: 5 May 2018

[42] R. McMillan, "Bitcoin's $460 Mliion Disaster," 2014. [Online]. Available: https://www.wired.com/2014/03/bitcoin-exchange/ Last accessed: 5 May 2018

[43] J. Goldman, "The Inside Story of Mt. Gox, title = Bitcoin Exchange Mt.Gox Hit by Cyber Attack, [Online]. Available: https://www.esecurityplanet.com/network-security/bitcoin-exchange-mt.gox-hit-by-cyber-attack.html, year = 2014." Last accessed: 5 May 2018

[44] C. Baldwin, "Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong," 2016. [Online]. Available: https://www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP Last accessed: 5 May 2018

[45] D. Siegel, "Understanding The DAO Attack," 2016. [Online]. Available: https://www.coindesk.com/understanding-dao-hack-journalists/ Last accessed: 5 May 2018

[46] L. Constantin, "Hackers break into bitcoin exchange site Bitcoinica, steal $90,000 in bitcoins," 2012. [Online]. Available: https://www.networkworld.com/article/2188554/applications/hackers-break-into-bitcoin-exchange-site-bitcoinica–steal–90-000-in-bitcoins.html Last accessed: 5 May 2018

[47] NXT, "NXT Platform," 2017. [Online]. Available: https://nxtplatform.org/ Last accessed: 5 May 2018

[48] Zerocash, "Zerocash," 2017. [Online]. Available: http://zerocash-project.org/ Last accessed: 5 May 2018

[49] Peercoin, "Peercoin," 2017. [Online]. Available: https://peercoin.net/ Last accessed: 5 May 2018

[50] S. Tripathi, B. Gupta, A. Almomani, A. Mishra, and S. Veluru, "Hadoop based defense solution to handle distributed denial of service (ddos) attacks," Journal of Information Security, vol. 4, no. 03, 2013, p. 150.