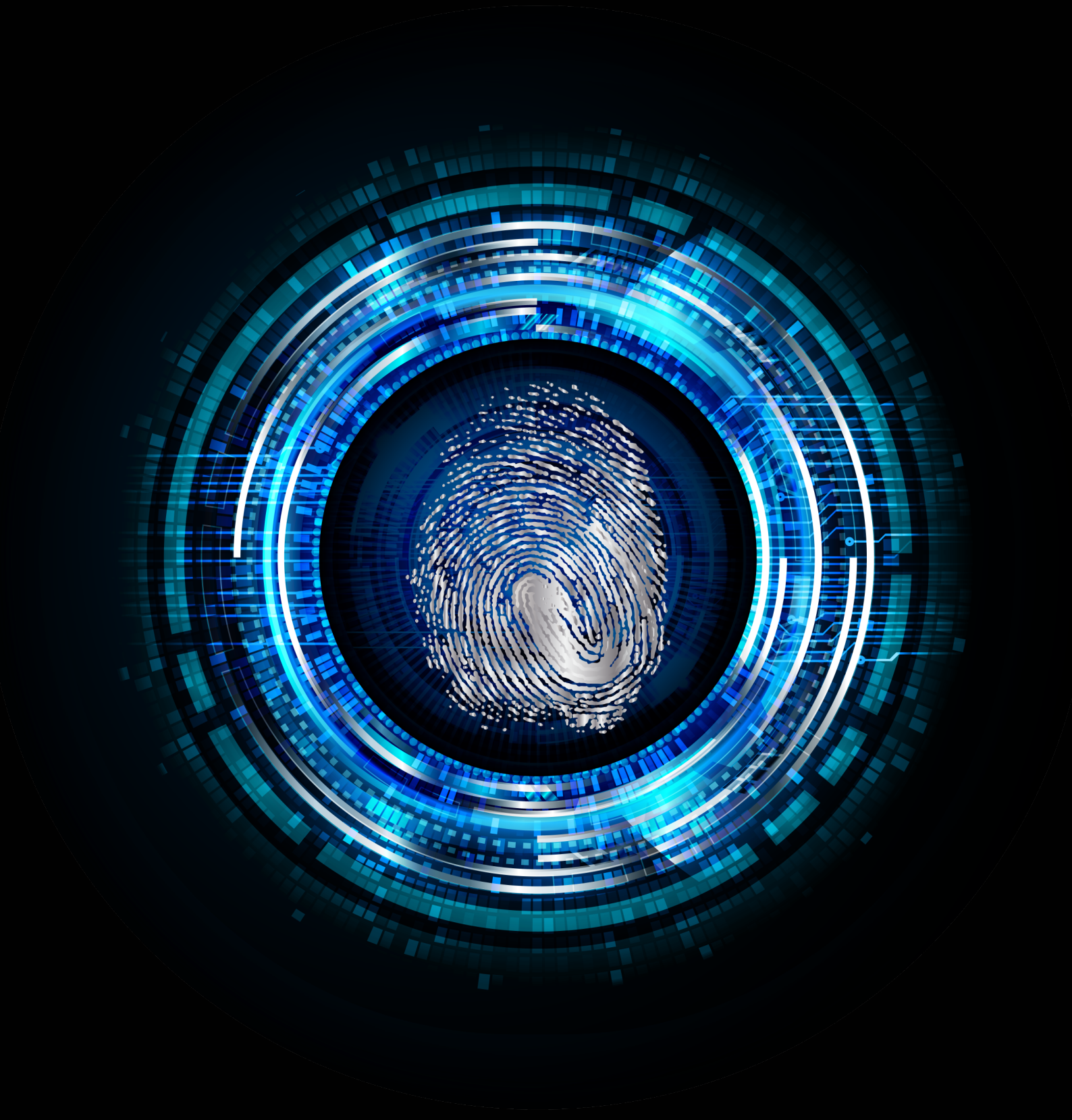
Deloitte.



Blockchain & Cyber Security. Let's Discuss

Written by the Deloitte EMEA Grid Blockchain Lab with insights from Deloitte global cyber SMEs from members firms including Ireland, the United States of America, China, U.K, Argentina, Germany, Spain, Portugal and Israel

Authors:
Eric Piscini (Deloitte U.S.), David Dalton (Deloitte Ireland) and Lory Kehoe (Deloitte Ireland)

Special Acknowledgements:
Niamh O'Connell (Deloitte Ireland) and Guilherme Campos (Deloitte Portugal)

For more information please contact:

Eric Piscini
Principal
T: +14046312484
E: episcini@deloitte.com

David Dalton
Partner
T: +353 1 417 4801
E: ddalton@deloitte.ie

Lory Kehoe
Director
T: +353 1 417 3084
E: lkehoe@deloitte.ie

Introduction

Blockchain is gaining traction today, but critics who question the scalability, security, and sustainability of the technology remain. Deloitte member firms across the globe are continuing to collaborate to build blockchain capabilities to develop world class solutions and services for clients.

In this paper Deloitte's global blockchain and cyber security experts from around the globe have joined forces to assess specifically the security of blockchain technology.

More specifically, this global point of view will review and address:

- Blockchain's current level of security from a system and data perspective for both public and private ledgers
- The CIA security triad model, composed of three areas; (1) Confidentiality, (2) Integrity and (3) Availability will be referenced to assess the current maturity level of blockchain technology
- Authentication, Authorization and Audit (AAA), and Non Repudiation, fundamental security aspects for protecting information and designing / managing new systems and networks[1] will also be addressed

For the purpose of this article public blockchains are defined as permission-less, where data is publically available to anyone who wishes to participate in the network. Whereas, private blockchains are permission based platforms established generally by groups of firms, individual firms or divisions within an organization (e.g. a consortia), where data can only be accessed by those users who are part of such consortia and properly authenticated.

Blockchain Context

Blockchains (or distributed ledger technology) evolution has been compared to the early rising of the internet with comments and arguments of the technology's potential to disrupt multiple industries including Healthcare, Public Sector, Energy, Manufacturing and particularly Financial Services, where it is predicted to be the beating heart of finance[2] and the ultimate provider of a new industry fabric. According to David Schatsky, Managing Director at Deloitte U.S., *"the technology provides a way of recording transactions or any digital interaction in a way that is secure, transparent, highly resistant to outages, auditable, and efficient"*[3]. Such is the interest in the technology that in 2016 alone over $1.billion was invested in blockchain by financial services and technology firms globally & such investments are predicted to increase exponentially over the next five years[4]. According to a 2016 Gartner report, the technology is at the peak of a hype cycle[5] and it has become a priority for industry leaders to understand how it can transform their

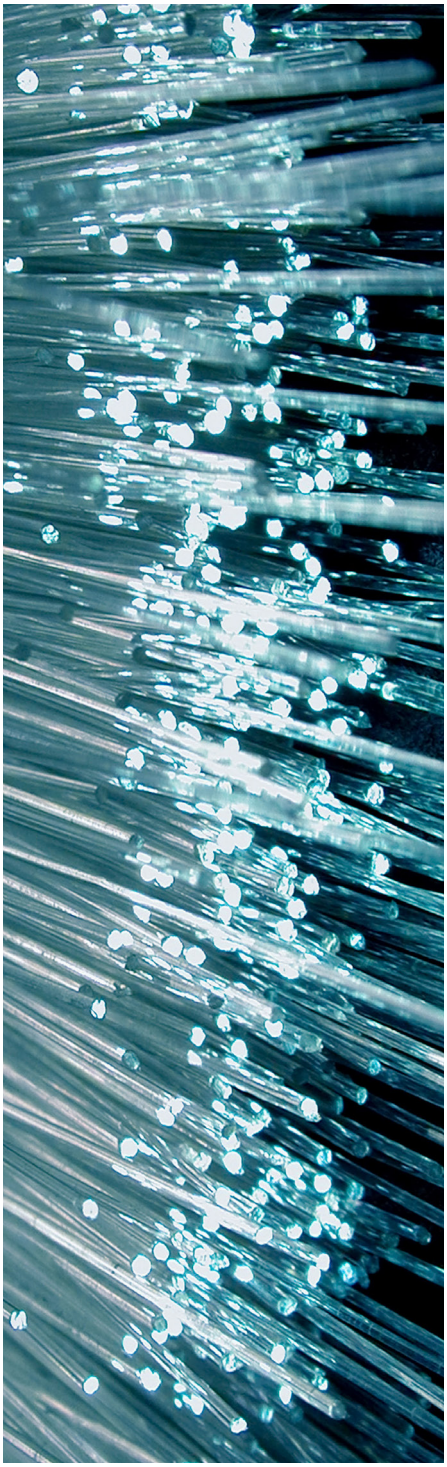
1 http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting
2 http://uk.businessinsider.com/world-economic-forum-potential-of-blockchain-in-financial-services-2016-8
3 https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/trends-blockchain-bitcoin-security-transparency.html
4 https://www.bloomberg.com/news/articles/2016-06-23/finance-firms-seen-investing-1-billion-in-blockchain-this-year
5 http://www.gartner.com/newsroom/id/3412017

business models and alter value chains to gain competitive advantage and perhaps more fundamentally to remain relevant. However, today the technology remains at the peak of inflated expectation and is about to dive down into the trough of disillusionment. Milan Sallaba, Deloitte Germany's Technology-Sector Leader points out *"some of the early use cases we have seen were deploying blockchain for the sake of it, without sufficiently focusing on the core attributes of the technology, which indeed has the potential to generate substantial process efficiencies across many industries and is likely to contribute to entirely new business models."* For this reason the blockchain industry is now moving beyond proof of concepts to production pilots with business cases being built to identify just how beneficial the technology is. A fundamental component of such reviews is a focus on security and privacy which must be addressed and tested if this technology is to become the real catalyst for social and industrial change that so many think it can be.

Cyber Security Context

The high level of dependency on technology and the internet today has resulted in new business models and revenue streams for organizations but with this comes new gaps and opportunities for cyber attackers to exploit. Cyber-attacks have become increasingly targeted and complex due to more sophisticated pieces of malware being leveraged and the increasing threat of professional cyber organizations[6]. These cyber criminals are attempting to steal valuable data, such as intellectual property (IP), personal identifiable information (PII), health records, financial data, and are resorting to highly profitable strategies such as monetizing data access through the use of advanced ransomware techniques or by disrupting overall business operations through Distributed Denial of Service (DDoS) attacks[7]. In October 2016, one of the biggest domain name service (DNS) providers Dyn experienced a major distributed denial of service (DDoS) attack that disrupted the service of several high traffic websites such as Twitter, Netflix, and Spotify[8]. Deloitte's cyber risk professionals suggest organizations follow the secure, vigilant and resilient approach when managing cyber regardless of the type of technology adopted[9].

So what about blockchain? Will the technology be a cyber security help or hindrance? According to Ed Powers, Deloitte's U.S. Cyber Risk Lead, *"while still nascent, there is promising innovation in blockchain towards helping enterprises tackle immutable Cyber Risk challenges such as digital identities and maintaining data integrity."* Blockchains could potentially help improve cyber defense as the platform can secure, prevent fraudulent activities through consensus mechanisms, and detect data tampering based on its underlying characteristics of immutability, transparency, auditability, data encryption & operational resilience (including no single point of failure). However as Cillian Leonowicz, Senior Manager at Deloitte Ireland opines *"blockchain's characteristics do not provide an impenetrable panacea to all cyber ills, to think the same would be naïve at best, instead as with other technologies blockchain implementations and roll outs must include typical system and network cyber security controls, due diligence, practice and procedures".*



6 https://www.fireeye.com/offers/thank-you/mtrends2017-download-confirmation.html
7 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
8 https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/
9 https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gra-Changingthegameoncyberrisk.pdf

Confidentiality

According to the National Institute of Standards and Technology (NIST), confidentiality refers to *"the property that sensitive information is not disclosed to unauthorized individuals, entities, or processes"*[10].

Ensuring only interested and authorized parties' access the correct and appropriate data to them is a common concern for organizations considering using a blockchain today. Protecting blockchain network access is fundamental in securing data access (particularly in private blockchains). If an attacker is able to gain access to the blockchain network, they are more likely to gain access to the data, hence authentication and authorization controls[11] need to be implemented, as is the case with other technologies. Although the technology was originally created without specific access controls (due to its public nature), there are some blockchain implementations starting to address the data confidentiality and access control challenges, by providing out of the box full block data encryption and AAA capabilities[12]. Full encryption of blockchain data ensures data will not be accessible by unauthorized parties while this data is in transit (especially if data is flowing through untrusted networks).

Network Access

In public blockchains there is no necessity to control network access as the chains protocols allows anyone to access and participate in the network, providing they firstly download the software. In contrast, private blockchains require that appropriate security controls are in place to protect network access. In a perfect world it would be tempting to assume that, because of its private nature, local networks and systems are already protected well behind an organizations perimeter by several internal security layers (such as firewalls, virtual private networks, VLANs, Intrusion Detection & Prevention Systems, etc.), through the adoption of a so called defense in depth strategy. However, perfect world scenarios are a utopia, especially in security, and relying solely on the effectiveness of such security controls is clearly insufficient. For this reason, security best practices recommend security controls (such as access controls) should also be implemented directly at the application level, being that the first and most important line of defense, particularly in scenarios such as an attacker gaining access to the local network or where a malicious insider is already present. Organizations, when considering their blockchain network architecture, will also need to consider how to treat uncommunicative or intermittently active nodes as the blockchains will need to continue functioning without these offline nodes but also must be able to bring them back up to speed providing they return to their original function[13].

"Every organization has to consider the inherent link between performance, innovation and cyber risk, and realize that protecting everything would be economically impractical and would likely impede some of the most important strategic initiatives", according to Andres Gil, Deloitte's LATCO Cyber Risk Lead. Organizations must assess its changing risk profile and determine what level and type of cyber risks are acceptable, considering what's most important and invest in cost-justified security controls to protect the most important assets. It's essential to address weak points along the end-to-end process, with the awareness that insiders, vendors and trusted partners at any point can be the source of errors or intentional actions that open the door to incidents. Organizations should implement an overall cyber security program to address these challenges including a governance framework with roles, processes, accountability measures, well-articulated performance metrics, and most of all, an organization-wide shift in mindset. In line with these requirements, blockchain can provide advanced security controls, for example, leveraging the public key infrastructure (PKI) to authenticate and authorize parties, and encrypt their communications (PKI is a set of roles, policies, and procedures required to create, manage, use, store, and revoke digital certificates and manage public-key encryption[14]).

Public blockchains could potentially be compared to the internet, where organizations could exchange and retrieve information with anyone who has access to a service provider. Whereas private chains could be compared to organizations intranet pages, where information is only shared and exchanged internally with those who have been authorized to access the site. If blockchains become widely adopted organizations will need to ensure they implement security controls to provide authentication, authorization, and encryption in order to properly protect data access. *"Attackers always seek for low hanging fruit from site to site, and confidential information stored on a blockchain will likely become a high priority target if such controls*

10 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
11 http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting
12 https://media.readthedocs.org/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf
13 https://hbr.org/2017/03/how-safe-are-blockchains-it-depends
14 http://searchsecurity.techtarget.com/definition/PKI

were inadequate", according to Eva Yee Ngar Kwok, Risk Advisory Technology Risk Partner at Deloitte China / Hong Kong.

Data Access & Disclosure

Today, if an attacker gains access to a blockchain network and the data, this does not necessarily mean the attacker can read or retrieve the information. Full encryption of the data blocks can be applied to data being transacted, effectively guaranteeing its confidentiality, considering the latest encryption standards are followed. The use of end to end encryption, which has become an important topic of discussion in recent years[15], where only those who have authorization to access the encrypted data i.e. through their private key, can decrypt and see the data. Using encryption keys in conjunction with PKI can provide organizations with a higher level of security. Encrypting data on a blockchain can provide organizations with a level of protection from a data confidentiality and data access control perspective. As an example, implementing secure communication protocols on blockchain (assuming the latest security standards and implementation guides), guarantees that even in a situation where an attacker tries to do a man-in-the-middle attack the attacker won't be able to either forge the interlocutor's identity or disclose any data while in transit. Even in an extreme situation scenario where long-term private keys are compromised, past sessions are kept confidential due to the perfect forward secrecy properties of security protocols[16] .

Although blockchain users generally back up their private key in a secondary place such as a cold storage, theft of private keys remains a high risk. It's important to note that keys are used for several purposes in the blockchain ecosystem: protection of user information, confidentiality of data, and authentication and authorization to the network. According to Lior Kalev, Director leading Deloitte Israels Cyber Risk Services, "*People want and need to be connected to their data at all times from any location and any device which bring about new cyber risks which makes network access management in enterprise and global organizations inherently challenging".* Organizations need to be conscious that accessing their blockchain account from multiple devices puts them at a higher risk of losing control of their private keys. Considering this, its important entities follow suitable key management procedures (such as the IETF or RFC 4107 cryptographic key management guidelines)[17] and develop secure key governance practices internally, since this will be fundamental to the security of the blockchain network. According to Artur D'Assumpção, head of Cyber Risk / Cyber Security at Deloitte Portugal *"In an enterprise environment it will be fundamental to properly secure secret key material as to not jeopardize the ledger confidentially and integrity. An example of adequate protection is the use of special purpose key vaults that implement technologies such as Hardware Security Modules to secure master secrets and provide a highly secure and tamper-resistant environment."*

Today's cryptographic algorithms, used for public/private key generation, rely on integer factorization problems, which are hard to break with current computing power. According to Jacky Fox, Deloitte Ireland's Cyber Lead, *"Advances in quantum computing will become significant for the security of blockchain due to their impact on current cryptography practice.* For example Bitcoin uses cryptographic algorithms to produce a public/private key pair and an address which is derived using hashing and checksum operations on the public key. Exposure of the address alone is not high risk. However exposure of the address and the public key required to transact will potentially, given sufficient advances in quantum computing, enable the derivation of the private key. Jacky Fox highlights *"while commercial quantum computing is not available as a large scale reality it makes sense to plan now for the move to quantum resistant cryptography. NIST is currently in the process of developing quantum resistant cryptography standards and the NSA are recommending their suppliers plan to implement SHA-384 instead of SHA-256".*

15 https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/
16 https://www.wired.com/2016/11/what-is-perfect-forward-secrecy/)
17 https://tools.ietf.org/html/rfc4107

Integrity

Integrity is defined as the *"guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity"according to NIST"*[18].

Maintaining data consistency, and guaranteeing integrity, during its entire life cycle is crucial in information systems. Data encryption, hash comparison (data digesting), or the use of digital signing, are some examples of how system owners can assure the integrity of the data, regardless of the stage it is in (in transit, at rest and in use storage). Blockchain's built in characteristics, immutability and traceability, already provide organizations with a means to ensure data integrity.

Immutability

Blockchain technology can be regarded as a secure technology, from the point of view that it enables users to trust that the transactions stored on the tamper proof ledger are valid. The combination of sequential hashing and cryptography along with its decentralized structure makes it very challenging for any party to tamper with it in contrast to a standard database[19]. This provides organizations using the technology with assurance about the integrity and truthfulness of the data. The consensus model protocols associated with the technology also present organizations with a further level of assurance over the security of the data, as generally 51%[20] of users in public and private blockchains need to agree a transaction is valid before it is then subsequently added to the platform. Organizations can implement further mechanisms to prevent and control ledger splitting in the event of a 51% cyber control attack occurring for example monitor if one of the nodes increases processing power and is executing a significantly higher number of transactions[21].

Right to be Forgotten

With regards to data immutability, it is important to consider how blockchains will fit side by side with data privacy laws. How to implement the right to be forgotten in a technology that guarantees that nothing will be erased is an interesting challenge for which, fortunately, there are multiple solutions. One solution is to encrypt the personal information written in the system, to ensure that, when the time comes, forgetting the keys will ensure that sensitive information is no longer accessible. Another possibility is to focus on the value of blockchain to provide unalterable evidence of facts by writing the hash of transactions to it, while the transactions themselves are stored outside of the system. This maintains the integrity of transactions, while enabling the ability to erase the transactions, leaving only vestigial traces of forgotten information in the blockchain.

18 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
19 https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/
20 https://learncryptography.com/cryptocurrency/51-attack
21 https://learncryptography.com/cryptocurrency/51-attack

Traceability

Every transaction added to a public or private blockchain is digitally signed and timestamped, which means that organizations can trace back to a specific time period for each transaction and identify the corresponding party (via their public address) on the blockchain. This feature relates to an important information security property: non repudiation[22], which is the assurance that someone cannot duplicate the authenticity of their signature on a file or the authorship a transaction that they originated. This out of the box functionality of the blockchain increases the reliability of the system (detection of tamper attempts or fraudulent transactions), since every transaction is cryptographically associated to a user.

Any new transaction added to a blockchain will result in the change of the global state of the ledger. The implication of this is that with every new iteration of the system, the previous state will be stored, resulting in a fully traceable history log. The technology's audit capability provides organizations with a level of transparency and security over every interaction. From a cybersecurity perspective, this provides entities with an extra level of reassurance that the data is authentic and has not been tampered with.

Smart Contracts

Smart contracts, computer programs running on the ledger, have become a core feature of blockchains today[23]. This type of program can be used to facilitate, verify, or enforce rules between parties, allowing for straight through processing and interactions with other smart contracts. Such software provides a large surface area for attack, so an attack on one smart contract could have a domino effect on other parts of the platform i.e. the language itself or implementation of contracts. During the DevCon 2 event in Shanghai a DDoS attack exploiting a vulnerability in the Go-based Ethereum client's smart contract implementation prevented miners from mining further blocks[24].

Blockchain brings a new paradigm to software development and, as such, secure development standards and practices (such as implementing secure coding and security testing) need to be implemented (and updated) to account for smart contract life cycle (creation, testing, deployment, and management). According to Diego Rodriguez Roldan, Director at Deloitte Advisory practice in Spain, *"it will be necessary to apply methodologies such as the Secure Software Development Life Cycle (S-SDLC) in order to minimize the threat of a critical bug during the life cycle smart contracts"*. The attack on The DAO, a decentralized organization built on top of Ethereum, is an example where smart contracts was attacked. An attacker managed to exploit a bug in a smart contract that led to the theft of 60M Ether[25].

Data Quality

Blockchain technology does not guarantee or improve data quality. Private and public blockchains can only take responsibility for the accuracy and quality of the information once it has been inputted into the blockchain, meaning that you need to trust the data being pulled from organizations existing source systems is of good quality, as is the case with all other technology systems. According to Prakash Santhana, Advisory Managing Director at Deloitte U.S. *"the biggest vulnerability in the blockchain framework will lie outside the framework in 'trusted' oracles. A corrupted oracle could potentially cause a domino effect across the entire network. An attack on an oracle could either be direct or indirect via third parties connected to the oracle"*. Oracles result in untrusted data entering a trusted environment and so organizations might need to consider using multiple oracles to increase the trust in the integrity of the data entering the blockchain from the oracle.

Providing the inputted data is accurate, blockchain technology can play a powerful role in transforming the data output as the technologies near real time capabilities, grant organizations to verify transactional data faster than any other system, facilitates organizations to take more proactive actions. Given that data will inevitably be transmitted from an organizations source system to a blockchain, entities must ensure the exchange channels are secure as this is no doubt a point of attack and entry for attackers.

22 http://searchsecurity.techtarget.com/definition/nonrepudiation
23 http://www.coindesk.com/making-sense-smart-contracts/
24 https://www.ethnews.com/looking-back-at-ethereum-in-2016
25 http://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/

Availability

NIST defines availability as "ensuring timely and reliable access to and use of information"[26].

Cyberattacks attempting to impact technology services availability continue to increase[27]. DDoSs, being one of the most common type of attacks[28], can also cause the most disruption to internet services and hence blockchain enabled solutions. The resulting implications are that websites get disrupted, mobile apps become unresponsive, and this can generate ever increasing losses, and costs, to businesses[29]. Given blockchains are distributed platforms, DDoS attacks on blockchains are not like regular attacks. They are costly as they attempt to overpower the network with large volumes of small transactions (or in the case of the recent Ethereum DDoS attacks, actions with disproportionately low gas costs costing €3,000)[30]. The decentralization and peer-to-peer characteristics of the technology make it harder to disrupt than conventional distributed application architectures (such as client-server), yet they are also subject to DDoS attacks, and as such adequate protection measures are still necessary, both at the network and application level[31]. The Bitcoin network withstood a DDoS attack in 2014[32], where attackers attempted to overflow the network with requests. According to Peter Gooch, Partner at Deloitte UK, Risk Advisory practice, *"this is likely to happen again, and estimates that DDoS attacks will increase in size and scale, with regular Terabit / second attacks straining the capacity of regional and even global internet infrastructure"*. This increase will be due largely to the growing installed base of insecure Internet of Things (IoT) devices, the online availability of DDoS malware, and the availability of ever higher bandwidth speeds. Although resilient, decentralised blockchain solutions depend on high availability, and DDoS attacks will remain a persistent threat.

26 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, pg 21
27 http://www.zdnet.com/article/ddos-attacks-increase-over-125-percent-year-over-year/
28 https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/
29 https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf
30 http://www.coindesk.com/so-ethereums-blockchain-is-still-under-attack/
31 https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/
32 https://www.forbes.com/sites/leoking/2014/02/12/bitcoin-hit-by-massive-ddos-attack-as-tensions-rise/#2442aa4246ad

No Single Point of Failure

Blockchains have no single point of failure, which highly decreases the chances of an IP-based DDoS attack disrupting the normal operation[33]. If a node is taken down, data is still accessible via other nodes within the network, since all of them maintain a full copy of the ledger at all times. The distributed nature of the technology solves the Byzantine General's problem[34] of false consensus.

Bitcoin, to date, is the most tried and tested platform in the market, which has successfully withstood cyber-attacks for more than 7 years[35] . Blockchain infrastructure evidently provides a further level in data accessibility, given that data is accessible through any of the nodes in the network, even in the event of a DDoS attack disrupting some of the nodes.

Even though a blockchain network is considered to have no single point of failure, organizations could still face risks from external events outside of their control. For example, a global internet outage would disrupt even a public blockchain network as distributed as Bitcoin or Ethereum, creating outages which would impact an organization's operations as with any other technology. Private blockchain networks with a lower number of nodes would need to ensure that their network is sufficiently distributed globally and resilient with no single points of failure on an organization or platform level to ensure continuous operation even in the event of a natural disaster or coordinated attack.

Operational Resilience

The combination of the peer to peer nature and the number of nodes within the network, operating in a distributed and 24/7 manner, make the platform operationally resilient. Given that both public and private blockchain consists of multiple nodes, organizations can make a node under attack redundant and continue to operate as business as usual. So, even if a major part of the blockchain network is under attack, it will continue to operate due to the distributed nature of the technology.

This does not mean that the network is completely "bullet-proof". Since blockchain's inception, in 2008, platforms have faced threats where attackers have attempted to jeopardize their stability, using different attack vectors. Transaction malleability, a bug found when transactions are in a pending validation status, resulted in an attack to the Bitcoin network in 2014[36], which impacted the users experience. In 2016, an attacker exploited the smart contracts in Ethereum, and the way they can be used, to create an overflow in the network, to the point where the creation of blocks, and validation of transactions were severely impacted, slowing the network[37]. This has been addressed with the creation of a hardfork (permanent divergence from the previous blockchain version)[38]. According to Suchitra Nair, Director at Deloitte U.K.'s Risk Advisory practice *"Operational resilience of the blockchain will be a key focus area for regulators and will need to be rigorously tested and evidenced by the firm to gain regulatory assurance. Senior management should be able to articulate the key risks underpinning the blockchain solution and the governance and control framework that has been established to manage them"*. The importance of involving regulators to facilitate in blockchain development and adoption is further mentioned by Deloitte's Asia Pacific Investment Management Leader, Jennifer Qin, who notes *"to make blockchain commercially viable to be fully adopted by business and governments, it has to be fully compliant with regulatory requirements, business customs and various business environments"*.

33 https://blog.ethereum.org/2016/09/22/transaction-spam-attack-next-steps/
34 https://ice3x.co.za/byzantine-generals-problem/
35 http://performermag.com/band-management/contracts-law/dot-blockchain-music-project/
36 http://www.coindesk.com/bitcoin-bug-guide-transaction-malleability/
37 http://www.coindesk.com/so-ethereums-blockchain-is-still-under-attack/
38 https://blog.ethereum.org/2016/11/18/hard-fork-no-4-spurious-dragon/

Secure. Vigilant. Resilient. Cyber Risk Program

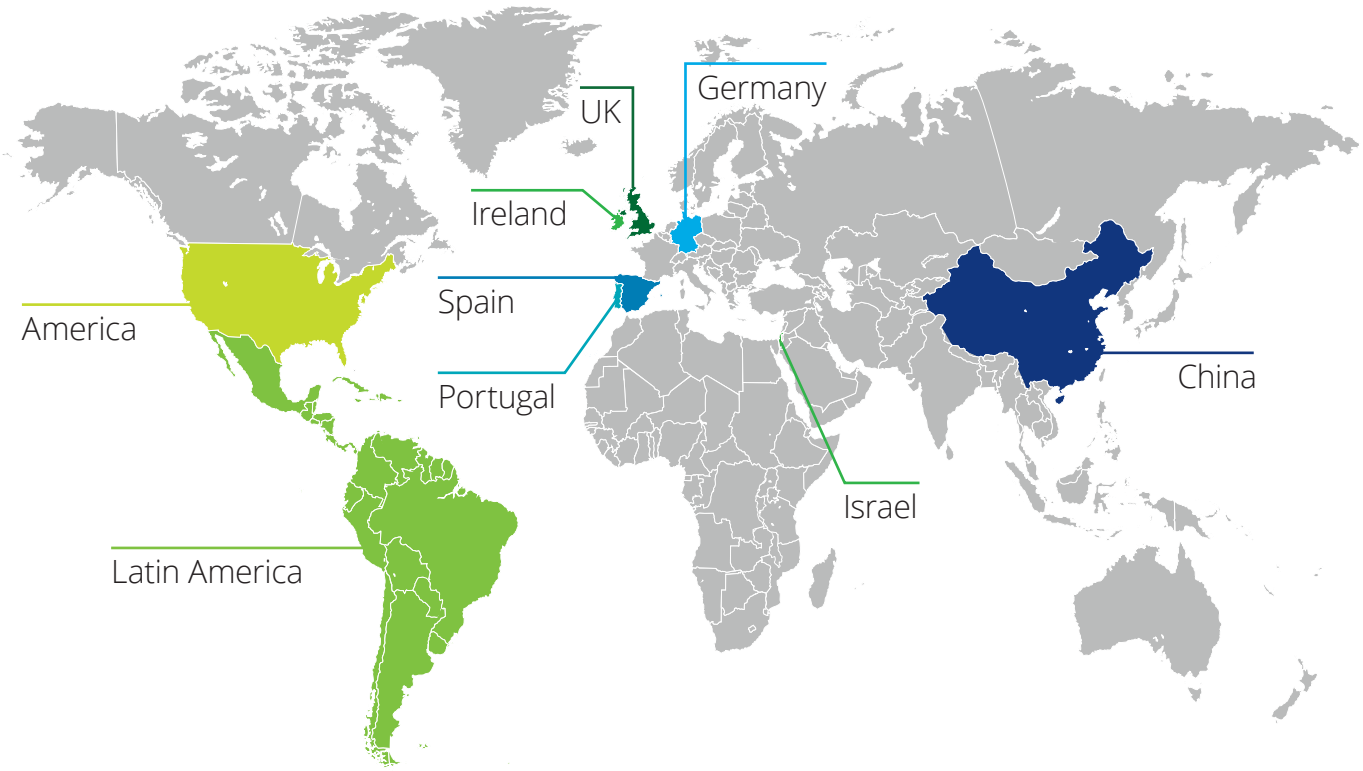
No cyber defense or information system can be regarded as 100 % secure. What is deemed safe today won't be tomorrow given the lucrative nature of cybercrime and the criminal's ingenuity to seek new methods of attack. Although some of blockchains underlying capabilities provide data confidentiality, integrity and availability, just like other systems, cyber security controls and standards need to be adopted for organizations using blockchains within their technical infrastructure in order to protect their organizations from external attacks.

Deloitte cyber professionals across the globe suggest entities follow our Secure, Vigilant & Resilient (SVR) cyber approach which will not only support entities to remain secure but also become more vigilant and resilient to evolving cyber threats. We believe that adopting this secure, vigilant and resilient approach to cyber is a key step in helping leaders continue to drive performance at their organizations[39].

As Eric Piscini, Deloitte's Global Blockchain Lead, U.S., highlights *"while cyber security is critical to the large adoption of blockchain, operations, technology architecture, consortium building, talent and global regulations are key components to be considered as well"*. To learn more about protecting your blockchain or more generally your business from cyber-attacks please contact our cyber and blockchain teams in your region.

39 https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gra-Changingthegameoncyberrisk.pdf

Deloitte Global Contributors List



Abhishek Biswas *(abiswas@deloitte.com)* – Deloitte US Advisory Senior Manager
Andres Gil *(angil@deloitte.com)* – Deloitte LATCO Cyber Risk Lead
Artur D'Assumpção *(adassumpcao@deloitte.pt)* – Deloitte Portugal Cyber Risk / Cyber Security Lead
Charles Ho Lam Low *(clow@deloitte.com.hk)* – Deloitte China Risk Advisory Technology Risk Manager
Cillian Leonowicz *(cleonowicz@deloitte.ie)* – Deloitte Ireland Senior Manager
Dave Clemente *(daclemente@deloitte.co.uk)* – Deloitte UK Risk Advisory Senior Manager
Diego Roldan Rodriguez *(drodriguezroldan@deloitte.es)* – Deloitte Spain Advisory Director
Edward Powers *(episcini@deloitte.com)* – Deloitte U.S Cyber Risk Lead
Eva Yee Ngar Kwok *(evakwok@deloitte.com.hk)* – Deloitte China Risk Advisory Technology Risk Partner
Fernando Picatoste *(fpicatoste@deloitte.es)* – Deloitte Spain Risk Advisory Partner
Irfan Saif *(isaif@deloitte.com)* – Deloitte US Advisory Principal
Jacky Fox *(jacfox@deloitte.ie)* – Deloitte Ireland Cyber Lead
Jennifer Yi Qin *(jqin@deloitte.com.cn)* – Deloitte Asia Pacific Investment Management Lead
Lior Kalev *(lkalev@deloitte.co.il)* – Deloitte Israel Cyber Risk Services Lead
Luciana Gaspari *(lgaspari@deloitte.com)* – Deloitte Latin America Risk Advisory Senior Manager
Milan Sallaba, Deloitte Germany's Technology-Sector Lead
Pablo Cabellos Rodriguez *(prodriguezcabellos@deloitte.es)* – Deloitte Spain Risk Advisory Manager
Peter Gooch *(pgooch@deloitte.co.uk)* – Deloitte UK Risk Advisory Partner
Prakash Santhana *(psanthana@deloitte.com)* – Deloitte US Advisory Managing Director
Suchitra Nair *(snair@deloitte.co.uk)* – Deloitte UK Risk Advisory Director
Vikram Bhat *(vbhat@deloitte.com)* – Deloitte US Advisory Principal
Yang Chu *(yangchu@deloitte.com)* – Deloitte US Advisory Senior Manager

Blockchain Lab Contacts:

U.S. Deloitte Blockchain Lab
140 Broadway, 49th Floor
New York, NY 100005
United States
T: +1 212 492 4000

EMEA Deloitte Blockchain Lab
Whitaker Court
Sir John Rogersons Quay
Dublin 2
Ireland
T: +353 1 417 2200

deloitte.com

Deloitte.