Could Block Chain Technology Help Resolve the Cloud Forensic Problem?

Conference Paper · February 2018

CITATIONS
0

READS
112

2 authors, including:

Bob Duncan
University of Aberdeen
40 PUBLICATIONS **201** CITATIONS

SEE PROFILE

Could Block Chain Technology Help Resolve the Cloud Forensic Problem?

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 blindly heading into a potentially devastating regulatory disaster zone. Given the shortcomings of the cloud due to the cloud forensic problem, this is likely to mean many cloud users will be unable to be compliant with the forthcoming EU General Data Protection Regulation when it comes into effect on 25th May, 2018. 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, and 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. The operational risk encompasses the actions that undermine the technological infrastructure and security assumptions of crypto-currencies. We discuss how the implementation of block chain technology could improve the efficiency of financial infrastructure, as well as the inevitable vulnerabilities of operational risk of software, open-source governance, and code maintenance. The market risk associated with crypto-currencies denotes the fluctuation in the exchange rate between crypto-currency and other currencies or financial asset classes. 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. In the light of the robustness of this approach, we consider whether the underlying block chain 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, the potential benefits offered versus the additional resource costs involved, the increased latency necessarily introduced and considers whether there is any mileage in using such an approach to secure cloud forensic trails.**

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

I. INTRODUCTION

All computing systems 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.

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. Needless to say, they are perfectly happy to remain hidden in the system, where they can carry on stealing information, while continuing to hide their presence.

This is about to become 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 forthcoming EU General Data Protection Regulation (GDPR) [1]. Those who use cloud will by default be unable 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.

Given the widespread convenience of cloud use for a great many companies, it is likely that this fact will place them at a competitive disadvantage once the GDPR goes live on 25th May. Given the long lead time required, the enormous costs involved, and the level of expertise needed to securely set up such systems, moving back to distributed network systems is unlikely to present a feasible option for many companies, who will effectively be "sitting ducks" once the legislation takes effect on 25th May 2018.

Therefore, it is imperative that a viable solution be found in the meantime, and as quickly as possible. For this paper, we take a look at the latest global phenomenon of crypto-currencies, and the technologies they use to ensure security. Security for all financial systems takes an necessary ultra high level 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 crypto-currencies, as well as the market risk related to crypto-currencies.

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 crypto-currencies 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 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. In Section VI, we consider the robustness of this approach for dealing with security issues. In Section VII, we discuss our findings and consider future work, and in Section VIII, presents our conclusions.

II. The Cloud Forensic Problem and GDPR Compliance

All computer systems 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. However, despite all that effort, 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 [2] [3]. This had improved to some 4 weeks by 2016 [4] — 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 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.

As all firms involved in financial services are generally subject to greater 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 crypto-currencies, 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.

III. Operational Risk of Crypto-Currencies

Operational risk referrers to the action that undermines 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. Operational insecurity has been addressed by Moore and Christin [5], who suggests that fraudulence is an issue among cryptocurencies. Exchanges acts 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. [6] 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 [7] 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 [8] observed that larger blocks are less likely to win a block race when including new transactions into blocks. Karame, Androulaki and Capkun [9] analysed the security of using Bitcoin for past 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. [10] 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 [11] examined the anonymous online marketplace in crypto-currencies. Böhme et al. [12] 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. [13] 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 [14] 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 [15] provided institutional details about digital currency developments. The security, privacy and anonymity issue related to Bitcoin has been addressed by Krombholz et al. [16], 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. [12], 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.

IV. Market Risk of Crypto-Currencies

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 are also some attentions from the literature focusing on the price dynamics and speculative bubbles in the crypto-currency markets. Cheah and Fry [18] claimed that the crypto-currencies are prone to substaintial speculative bubbles, and they found that the fundamental value of Bitcoin is zero, by examining the daily clothing prices of Bitcoin from 2010 to

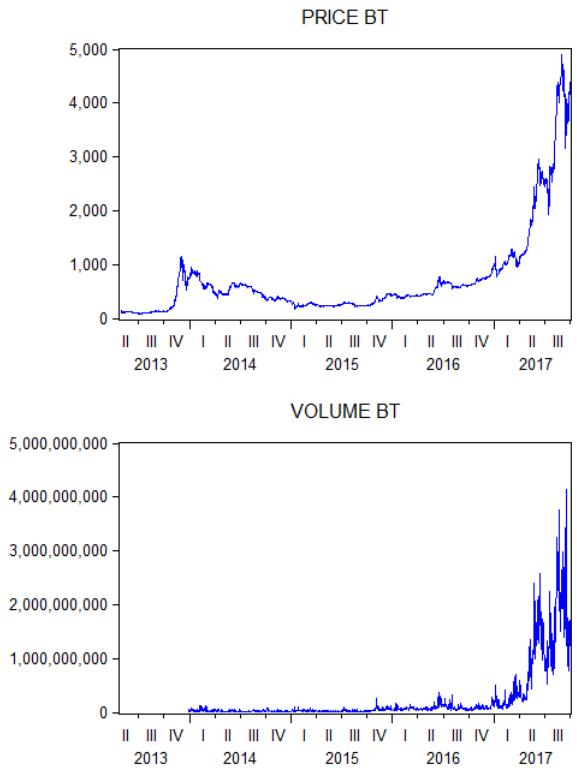

Figure 1. A Comparison Between Price and Volume [17].

2014. A more recent study is conducted by Blau [19], 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 [20]), Cheah and Fry [18], and many others.

There is no conclusive finding on whether the Bitcoin is a speculative investment asset or a currency. Glaser et al. [21] 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 [22]. They found Bitcoin can offer diversification benefits after looking into the correlation between Bitcoin and other asset classes. Gandal and Halaburda [23] 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 [24] 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. [25].

V. 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 [26]–[28]. Dyhrberg [26] 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 [29] 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.

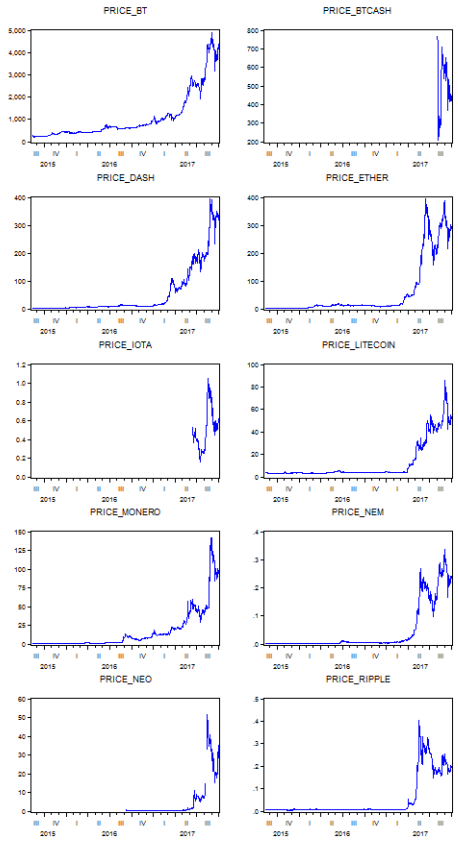

Figure 2. A Co-Movement View of Crypto-Currencies Based on Price [17].

Bouri, Azzi and Dyhrberg [28] 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 [30]. The results show limited evidence of hedging and safe haven properties of the Bitcoin; however, Bitcoin still can be an effective diversifier. In Figure 3, we see how a basket of crypro-currencies compare with each other based on volume.

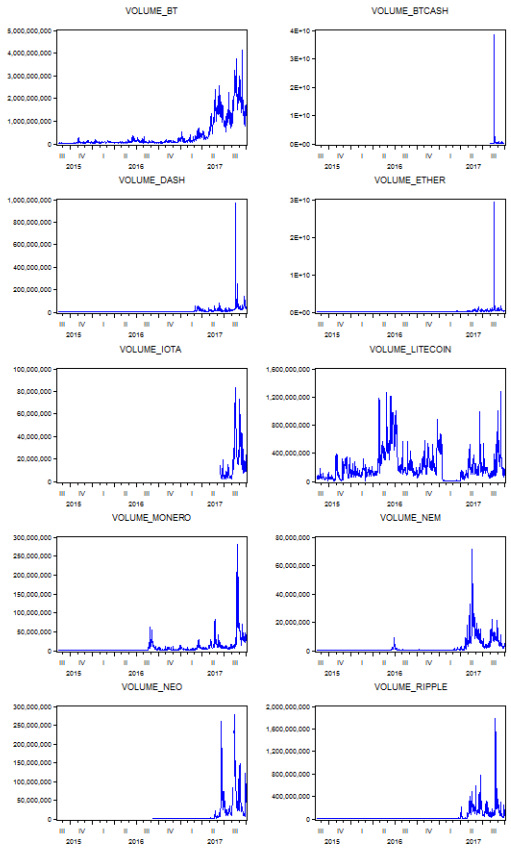

Figure 3. A Co-Movement View of Crypto-Currencies Based on Volume [17].

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 cryptocurrencies.

The 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.

The 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 comovement of price of a bundle of croptocurrencies 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 [31] reduces the electronic and computational burden of Bitcoin mining by replacing the proof-of-work mining with proof-of-stake, assigning block chain duties in proportion to coin holdings. Zerocash [32], which is not yet operational, will seek to improve privacy protections by concealing identifiers in

the public transaction history. Peercoin [33] 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. [34] 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.

VII. 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 for us. 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 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 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.

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 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 becoms worthwhile to spend the kind of money it takes to perpetrate such an attack.

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. 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 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 eliminat 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 othrwise 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, accessability 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 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/ [Retrieved: December 2017]

[2] PWC, "UK Information Security Breaches Survey - Technical Report 2012," London, Tech. Rep. April, 2012. [Online]. Available: www.pwc.com www.bis.gov.uk [Retrieved: December 2017]

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

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

[5] 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.

[6] 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.

[7] 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.

[8] N. Houy, "The Economics of Bitcoin Transaction Fees." GATE WP 1407 Université de Lyon, Groupe d'Analyse et de Théorie Economique (GATE), February. [Online] Available: http://ssrn.com/abstract=2400519 [Retrieved: December 2017]

[9] 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.

[10] E. K. Kogias et al., "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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

[17] Coindesk, "Coindesk," 2017. [Online]. Available: https://www.coindesk.com/ [Retrieved: December 2017]

[18] 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.

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

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

[21] F. Glaser, K. Zimmermann, M. Haferkorn, M. C. Weber, and M. Siering. "Bitcoin—Asset or Currency? Revealing Users' Hidden Intentions." Proceedings of the 22nd European Conference on Information Systems, Tel Aviv, June 2014.

[22] 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.

[23] 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.

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

[25] 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.

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

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

[28] E. Bouri, G. Azzi, and A. H. Dyhrberg, "On the return-volatility relationship in the bitcoin market around the price crash of 2013". Economics: The Open-Access, Open-Assessment E-Journal, 11:1–16.

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

[30] 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.

[31] NXT, "NXT Platform," 2017. [Online]. Available: https://nxtplatform.org/ [Retrieved: December 2017]

[32] Zerocash, "Zerocash," 2017. [Online]. Available: http://zerocash-project.org/ [Retrieved: December 2017]

[33] Peercoin, "Peercoin," 2017. [Online]. Available: https://peercoin.net/ [Retrieved: December 2017]

[34] 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.