Fixing the Cloud Forensic Problem with Blockchain

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

Abstract—**Many cloud users are heading into a potentially devastating regulatory disaster zone. A major unresolved cloud issue, namely the cloud forensic problem, this is likely to mean many cloud users will be unable to be compliant with the new EU General Data Protection Regulation. We consider the possible use of blockchain, a cryptocurrency based mechanism, to address the as yet unsolved cloud forensic problem. We believe that the underlying blockchain could be adopted to provide a robust mechanism for ensuring that cloud forensic and audit trail records can be securely maintained. This would ensure that cloud users would in turn be able to ensure they are compliant with the new EU General Data Protection Regulation, thus minimising their exposure to punitive levels of fines. We analyse the key risks in cryptocurrencies, namely the operational risk, market risk and cross contamination risk associated with co-movement of cryptocurrencies with other asset forms, using the most predominant and oldest of those, Bitcoin, to provide an example of how removing these risks might provide a far more effective solution to the cloud forensic problem. Our contribution is to demonstrate how this might be done, and by removing the incentive for attackers, to provide a much higher level of compliance with the EU General Data Protection Regulation for cloud users.**

Keywords*–*Cloud forensic problem; GDPR; blockchain/bitcoin technology.

I. Introduction

All computing systems connected to the internet are constantly under attack, and 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, especially in light of their disparate agendas.

There remains one serious, but as yet, unresolved challenge, namely the cloud forensic problem. This problem arises where an attacker breaches a cloud system and becomes an intruder, whereby there is nothing then to prevent that intruder from escalating privileges and removing all trace of their incursion by deleting or modifying the forensic trail identifying all their actions and routes into the system. The intruder seeks to remain hidden in the system, where they can continue absorbing information. In [1], we considered whether it might be possible to utilise blockchain technology to help deal with this problem. This article extends that earlier work.

The cloud forensic problem is particularly problematic for companies who both use cloud, and are liable to fall under the jurisdiction of, and therefore require to be compliant with, the new EU General Data Protection Regulation (GDPR) [2]. Without ensuring their cloud provision can properly retain full audit and forensic records, those who use cloud will struggle to meet compliance requirements. Given the punitive level of possible fines for non-compliance (up to the greater of €20million or 4% of last year's global turnover), this is likely to have a considerable impact on companies who are unable to be compliant.

The very convenience of cloud use for a great many companies is likely to place them at a competitive disadvantage now that the GDPR is live. Due to the long lead time required, the enormous costs involved, and the level of expertise needed to securely set up such systems, moving back to conventional distributed network systems is currently unlikely to present a feasible option for many companies, who will effectively be "waiting for the sword of Damocles to fall".

It is imperative that a viable solution be found as quickly as possible. We take a look at the latest global phenomenon of cryptocurrencies, and the technologies they use to ensure security. Security for all financial systems is a necessary priority in all financial companies. They are subject to an incredible range of risks, and we believe it may be worthwhile looking at the operational risk which encompasses the actions that undermine the technological infrastructure and security assumptions of cryptocurrencies, as well as the market risk related to cryptocurrencies.

We start by examining the cloud forensic problem to understand why it is such a challenge for cloud users to become compliant with the GDPR in Section II. Next, we turn to cryptocurrencies and consider operational risk in such systems in Section III. In Section IV, we conside the implications of market risk, while in Section V, we look at the co-movement of cryptocurrencies with different currencies, indices, and commodities, to show the role of cryptocurrency as a commodity, currency, or a speculative investment under portfolio diversification theory. In Section IX, we consider the robustness of this approach for dealing with security issues. In Section X, we discuss our findings and consider future work, and in Section XI, presents our conclusions.

II. The Cloud Forensic Problem and GDPR Compliance

All computer systems connected to the internet are continuously subject to attack, and cloud systems are no exception. It is certainly the case that no system is immune to attack, and that is particularly true for cloud systems. During the past decade, a great many research papers have allowed a far greater level of security and privacy to be achieved in cloud systems. There have been many good papers produced on both security [3]–[14] and privacy [11], [15]–[30], and a number of others have looked at better accountability as a means to meeting these ends [7], [8], [12], [17], [24], [27], [31]–[50] However, despite all those efforts, no solutions have yet been found to address the cloud forensic problem.

This problem arises once an attacker compromises a cloud system, thus gaining even a small foothold. Once embedded in a system, the attacker becomes an intruder and seeks to escalate privileges until they can access and delete, or modify, the forensic logs in order to hide all trace of their incursion into the system. This allows them to retain a long term foothold within the system, thus allowing them to help themselves to whatever data they wish.

Many companies do not retain records of which database records have been accessed, and by whom, meaning that once a breach occurs, the ability of the company to be able to report which records have been accessed, copied, modified, deleted or ex-filtrated from the system becomes an impossible task. This results in non-compliance with the GDPR, meaning exposure to potentially punitive levels of fines.

To achieve compliance with the GDPR, all companies must first 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 [51] [52]. This had improved to some 4 weeks by 2016 [53] — still far short of what is needed to understand what has been going on with the intruders while they were undiscovered.

In the light of 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 is moot, since in the first place, it will have no means of knowing that it has been breached, so will have nothing to report, since the requirement is to report within 72 hours of discovery. However, once discovery does occur, there will be no realistic prospect of that company ever finding out just which records have been compromised. When the forensic and audit trail is gone — it is gone!

The IoT, of course, brings a whole new suite of problems to bear, not least of which is the general insecure level of devices, their small resource level, yet high throughput level of data. some of which may be lost in transit. The issue might not be so much with the data lost from IoT devices, rather than with the ability of attackers to easily compromise the devices, thus allowing them access via corporate networks to other more valuable devices in the system. We do not address the IoT within the scope of this paper, but do recognise that any company using IoT devices will require to take special measures to ensure GDPR compliance can be achieved.

Where a company does not take these special measures to safeguard their forensic and audit trail data, they will be less likely to be able to discover the occurance of the breach. Shoud they by chance manage to discover the breach, they would certainly be in a position to report it with 72 hours of discovery, they will simply struggle to be able to report what has been compromised, meaning they will be liable for some level of fine.

Obviously, the longer an intruder has available to spend inside a company system, the more information they will be able to acquire, and the more potential damage they can cause. While 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 will they possibly be able to discover that is has arisen at all, let alone what data has been compromised once the intruder has deleted all forensic and audit trails?

So, not being able to discover that a breach has arisen, while not putting the company technically in breach of the GDPR, it will certainly make it extremely difficult to enable them to report which records have been compromised once discovery actually occurs. This means the non-compliance will necessarily become far more serious, thus enlarging the exposure to risk of steeper fines.

While there is no specific requirement to encrypt data, there is certainly a strong recommendation that this should take place, and should do so within a reasonable time. Encryption and decryption keys should not be stored on the cloud instance. Failure to address these issues will certainly lead to steeper fines in the event of a breach. An obvious point is that if encryption is not used, then the regulator will require the company to report the breach to every compromised user, which will prove an impossible task where the forensic and audit trails have been lost, again leading to yet steeper fines.

Due to the large number of high value clients, firms involved in financial services are generally subject to greater attack than many other market sectors [54]. It is worth taking a look at how they address security requirements. We believe there may be some merit in considering cryptocurrencies, since as a new entrant to the market, there is more likelihood that their security approach, being designed from the beginning, might offer better prospects rather than relying on existing methods.

III. Operational Risk of cryptocurrencies

Operational risk refer to any action that undermines the technical infrastructure and security assumptions relating to cryptocurrencies. Considering operational risk will provide us with an understanding of how well these risks are dealt with in cryptocurrencies. In looking at high value successful breaches of cryptocurrencies, we can see that these vulnerabilities relate mainly to operator errors and security flaws, which we discuss later. And most importantly, the Bitcoin platform also faces potential vulnerabilities from protocol designs. Operational insecurity has been addressed by Moore and Christin [55], who suggests that fraudulence is an issue among cryptocurencies. Exchanges act as de facto banks, but almost half of them ceased operation due to the resultant impact of security breaches. However, these exchanges failed to reimburse their customers after shutting down. As an alternative approach, other users have instead deposited their Bitcoins in a digital wallet which has also become a target for cyber-criminals.

A small number of theoretical papers written by computer scientists address the mining pool protocols and anonymity. Miners opted out for the pool in long rounds, in which a potential block will be shared with large groups. Based on a peer-to-peer network layer, Babaioff et al. [56] argue that the current Bitcoin protocols do not provide an incentive for nodes to broadcast transactions. This is problematic, since the system is based on the assumption that there is such an incentive. Instead, by focusing on block mining protocol, Eyal and Sirer [57] show that mining is not incentive-compatible and that so-called “selfish mining” can lead to higher revenue for miners who collude against others. Houey [58] observed that larger blocks are less likely to win a block race when including new transactions into blocks. Karame, Androulaki and Capkun [59] 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. [60] proposed the usage 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.

The protection of online privacy and anonymity arises and are both addressed in the literature. Christin [61] examined the anonymous online marketplace in cryptocurrencies. Böhme et al. [62] 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. [63] 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 [64] 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 [65] provided institutional details about digital currency developments. The security, privacy and anonymity issue related to Bitcoin has been addressed by Krombholz et al. [66], 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 (DoS), or distributed-denial-of-service (DDoS) attack is the prominent form suggested by Böhme et al. [62], 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.

We need to consider another major risk of cryptocurrencies, market risk, and how this affects the volatility of the currency element.

IV. Market Risk of cryptocurrencies

Market risk via price fluctuation in the exchange rate is inevitable for users holding Bitcoin and other cryptocurrencies. Figure 1 shows the average US dollar-Bitcoin exchange rate, along with its trading volume. It is clear that the market volatility is tremendous for Bitcoin, leading to a high potential market risk.

There is also some attention from the literature focusing on the price dynamics and speculative bubbles in cryptocurrency markets. Cheah and Fry [68] claimed that cryptocurrencies 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 [69], which emphasised that the high volatility of Bitcoin is not related to the speculative activities in this period. The volatility of Bitcoin has been analysed by Katsiampa [70]), Cheah and Fry [68], and many others.

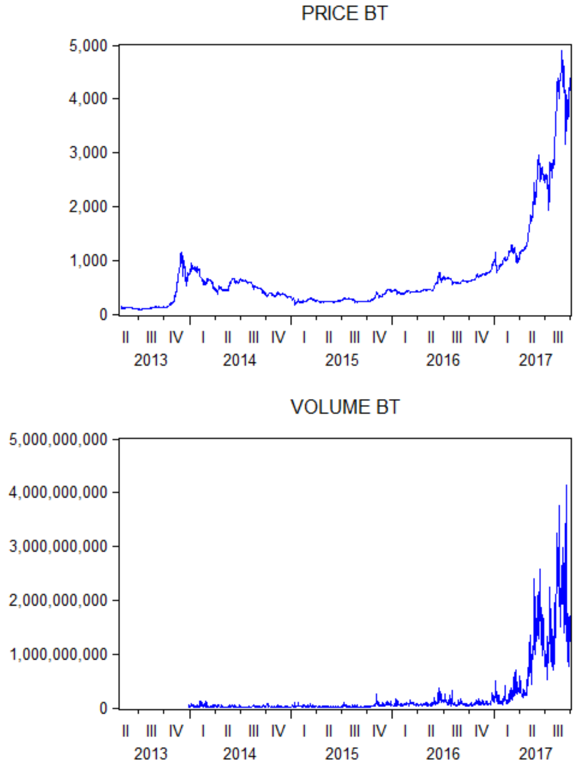

Figure 1: A Comparison Between Price and Volume [67].

Glaser et al. [71] suggest users treat Bitcoin as speculative assets rather than as a type of currency. The diversification benefits offered by Bitcoin is also studied by Briére, Oosterlinck and Szafarz [72]. They found Bitcoin can offer diversification benefits after looking into the correlation between Bitcoin and other asset classes. Gandal and Halaburda [73] 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 [74] 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. [75].

The market risk of cryptocurrencies is also reflected in behavioural factors, such as trading volume and other exogenous factors. Corbet et al. (2017) investigated the fundamental drivers for cryptocurrency price behaviour, and found that there is the existence of bubbles. Jiang (2017) reported the existence of long-term memory and the inefficiency of the cryptocurrency market, using a similar approach. Alvarez-Ramirez et al (2018) analysed long-term correlation and information efficiency, and reported that the Bitcoin market exhibits time-varying efficiency and price dynamics, which are driven by anti-persistence. Bariviera et al. (2017) compared crytocurrencies with other standard currencies and found that the hurst exponents changed significantly in the initial stage and stabilised thereafter. Bouri et al. (2018) found that the financial stress index could be used to forecast the price movement of cryptocurrencies. Other behavioural factors were found by later researchers. Feng et al. (2017) found evidence on informed insider trading of Bitcoins prior to big events, implying that the informed trading may contribute to explaining the dynamics of the Bitcoin price. Dotsika and Watkins (2017) employed keyword network analysis and identified potential disruptive trends in block-chain technologies.

Next we turn to how cryptocurrencies relate to conventional assets in the context of portfolio theory in order to understand-where the weaknesses arise.

V. Co-movement of cryptocurrencies and Portfolio Theory

Despite extensive studies on the economic 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 [76]–[78]. Dyhrberg [76] 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 [79] showed that Bitcoin can be used in hedging against the dollar and the UK stock market, showing similar hedging capabilities to gold. In Figure 2, we see how a basket of crypro-currencies compare with each other based on price.

Bouri, Azzi and Dyhrberg [78] used a quantile regression approach to analyse the relationships between 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 a 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 [80]. The results show limited evidence of hedging and safe haven properties of Bitcoin; however, Bitcoin still can be an effective diversifier.

Next, we carried out some empirical research using the three largest cryptocurrencies, Bitcoin, Ethereum and Ripple, by addressing the impact of volatility, which we cover in the next section.

VI. The Empirical Tests, Results and Analysis

In this section, we carry out some empirical tests on the volatility of the three largest cryptocurrencies, Bitcoin, Ethereum and Ripple. Figure 3 shows the market capitalisation of the largest three cryptocurrencies, including Bitcoin, Etherum, and Ripple. In this section, we will look into the conditional volatility, correlations, causal relationships, time variation on such relationships, and external factors that may affect the relationships.

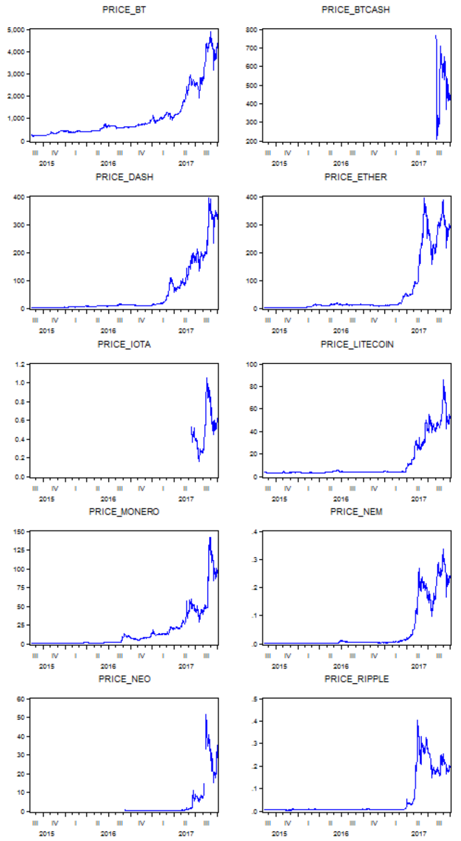

Figure 2: A Co-Movement View of cryptocurrencies Based on Price [67].

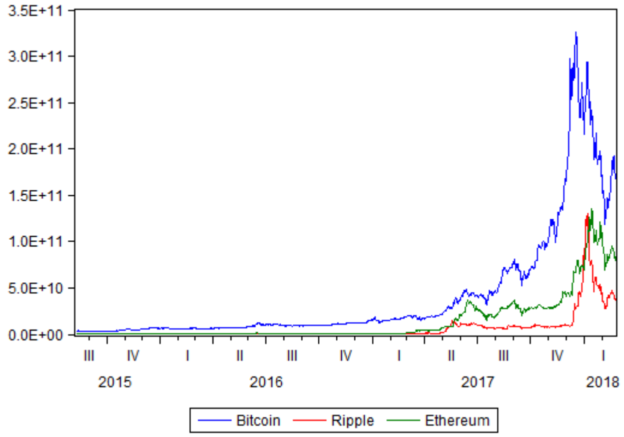

Figure 3: A Comparison of largest three cryptocurrencies [67].

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

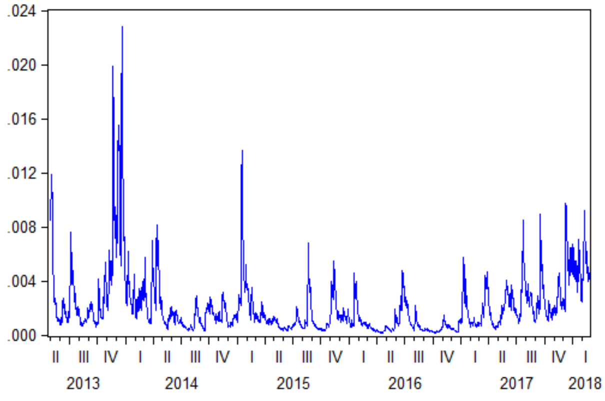

Figure 4: Conditional volatility of Bitcoin returns, from [67].

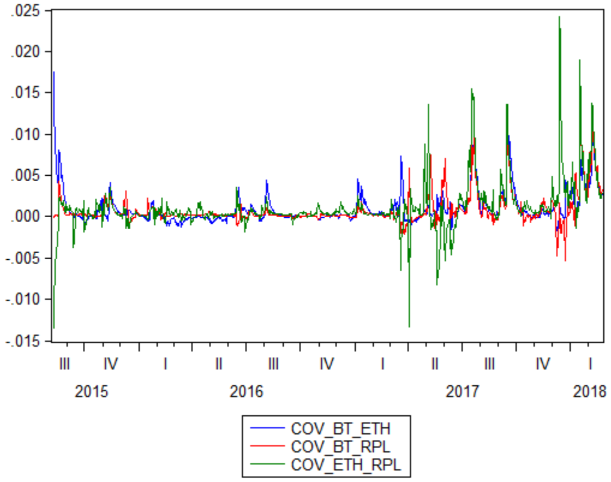

Figure 5: The covariance of largest three cryptocurrencies [67].

- We model the conditional volatility for cryptocurrencies, by comparing different volatility models. We present the findings on Bitcoin as the baseline cryptocurrency. We examine the natural logarithm of the closing price ratio of consecutive days from 28 April 2013 to 24 Feb 2018. 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 the Jarqu-Bera test indicates that the returns deviate from a 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 in Table I.
  We follow a similar approach to [70], 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 based on the results of likelihood ratio test. We forecast the conditional volatility from this specification. Figure 4 shows the persistence and asymmetry in Bitcoin return volatility, especially around late 2013, the beginning of 2015, and the end of 2017.
- The contagion of spillover effects of multiple cryptocurrencies can be investigated using trivariant-GARCH models. The following Figure 5 exhibits the covariance of each pair of cryptocurrencies. It is evident that the covariance between these three cryptocurrencies increases significantly around the recent one year compared to the initial one year. The covariance between Ripple and Ethereum is more sensitive to external economic conditions, implied by the more volatile fluctuations.
- According to Markowitz portfolio theory, an asset that is unrelated or even negatively correlated with another asset in the portfolio is characterised as hedging effective. Thus, it is worth looking into the correlation among the major cryptocurrencies in terms of their roles on portfolio diversification. In this study, we utilise the Granger causality test and vector autoregressive (VAR) model, in order to investigate the short-term dynamic causal relationship between different pairwise cryptocurrencies. In Table II, we present the findings for the short-run causality from different directions, on the null hypothesis of no short-term causal relationships. A p-value (Prob.) less than a predefined significance level (5%) indicates a rejection of the existence of a causal relationship. We find that under the condition of short-run exogenous economic shock, Ripple has a significant causal impact on the returns of Bitcoin. And Etherum has a causal relationship with Ripple. The direction of such causal relationship can be seen in Figure 6, by impulse response function. We find positive causal relationships from all directions.
- As indicated in the previous findings, cryptocurrencies have entered into a more dynamic market with more potential risks. Hence, we especially focus on the recent full year from 2016 to 2017, to examine the time variation of the causality. The following Figure

TABLE II: Granger causality test of the largest three cryptocurrencies

Granger block exogeneity Wald test		
Dependent variable: Bitcoin		
Excluded	Chi-sq	Prob.
Ethereum	1.119537	0.5713
Ripple	10.46673	0.0053
All	12.08829	0.0167
Dependent variable: Ethereum		
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
Ethereum	5.116094	0.0775
All	5.351787	0.2531

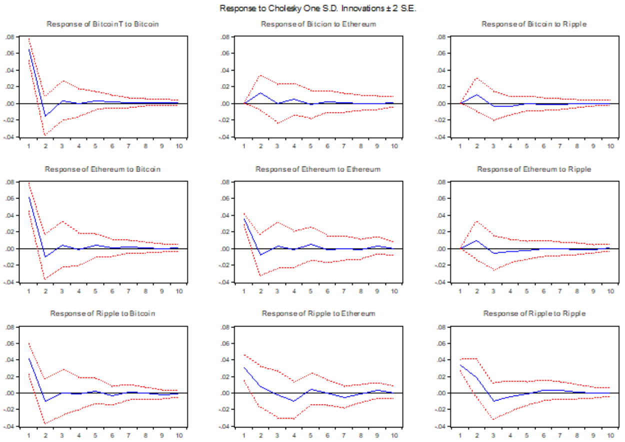

Figure 6: The Impulse Response Function of largest three cryptocurrencies [67].

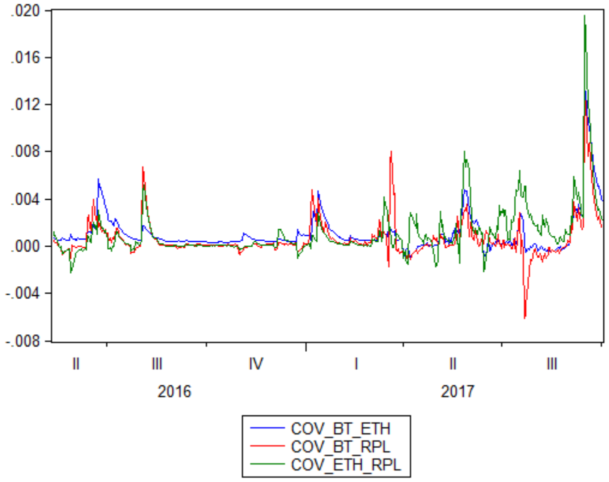

Figure 7: The covariance of largest three cryptocurrencies [67].

TABLE III: Granger causality test of the largest three cryptocurrencies

Granger block exogeneity Wald test 2016-2017		
Dependent variable: Bitcoin		
Excluded	Chi-sq	Prob.
Ripple	3.1278	0.2093
Ethereum	0.8272	0.6613
All	3.6444	0.4563
Dependent variable: Ethereum		
Bitcoin	6.5079	0.0386
Ripple	1.3257	0.5154
All	7.4076	0.1159
Dependent variable: Ripple		
Bitcoin	1.5218	0.4672
Ethereum	0.7558	0.6853
All	3.0384	0.5514

7 exhibits the covariance of each pair of cryptocurrencies, Table III shows the Granger causality of pairwise cryptocurrencies, and Figure 8 illustrates the directions of such causality, in the recent one year. We find that in the recent one year, Bitcoin dominates others by having an increasing covariance with the other two. There is a significantly positive causal relationship from Bitcoin to other currencies, which can be concluded according to the Granger block exogeneity Wald test p-value as 0.0386 and positive responses from Ethereum and Ripple.

- Other external factors may also become sources affecting the market risk of cryptocurrencies. According to the review of financial literature, trading volume is a main factor affecting the risks and returns of financial assets. Therefore, we examine the causality of behavioural factors like trading volume on cryptocurrencies by implementing a VAR model and Granger causality test. Table IV shows the causality of volume from these three currencies to their returns. We find that the trading volume of Ripple has a significant causal relationship over Bitcoin and Bitcoin volume. And the Bitcoin trading volume has the reverse causality over Ripple volume and Ethereum volume, which further confirms our inferences on the increasing impact of Bitcoin in the recent full year over others.

VII. A Summary of the Empirical Results

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 cryptocurrencies.

Operational risk occurs when certain actions undermines the technical infrastructure and security assumption of crypotocurrencies, such as fraudulence of exchanges, mining pool inefficiency, double spending attacks, and online anonymity. However, we know that a DoS or DDoS attack can be very debilitating for blockchain systems.

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.

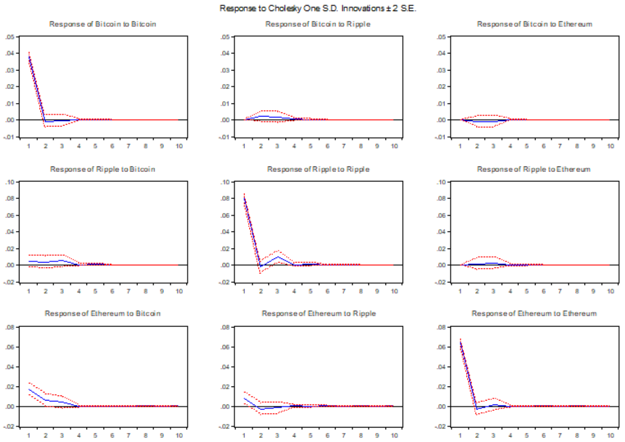

Figure 8: The Impulse Response Function of the largest three cryptocurrencies during 2016-2017 [67].

Contagion risk arises when the co-movement of price of a bundle of cryptocurrencies 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 [81] 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 [82], which is not yet operational, will seek to improve privacy protections by concealing identifiers in the public transaction history. Peercoin [83] allows a perpetual 1% annual increase in the money supply.

In looking at the empirical results, we can see that there is a bi-directional potential contagion effect between each of the cryptocurrencies, which will vary depending on economic conditions. This demonstrates an increased risk of cross contagion between different cryptocurrencies. This contagion appears to be increasing over recent years, which would suggest the contagion risks are increasing. These calculations will help any potential user to consider the impact of these risks in the light of their own risk appetite.

In the next section, we analyse some of the largest successful cyber breaches of cryptocurrencies in order to determine whether there might be any weakness in the fundamental blockchain component.

VIII. An Analysis of Some of the Largest Successful cryptocurrency Attacks

In this section, we take a look at some of the largest cryptocurrency breaches in recent years, in order to understand how the breaches arose.

The earliest large scale breach to a cryptocurrency exchange was in 2010 due to the value overflow incident — where an early flaw in the bitcoin system allowed the intruder to create 184 billion units of bitcoin. The value then was $21.2bn, although at recent prices the value would have been $1.8 quadrillion. It was notable for the speed at which it was discovered and dealt with, resulting in no actual loss of value. The perpetrator has never revealed themselves and their original 0.5 BTC used in the exploit remains unspent to this day, despite being valued at more than $3,000.

TABLE IV: Granger causality test of the largest three cryptocurrencies return versus trading volume

Granger block exogeneity Wald test		
Dependent variable: Bitcoin		
Excluded	Chi-sq	Prob.
Ethereum	0.0787	0.9614
Ripple	4.6776	0.0964
Bitcoin volume	2.2668	0.3219
Ethereum volume	2.5613	0.2779
Ripple volume	6.5272	0.0383
All	17.6204	0.0617
Dependent variable: Ethereum		
Bitcoin	4.8802	0.0872
Ripple	0.5197	0.7712
Bitcoin volume	3.4664	0.1767
Ethereum volume	1.1715	0.5567
Ripple volume	3.0683	0.2156
All	11.7578	0.3016
Dependent variable: Ripple		
Bitcoin	2.0651	0.3561
Ethereum	1.0425	0.5938
Bitcoin volume	2.4065	0.3002
Ethereum volume	0.3773	0.8281
Ripple volume	2.2058	0.3319
All	10.4823	0.3992
Dependent variable: Bitcoin volume		
Bitcoin	0.7594	0.6841
Ethereum	4.3616	0.1129
Ripple	0.2130	0.8990
Ethereum volume	4.4428	0.1085
Ripple volume	10.7419	0.0046
All	23.4696	0.0091
Dependent variable: Ethereum volume		
Bitcoin	0.3634	0.8338
Ethereum	7.2534	0.0266
Ripple	0.4723	0.7897
Bitcoin volume	6.1108	0.0471
Ripple volume	2.6953	0.2598
All	21.2929	0.0191
Dependent variable: Ripple volume		
Bitcoin	4.6771	0.0965
Ethereum	1.2313	0.5403
Ripple	5.8466	0.0538
Bitcoin volume	17.1896	0.0002
Ethereum volume	2.1749	0.3371
All	40.2409	0.0000

Jan 2018 - Tokyo based Coincheck 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. Customer funds were stored in “hot” wallets which were live to the internet, instead of using “cold” wallets should have been offline and not visible to the internet.

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

The February 2018 hack on BitGrail was worth $195 million. While there was speculation that the BitGrail founder Francesco Firano siphoned off the funds, he in turn insists it was a hack.

In 2016, Bitfinex, 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. Rather than ceasing operations, Bitfinex reduced the balance on all accounts by 36%, ragardless of whether their account had been compromised to cover all the losses, and were given an alternative cryptocurrency, BFX tokens, in exchange which Bitfinex promised to buy back over time. As of April 2017, Bitfinex had fully reimbursed all of its customers.

Also in 2016, the Decentralized Autonomous Organization (DAO) which was created to operate like a venture capital fund for decentralized cryptocurrency projects, built on a smart contract on the Ethereum blockchain, were hacked. 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 December 2017, hackers attacked the NiceHash mining service, and with the assistance of a compromised company computer, made off with 4,400 bitcoins from customer accounts worth $64 million. While the funds were not recovered, NiceHash promised to compensate their customers in full. Within a few weeks the lost bitcoins were back in customer accounts.

In June 2018, Coinrail, a South Korean exchange, was the target of an attack, losing around $37 million of cryptocurrencies Pundi X and Aston. Again, they were storing bitcoin online. The remaining 70% of currency was rapidly switched to offline storage. The attack was traced to an Ethereum address, which has subsequently had its assets frozen.

In July 2017, the parity multisig wallet exploit was used against three large Ethereum accounts, netting $32 million. The owners of these accounts were believed to be the Ethereum-powered casino Edgeless, decentralised commerce platform Swarm City amd the smart contracts platform aeternity. All three accounts had recently held initial coin offerings , thus their wallets contained large amounts of money. Swarm City recently confirmed that it was one of the targets.

In June 2018, Bithumb, a South Korean exchange were hit by hackers, reporting $31.5 million stolen.

In 2012, Bitcoinica, another large bitcoin trading platform was 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 sheer inexperience.

IX. The Robustness of this Approach for Security Issues

In previous sections, we have seen that there are a number of key risks pertaining to cryptocurrencies, namely operational risk, market risk, and contagion risks with other cryptocurrencies. In looking at the largest successful cryptocurrency breaches, we can see that while the breaches were successful, the underlying blockchain was never breached. The original part-bitcoin leveraged to perpetrate the Mt Gox attack in 2014 has never been sold as this would provide proof to the authorities who perpetrated the attack, which is testament to the inherent strength of the blockchain.

In looking at a number of real world instances, we can see that there are potential issues that must be considered. Attacks, such as DoS and DDoS attacks, can prove lethal to both functionality and performance, although Tripathi et al. [84] have suggested a workaround to mitigate this particular issue. One obvious approach is to discuss the matter with the CSP to ensure they have the capacity to be able to handle such an attack should it arise.

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, due to the high redundancy provided, 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 cryptocurrencies inextricably linked to it. While the high value of the cryptocurrency element provides a strong incentive to attackers, if we remove this element by simply removing the cryptocurrency, we can see that at one fell swoop, we also lose operational risk, market risk, and contagion risks with other cryptocurrencies. We also lose a huge volume of transactional data involved in the trading of cryptocurrencies, meaning we are left with blockchain only, the distributed ledger element. With vastly reduced transactional volumes, latency of operation will be much less of an issue.

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. An economic balance will need to be determined. Carlsten et al. [85] warn of the potential instability of bitcoin without the block reward, so clearly paying service providers to run the blockchain would be required to provide a sufficiently robust service. We would also have the option of using the same approach with the Ethereum cryptocurrency, which would offer the option of being able to deal with smart contracts. However, for most purposes, the basic blockchain will be more than adequate for our needs.

We have seen how Azaria et al. [86] have suggested a similar approach to improve privacy with medical records. Christidis and Devetsikiotis [87] have suggested the use of both blockchain and smart contracts to improve security and privacy for the Internet of Things. Dinh et al. [88] offer a blockchain benchmarking system to compare the relative efficiencies of differing blockchain and smart contract options. Gaetani et al. [89] have proposed a blockchain based database to ensure data integrity for cloud. Kiayias and Panagiotakos [90] suggest the GHOST protocol at the core of Ethereum could offer significant increases in speed for transactional recording. Yermack [91] suggests that the use of blockchain can improve help to Corporate Governance. There is no doubt that there is a great deal of interest in trying to apply this new approach to make improvements for cloud users.

X. Discussion

Thanks to 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 blockchain approach affords us with increased 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 point to the huge volumes of processing generated by the blockchain process as used in Bitcoin, suggesting that it would be too computationally expensive for our purposes. We take a different view. Because it is a cryptocurrency and highly volatile, Bitcoin is subject to transactional volumes measuring in multi-trillions per year. By stripping out the cryptocurrency 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.

Some express concerns at the impact of selfish miners. We take the view that by removing the need for mining from the equation, and 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 DoS and 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 reduce to a significantly lower level. 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.

XI. 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. Discovering this fact after a cyber breach will not be grounds for mitigation from the regulator after the fact. It will be far too late by then. Therefore, cloud users who require to be compliant with the GDPR will have to take steps now to be thoroughly prepared ahead of time.

We have looked at the Operational Risk and the Market Risk of cryptocurrencies as well as considering the comovement of cryptocurrencies in the light of portfolio theory. Many of these risks arise through the perceived mass value attributable to these cryptocurrencies 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.

To that end, 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 run around a miniature cloud in a box system, offering both cloud-based and non-cloud based ledgers to assess what the optimum configuration might be.

References

[1] 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.

[2] EU, “EU General Data Protection Regulation (GDPR),” 2017. [Online]. Available: http://www.eugdpr.org/ [Last accessed: August 2018]

[3] M. Almorsy, J. Grundy, and I. Müller, “An analysis of the cloud computing security problem,” 17th Asia-Pacific Softw. Eng. Conf. (APSEC 2010) Cloud Work. Aust., no. December, 2010, p. 7.

[4] M. Almorsy, J. Grundy, and I. Mller, “An analysis of the cloud computing security problem.” proc. 2010 Asia Pacific Cloud Work. Coloca. with APSEC2010, Aust., 2010.

[5] V. Chang, Y. H. Kuo, and M. Ramachandran, “Cloud computing adoption framework: A security framework for business clouds,” Futur. Gener. Comput. Syst., vol. 57, 2016, pp. 24–41.

[6] F. Doelitzscher, T. Ruebsamen, T. Karbe, M. Knahl, C. Reich, and N. Clarke, “Sun Behind Clouds - On Automatic Cloud Security Audits and a Cloud Audit Policy Language,” Int. J. Adv. Networks Serv., vol. 6, no. 1, 2013, pp. 1–16.

[7] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, B. S. Lee, and Q. Liang, “TrustCloud: A Framework for Accountability and Trust in Cloud Computing,” Perspective, 2011, pp. 1–9.

[8] 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, 2011, pp. 432–444.

[9] K. Lee, "Security Threats in Cloud Computing Environments," Int. J. Secur. its Appl., vol. 6, no. 4, 2012, pp. 25–32.

[10] 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.

[11] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services," Current, 2009, pp. 44–52.

[12] S. Pearson, "Toward accountability in the cloud," IEEE Internet Comput., vol. 15, no. 4, jul 2011, pp. 64–69.

[13] S. Ramgovind, M. Eloff, and E. Smith, "The Management of Security in Cloud Computing," in Inf. Secur. South Africa (ISSA), 2010, 2010, pp. 1–7.

[14] H. Takabi, J. B. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Secur. Priv. Mag., vol. 8, no. 6, nov 2010, pp. 24–31.

[15] S. Creese, P. Hopkins, S. Pearson, and Y. Shen, "Data Protection-Aware Design for Cloud Computing," Work, no. December, 2009, pp. 1–13.

[16] K. Hon, C. Millard, and I. Walden, "The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated ?" 2011.

[17] W. K. Hon, C. Millard, and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," Leg. Stud., no. 77, 2011, pp. 1–31.

[18] W. K. Hon, J. Hörnle, and C. Millard, "Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law?" Leg. Stud., 2011, pp. 1–40.

[19] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," 2009 Eighth IEEE Int. Conf. Dependable, Auton. Secur. Comput., dec 2009, pp. 711–716.

[20] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," NIST, Tech. Rep., 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf [Last accessed: August 2018]

[21] H. Katzan Jr, "On The Privacy Of Cloud Computing," Int. J. Manag. Inf. Syst., vol. 14, no. 2, 2011, pp. 1–12.

[22] W. K. Hon, C. Millard, J. Singh, I. Walden, and J. Crowcroft, "Policy, legal and regulatory implications of a Europe-only cloud," Int. J. Law Inf. Technol., vol. 24, no. 3, 2016, pp. 251–278.

[23] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations," Natioinal Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. February, 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [Last accessed: August 2018]

[24] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," Computing, no. December, 2009, pp. 1–15.

[25] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," 2010 IEEE Second Int. Conf. Cloud Comput. Technol. Sci., nov 2010, pp. 693–702.

[26] S. Pearson, "Privacy, Security and Trust in Cloud Computing," in Priv. Secur. Cloud Comput. e: Springer, 2013, pp. 3–42.

[27] J. Prüfer, "How to govern the cloud? Characterizing the optimal enforcement institution that supports accountability in cloud computing," Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, vol. 2, 2013, pp. 33–38.

[28] S. S. Shapiro, "Privacy by Design," Commun. ACM, vol. 53, no. 6, jun 2010, p. 27.

[29] G. Kambourakis, "Anonymity and closely related terms in the cyberspace: An analysis by example," J. Inf. Secur. Appl., vol. 19, no. 1, 2014, pp. 2–17.

[30] J. Singh, T. F. J. M. Pasquier, and J. Bacon, "Securing tags to control information flows within the Internet of Things," 2015 Int. Conf. Recent Adv. Internet Things, RIoT 2015, 2015.

[31] EU, "Accountability for Cloud (A4Cloud)," 2018. [Online]. Available: http://a4cloud.eu/ [Last accessed: August 2018]

[32] C. A. Adams and R. Evans, "Accountability, Completeness, Credibility and the Audit Expectations Gap," JCC 14 Summer 2014, vol. 14, no. Summer, 2014, pp. 97–115.

[33] W. Benghabrit, H. Grall, J.-C. Royer, M. Sellami, M. Azraoui, K. Elkhiyaoui, M. Onen, A. S. D. Olivera, and K. Bernsmed, "A Cloud Accountability Policy Representation Framework," in CLOSER-4th Int. Conf. Cloud Comput. Serv. Sci., 2014, pp. 489–498.

[34] K. Bernsmed, W. K. Hon, and C. Millard, "Deploying Medical Sensor Networks in the Cloud – Accountability Obligations from a European Perspective," in Cloud Comput. (CLOUD), 2014 IEEE 7th Int. Conf. IEEE Comput. Soc, 2014, pp. 898–905.

[35] D. Butin, M. Chicote, and D. Le Métayer, "Log design for accountability," in Proc. - IEEE CS Secur. Priv. Work. SPW 2013, 2013.

[36] D. Catteddu, M. Felici, G. Hogben, A. Holcroft, E. Kosta, R. Leened, C. Millard, M. Niezen, D. Nunez, N. Papanikolaou, S. Pearson, D. Pradelles, C. Reed, C. Rong, J.-C. Royer, D. Stefanatou, and T. W. Wlodarczyk, "Towards a Model of Accountability for Cloud Computing Services," in Int. Work. Trust. Account. Forensics Cloud, 2013, pp. 21–30.

[37] A. Haeberlen, "A Case for the Accountable Cloud," ACM SIGOPS Oper. Syst. Rev., vol. 44, no. 2, 2010, pp. 52–57.

[38] W. Hon, E. Kosta, C. Millard, and D. Stefanatou, "Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation," Queen Mary Sch. Law Leg. Stud. Res. Pap., no. 172, 2014, pp. 1–54.

[39] K. L. R. Ko, P. Jagadpramana, and B. S. Lee, "Flogger: A File-Centric Logger for Monitoring File Access and Transfers within Cloud Computing Environments," Computing, 2011, pp. 1–8.

[40] T. Lynn, P. Healy, R. McClatchey, J. Morrison, C. Pahl, and B. Lee, "The Case for Cloud Service Trustmarks and Assurance-as-a-Service," in CLOSER 2013 - Proc. 3rd Int. Conf. Cloud Comput. Serv. Sci., 2013, pp. 110–115.

[41] N. Papanikolaou, S. Pearson, M. C. Mont, and R. K. L. Ko, "Towards Greater Accountability in Cloud Computing through Natural-Language Analysis and Automated Policy Enforcement," Engineering, 2011, pp. 1–4.

[42] N. Papanikolaou, T. Rübsamen, and C. Reich, "A Simulation Framework to Model Accountability Controls for Cloud Computing," CLOUD Comput. 2014, Fifth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. c, 2014, pp. 12–19.

[43] S. Pearson, M. C. Mont, and G. Kounga, "Enhancing Accountability in the Cloud via Sticky Policies," in Secur. Trust Comput. Data Manag. Appl., 2011, pp. 146–155.

[44] S. Pearson, V. Tountopoulos, D. Catteddu, S. Mario, R. Molva, C. Reich, S. Fischer-Hubner, C. Millard, V. Lotz, M. G. Jaatun, R. Leenes, C. Rong, and J. Lopez, "Accountability for Cloud and Other Future Internet Services," in CloudCom, 2012, pp. 629—-632.

[45] K. Bernsmed and S. Fischer-Hübner, "Secure IT Systems: 19th Nordic Conference, NordSec 2014 Tromsø, Norway, October 15-17, 2014 Proceedings," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8788, 2014, pp. 3–24.

[46] T. Ruebsamen and C. Reich, "Supporting Cloud Accountability by Collecting Evidence Using Audit Agents," in CloudCom 2013, 2013, pp. 185–190.

[47] J. Singh, J. Powles, T. Pasquier, and J. Bacon, "Data Flow Management and Compliance in Cloud Computing," Cloud Comput., no. Special Issue on Legal Clouds., 2015, pp. 1–12.

[48] A. Squicciarini, S. Sundareswaran, D. Lin, and S. Huang, "Promoting Distributed Accountability in the Cloud," in IEEE 4th Int. Conf. Cloud Comput. Promot., 2011, pp. 113–120.

[49] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," in IEEE Trans. Dependable Secur. Comput., vol. 9, no. 4, 2012, pp. 556–568.

[50] M. Theoharidou, N. Papanikolaou, S. Pearson, and D. Gritzalis, "Privacy risk, security, accountability in the cloud," in Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, vol. 1, 2013, pp. 177–184.

[51] PWC, "UK Information Security Breaches Survey - Technical Report 2012," PWC2012, Tech. Rep. April, 2012.

[52] Trustwave, "2012 Global Security Report," Tech. Rep., 2012.

[53] Verizon, "2016 Verizon Data Breach Report," Tech. Rep., 2016.

[54] D. Marcus and R. Sherstobitoff, “Dissecting Operation High Roller,” White Pap. McAfee, vol. 000, 2012, pp. 1–20.

[55] 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.

[56] 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.

[57] 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.

[58] N. Houy, “The economics of Bitcoin transaction fees,” 2014.

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[63] 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.

[64] 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.

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

[66] 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.

[67] Coindesk, “Coindesk,” 2017. [Online]. Available: https://www.coindesk.com/ [Last accessed: August 2018]

[68] 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.

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

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

[71] F. Glaser, K. Zimmermann, M. Haferkorn, M. C. Weber, and M. Siering, “Bitcoin-asset or currency? revealing users’ hidden intentions,” 2014.

[72] 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.

[73] 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.

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

[75] 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.

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

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

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

[79] T. Bollerslev, “Generalized autoregressive conditional heteroskedasticity,” J. Econom., vol. 31, no. 3, 1986, pp. 307–327.

[80] R. Engle, “Dynamic conditional correlation: A simple class of multivariate generalized autoregressive conditional heteroskedasticity models,” J. Bus. Econ. Stat., vol. 20, no. 3, 2002, pp. 339–350.

[81] NXT, “NXT Platform,” 2017. [Online]. Available: https://nxtplatform.org/ [Last accessed: August 2018]

[82] Zerocash, “Zerocash,” 2017. [Online]. Available: http://zerocash-project.org/ [Last accessed: August 2018]

[83] Peercoin, “Peercoin,” 2017. [Online]. Available: https://peercoin.net/ [Last accessed: August 2018]

[84] S. Tripathi, B. Gupta, A. Almomani, A. Mishra, and S. Veluru, “Hadoop based defense solution to handle distributed denial of service (ddos) attacks,” J. Inf. Secur., vol. 4, no. 03, 2013, p. 150.

[85] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, “On the Instability of Bitcoin Without the Block Reward,” in Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS’16, 2016.

[86] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” in Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016, 2016.

[87] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” 2016.

[88] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, “BLOCKBENCH: A Framework for Analyzing Private Blockchains,” 2017.

[89] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “Blockchain-based database to ensure data integrity in cloud computing environments,” in CEUR Workshop Proc., vol. 1816, 2017.

[90] A. Kiayias and G. Panagiotakos, “On Trees, Chains and Fast Transactions in the Blockchain.” IACR Cryptol. ePrint Arch., vol. 2016, 2016, p. 545.

[91] D. Yermack, “Corporate governance and blockchains,” 2017.