Chapter

Blockchain Applications in Cybersecurity

Oscar Lage, Santiago de Diego, Borja Urkizu, Eneko Gómez and Iván Gutiérrez

Abstract

Blockchain has been widely known thanks to Bitcoin and the cryptocurrencies. In this chapter, we analyze different aspects that relate to the application of blockchain with techniques commonly used in the field of cybersecurity. Beginning by introducing the use of blockchain technology as a secure infrastructure, the document delves into how blockchain can be useful to achieve several security requirements, common to most applications. The document has been focused on some specific cybersecurity disciplines to maintain simplicity: backup and recovery, threat intelligence and content delivery networks. As illustrated, some projects and initiatives are in the process of joining these two fields to provide solutions to existing problems.

Keywords: blockchain, DLT, trust, cybersecurity, IoT, IIoT

1. Introduction

Blockchain is a very-known term, which was used for the first time in [1], where Satoshi Nakamoto described Bitcoin in 2008. Bitcoin is the best-known implementation of blockchain, and it is basically the implementation of a cryptocurrency. However, blockchain is much more than that, being seen as the service and structure behind cryptocurrencies to maintain records for currency transactions between untrusted participants. Nowadays, in addition to cryptocurrencies (hundreds of currencies exist today that use blockchain technology or derivatives), many other application areas rely on blockchain technology like energy trading, health, supply chain, manufacturing, identity management, e-government, etc.

Blockchain presents itself as a distributed ledger, referring this concept to the way a database is shared between several participants on a peer-to-peer network, without a central authority overseeing the process. In the case of blockchain, this ledger is arranged, as its name suggests, in an ordered chain of blocks, each of which agglutinates transactions in order. A block, therefore, is basically a structure composed of a header and a body containing transactions in order. Blocks are timestamped and signed by its creator. The way these blocks constitute a chain is through a pointer to the previous block; the header of each block contains a cryptographic hash of the previous block so that a block is linked to the previous one (while ensuring the immutability of that previous block). The very first block from which a blockchain is constituted is known as the "genesis block" (**Figure 1**).

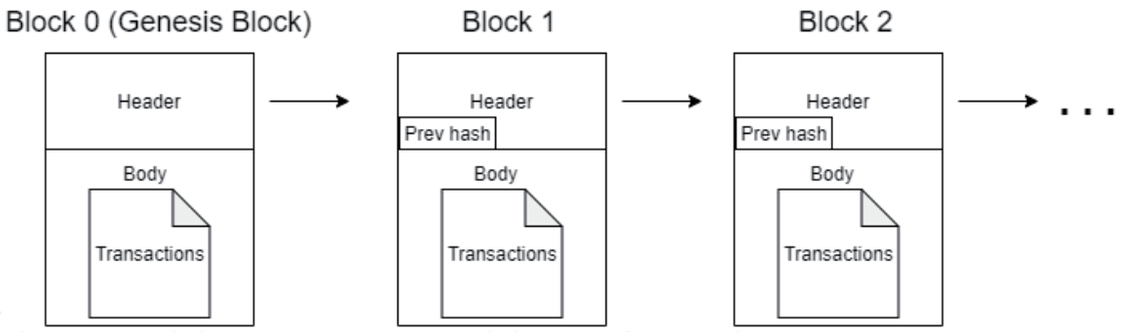

Figure 1.
Blockchain as a chain of blocks.

It should be noted again that a blockchain is a type of Distributed Ledger Technology (DLT) with a series of specific features. By DLT, we mean any type of technology that makes use of a distributed ledger and, therefore, not all DLTs are blockchains. As an example, new generation technologies, such as IOTA or Hashgraph, are based on DLT different from the blockchain, being named blockless technologies, which are out of the scope of this document.

As mentioned, in blockchain, the ledger is distributed between participants of a decentralized network without any central authority. In a public non-permissioned blockchain, all participants in the network keep a copy of the ledger, while in other more complex or restrictive kinds of blockchain, different ledgers can be held by subsets of participants. As an example of this statement, Hyperledger Fabric is presented as a permissioned blockchain technology, which allows us to separate the different nodes into different channels, having the nodes in the same channel the same copy of the ledger. At first sight, such kind of systems could be prone to issues related to the ledger synchronization. If any participant had the ability to promote their own version of the ledger and thereby their own version of the transactions, they could try to make a profit from it. However, how blockchain avoids this sort of incidences is through consensus mechanisms.

Consensus mechanisms govern the way participants storing and verifying blocks agree on one common version of the facts (a shared truth). The Consensus allows nodes to reliably validate new blocks in the network. There are a variety of proven types of consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT) or Proof of Elapsed Time (PoET), among other not-so-known ones, such as [2, 3], for example.

The most widely adopted consensus algorithm today is Proof of Work, used in both Bitcoin and Ethereum. Proof of Work basically consists of the resolution of a computationally complex challenge (related to the block itself) as a condition for the insertion of a block in the chain. The participants of the blockchain compete for the resolution of this challenge in return for a reward. The challenge is difficult to solve, but easy to verify so that the rest of the participants can easily verify the resolution of the challenge and agree on the new block. This algorithm guarantees consensus as long as no participant has more than half the computing capacity of the network, at the cost of high energy consumption. This high energy consumption and wastage of computing capacity is driving blockchain networks like Ethereum to migrate to lighter consensus algorithms, such as Proof of Stake.

The most used cryptographic function in Proof of Work is the hash. Hashes are trapdoor functions, which mean they are really easy to compute in one direction, but really hard in the opposite (find its inverse). When a participant of the network (called miner) finds a solution for a hash matching certain properties, it is enabled to assemble a new block and broadcast it. Upon reception, every other participant

can efficiently check that the block is valid given that is linked to the last one and matches the properties required by the network. This validation can be computed efficiently due to hashes being trapdoor functions. The consensus is reached when every participant has the same blocks, in other words, every participant agrees on the chain composition (longest blockchain). Hashes are also key tools for verifying data integrity and for the cryptographic signature process.

All this said, what advantages do we get with the use of blockchain? What leads us to adopt a network with such a load of processing and redundancy? All this complexity is necessary to constitute a decentralized network composed of multiple participants that reach a common consensus without the intervention of a central authority; to build a transparent and immutable ledger verifiable by itself; to establish a contract without the intervention of a notary (in fact, applications running on a blockchain are known as smart contracts). And all these goals are achieved with the highest level of trustworthiness and availability. Of course, blockchain is not the solution to everything. It is not the right solution for systems governed by a single central authority or to store data whose integrity and source is not relevant. It is a new paradigm that ensures the deterministic execution of a contract and the incorruptibility of the data in a ledger with full guarantees and without the intervention of a third party.

More technical information has been presented by [4, 5] so that the reader can obtain further knowledge on the functioning of protocols.

2. Blockchain as a secure ledger

Once blockchain technology has been introduced, the focus is on the fulfillment of the information security properties it provides.

Focusing on data integrity, blockchain ledger is immutable. Every transaction in a block is cryptographically signed by its sender, every block in the blockchain is cryptographically signed by its miner, every block contains a hash of the immediately preceding block and all the participants in the blockchain network reach a consensus about the chain as the shared truth. To alter a single transaction in the blockchain, an attacker should alter each subsequent block accordingly, resolve the consensus challenge of that block and subsequent blocks, and persuade more than 50% of network participants to adopt the new chain. That situation is close-to-impossible, due to the hashing properties and the amount of computational and electrical power required to achieve this goal. Blockchain is tamper-resistant and integrity is the greatest of its merits.

Merkle trees are a fundamental use of hashing in blockchain technologies that have not been mentioned before in the article. Merkle tree summarizes all transactions in a block into a single fingerprint, allowing to verify that all transactions in the block have been included without modification. Below we can find an example of one of these Merkle trees (**Figure 2**).

As we can see above, each leaf in the Merkle tree is a hash of transactional data and hashing is applied recursively over each subset of hashes forming the tree structure. Merkle trees are not only applied to block transactions but sometimes also to the ledger state (the result of the execution of all ledger transactions).

Non-repudiation is another information security property intimately linked to integrity. Since every transaction in the blockchain is cryptographically signed by its sender and the chain is immutable, the sender can never deny having ordered the transaction. However, that sender, in general, cannot be associated with a physical entity, but only with an account (as we will explain when discussing about privacy).

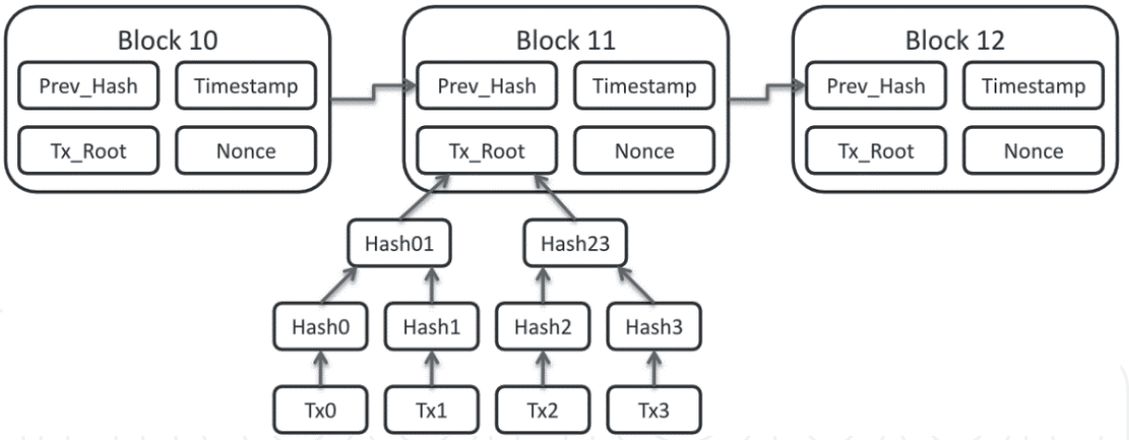

Figure 2.
Merkle tree.

In terms of availability, the distributed character of blockchain network makes it highly available. In addition, transactions on public blockchain networks usually involve a cost to the sender equivalent to their processing and storage consumption. This cost results in a reward for the miner of the block containing the transaction. Furthermore, it protects against Denial of Service (DoS) attacks, since an attack involves a cost proportional to the resources consumed for a potential attacker. For example, in Ethereum MainNet, this cost is reflected in the concept of gas. Gas represents the computational and storage cost of the transaction. At the same time, this gas has a variable cost in Ether, Ether that is obtained by mining or buying it. The availability concept is linked with the anti-SPoF (anti-Single Point of Failure) concept. Preventing a SPoF is usually a mandatory requirement when it comes to critical applications and, which need to offer a high availability rate, and even not-so-critical ones. If this point of failure is exploited, accidentally or intentionally by an attacker, the whole ecosystem breaks down, so it's interesting to be able to use resilient infrastructures, like Blockchain, to avoid this issue.

As for privacy, it is important not to confuse this concept with confidentiality, although they usually come hand in hand. In general, public blockchain networks bind transactions to accounts. These accounts are represented by a public-private key pair and may have a state associated with them, but they are not usually associated with an entity or individual. Only the individual in possession of the corresponding private key can launch a transaction on behalf of the account through a cryptographic signature, but the identity of the individual behind the key pair is unknown. In this way, a high degree of privacy is offered thanks to this pseudo-anonymity. Of course, there are identity management frameworks for blockchain, but these frameworks are not part of the core of a classic blockchain network.

One of the strong points of blockchain technologies is the transparency of transactions, a concept that in general is at odds with confidentiality (understood as encryption). Therefore, and except for specific blockchain technologies and private networks, blockchain does not provide encryption capabilities and this, if applies, must be implemented at the application level.

On the other hand, authorization is usually left to the application level in regular non-permissioned blockchain networks, while it can be part of the core of the technology in permissioned blockchain networks.

In short, we can conclude that blockchain is an extremely secure and resilient technology, but in general does not include confidentiality (understood as encryption) among its main objectives.

3. Blockchain for backup and recovery

Having shown to the reader the blockchain capabilities as a secure ledger, this section wants to analyze blockchain as a support tool to implement backup and recovery strategies. We have chosen this use case because it shows in a different way another use of blockchain, far from the common ones which usually appear in the literature.

One of the most innovative applications of blockchain technologies is to use it by secure storage and recovery systems. A Backup & recovery system usually has the following features:

- **Continuous/Automatic data backup**: It ensures that the changes you make to your files are simultaneously copied to the storage location. This lets you recover even the most recent changes in case of data loss, thus lowering your recovery point objective.

- **Incremental backup**: This is a type of backup where only the changes are copied, not the full file. This reduces the time taken for copying data and does not slow down your work.

- **Instant recovery**: This feature allows a backup snapshot to run temporarily on secondary storage to reduce the downtime of an application.

- **Data deduplication**: It eliminates duplicate data record blocks while data is transferred to the backup storage location. This reduces the network load and the storage space you require.

- **Error-free copy**: Data backup software features also ensure that the data copied from a source and stored at the backup server are the same and do not mismatch nor contain errors.

Historically, backup and recovery procedures were applied mainly to general-purpose devices in the enterprise environment. The number of incidents grows daily, and the consequences are increasingly alarming as, for example, security holes in IP cameras [6], DDOS attacks generated from the Mirai botnet [7, 8] known as Dyn Attack or event take control of a vehicle [9]. Due to these problems, Backup & Recovery systems are being extended to cover these devices too.

3.1 General-purpose devices

From the point of view of general-purpose systems, the main challenge that blockchain is expected to solve is the control data from tampering attacks; directly related to the integrity of the data.

We could find proprietary solutions that offer blockchain backup services at an enterprise level, see [10]. This solution provides mechanisms to ensure that legal documents existed on certain dates or to certificate authenticity of medical records.

3.2 IoT devices

Most IoT systems are managed through firmware so ensuring the integrity and authenticity of the firmware update of the devices is a complex and critical task that must be carefully addressed. In addition, it may happen that multiple devices

with their various subsystems need to be updated urgently and simultaneously, for example, to apply a critical fix. Therefore, the high availability of updates is a requirement.

Most existing solutions for firmware upgrades depend on the client-server model in which the manufacturer delegates the firmware distribution process to the suppliers of its products. The central client-server architecture has the drawback to be a Single Point of Failure (SPoF), and in case the server is not available IoT devices cannot access resources (updates). There are two approaches: manual and automatic.

On the one hand, in the manual update process, the device owner must start the firmware update process. In general, this type of update is adopted by devices that have limited bandwidth or directly it is the owner who decides to do it this way. However, the manual firmware update mechanism is not as efficient as the owner of the device must perform all operations manually. In addition, there is a high probability that human error may occur during the firmware update process or that devices are outdated due to lack of resources for updating.

On the other hand, the automatic updating seems more tempting to be adopted today. This way, the manufacturer of the IoT device could initiate the firmware update without the active participation of the device owner. The current automatic firmware update process uses the client-server architecture, where the repository of the provider is the server and the IoT device becomes the client-side. In general, there are two ways to deliver the firmware from the server to the client: PUSH and PULL methods. The differences between these two methods are in the initiator of the project firmware upgrade process. In the PUSH method, the device manufacturer starts the firmware update process by distributing the firmware binary file. In the PULL method, on the other hand, it is the IoT device that starts the firmware update process by sending a binary request to download the firmware to the server.

In Ref. [11], a blockchain-based firmware check and firmware update was proposed for IoT device systems. In the Lee and Lee scheme, the blockchain technology is used in your firmware proposal to verify the firmware version and the firmware authenticity file, as well as to distribute the firmware binary to the nodes connected to the network. Each IoT device is a network node, so each node must store all or part of the chain in its local storage, which means that only a few IoT devices are able to adopt this solution. So, the Lee and Lee proposition is not suitable for a heterogeneous IoT ecosystem.

In Ref. [12] the application of blockchain technology was proposed to update the firmware of IoT devices from different vendors. In this solution, each IoT device must periodically probe any random node in the network to check the firmware version. When a device vendor publishes a new version of the firmware upgrade to the block network, the newly created firmware upgrade needs to be verified first by the network through a consensus protocol. When one of the IoT devices of the associated device vendor wants to perform the firmware upgrade process, the device must create a transaction for the firmware upgrade request. In this scheme, IoT devices would not be able to download the firmware from their corresponding vendor unless all nodes in the network have verified the associated firmware. In this solution, all network nodes must store all firmware that has been published on the network.

3.3 Distributed file system (DFS)

When we find use cases such as the previous ones that require a distributed storage it is necessary to resolve where to store the files and who can access them. Blockchain technology does not offer storage solutions and it is not a recommended

practice to store files in the blockchain. A possible solution is the use of distributed storage systems, like the decentralized P2P file storage systems. When using this kind of storage, files are divided into pieces that are replicated in different peers. A peer requiring access to an archive collects pieces of this archive, which is partially located in several peers at a time. The performance is similar to that of the P2P BitTorrent network and files are indexed by their hash or fingerprint.

As the main solution for implementing this kind of storage is to use IPFS [13]. IPFS is a decentralized hypermedia P2P protocol that allows the storage of distributed files dividing the files in chunks and replicating them in the peers that require them. When a file is downloaded, chunks are collected from different sources at the same time. Each file is identified and accessed through its hash or fingerprint. IPFS is the basis of Filecoin, a distributed storage network based on Blockchain. This network basically integrates IPFS in a specific Blockchain network for data storage in which the nodes get tokens as payment for the storage service provided (and the customers pay them). As for privacy and access control, the IPFS protocol does not include any encryption mechanism or access control. It is up to the client or DApp to encrypt each file prior to sharing the archive to prevent its disclosure to third parties, which is not a very versatile and interoperable solution either.

In short, IPFS provides distributed and decentralized storage of large files with a certain degree of resilience, integrity, and very high availability. By storing in the Blockchain the hash of the files, which occupies only a few bytes, both systems are linked and the integrity of the file is guaranteed.

4. Blockchain and content delivery networks (CDN)

Another interesting use case, maybe not so known as the previous one, is the application of blockchain strategies to content delivery networks. These networks are widely used nowadays, so we have considered that they are a good example of how we can use blockchain to add value to existent processes or technologies.

4.1 Introducing the content delivery networks

A Content Delivery Network (CDN) consists of an overlapped network of computers containing different copies of the same set of data. The objective of its creation is to maximize the bandwidth available in a service to improve, as far as possible, the availability and access to data.

A client accesses one of the copies of the data. By providing information replicas and bringing closer the node that provides the service, the response time should be improved, and service outages avoided. But, how does that affect the information a customer can see? The Byzantine Generals Problem enunciated by [14] establishes that the components of a distributed computing system may fail, reaching a condition of imperfect information. In this situation, an observer could have different information depending on unnoticed facts, like the server consulted or the client's location. A different observer could have different information for the same service consulted if an inconsistent CDN state is making the network to fail in its responses. A consensus regarding which component has failed in the first place and which information is trustworthy would make things easier.

Prior to the emergence of Blockchain and the definition of the Distributed Ledger Technologies, it was already possible to find collaborative networks that allowed greater resistance to targeted attacks [15], such as DDoS. But it was difficult to incentivize a participant to offer their computing power to these networks. This lack of ability to attract new collaborators made the network growth very difficult

and undermined the power of defense systems. Blockchain, as a new concept of distributed system, allows to give a reward to the participants who take part in the improvement of a security system.

In addition to its application in cybersecurity, it is also possible to find deployments of CDNs with other purposes such as databases and DNS services, either in private or in a collaborative way. But they can also offer other different services such as the exchange of multimedia files or the distribution of software.

As stated by [16], the distribution of services is thought of as a solution to the problem presented by a centralized service. The distributed nature of blockchain allows these services to be decentralized. The characteristics obtained are common to both approaches, of which the most important and their counterpart are listed below.

- The load on each individual server is lowered, but the number of servers of the system is increased.

- The network traffic is distributed, but the information needs to be synchronized.

- The latency is diminished, and the bandwidth increased, in exchange for a higher maintenance cost.

In short, the use of CDNs adds some advantages, but it also increases the complexity of the architecture. There are several aspects that are affected by the need for offering copy mirrors and closer access to the client. The original server must have substitutes to ensure the high availability of the service. On the other hand, it is necessary to ensure the consistency of the data served. As there are a number of geographically distributed machines, which theoretically have the same information at all times, synchronization problems may arise.

Additionally, there must be a constant internal routing service to find all nodes in the network, to synchronize information internally and to provide better customer service externally. Furthermore, all these mechanisms are based on a record of user accesses and server use that improves the quality of service but generates an additional cost in computing and storage.

4.2 Use cases

Usually, actors such as data centers, mobile operators, digital advertising companies or online music providers, act as clients for companies like ISPs, media or news agencies, which distribute their content using this type of system.

One well known and widely used example for distributed data management is the peer-to-peer exchange of *torrent* files. The BitTorrent protocol defined by [17] uses computer networks that simultaneously and in a decentralized manner upload and download content over the network. But these exchanges are made without order or agreement on what content is propagated. What if we established a mechanism for the verification and validation of the exchanges? What if in addition to data we could transfer value? What if each of these participants could execute a business logic accepted by all?

Cybersecurity is a fundamental aspect of the industry at a global level. In modern times much media attention is being given to attacks that appear and cause serious damage all over the world. It is curious that so many systems are affected by security breaches, because as [18] indicates the attack vectors have not changed in the last 20 years.

Although there are mechanisms for distributing content prior to Blockchain, all the defense systems offered by security companies are, to a greater or lesser extent, centralized. In contrast, attacks are distributed. This fact already places the defenders in an initial disadvantageous situation.

A Blockchain-based defense would behave like Uber or like carsharing: in these two examples, the goal is to take advantage of resources that are normally underused for most of the vehicle's useful life, whereas when it comes to blockchain, the goal is to be able to use the computation of a data center that is not being used at a specific time. Resources could be rented from other network members and used to manage a powerful coordinated defense system. All of this without affecting the other computer owners when they need to use their resources.

Notice that a Blockchain solution is intended to record changes of ownership, different states of information, etc. that happen between two or more parties. Both the origin and the destination are known, although in many implementations of Blockchain it is only pseudonymous. And the execution of each one of these changes is deterministic, meaning that it will end with the same result regardless of who executes it within the network.

Coming back to the BitTorrent example, the question is if it is possible to be sure that the content offered by another user will always be available and whether any user should offer me the same content. The answer is no. And this is what will be changed by using Blockchain.

4.3 The great leap

Blockchain has revolutionized the Fintech world as we know it today. Revolutionizing content distribution could be its next goal. The big bet is the decentralization of services and the suppression of a single trust entity, relying on the system operation on distributed services.

To leverage the Blockchain capabilities and create a CDN that is truly disruptive, a method has been sought to obtain good latencies, and also to allow p2p files to be exchanged securely, without requiring an external auditor.

Using Blockchain can improve fundamental aspects of computational efficiency. Businesses adopting Blockchain could save on infrastructure and gain greater flexibility in the services they offer. In addition, related aspects such as scalability, security, reliability and performance could be improved. But as explained above, Blockchain also requires a physical network, software, and security procedures to allow it to operate properly.

The method that will achieve the best result is the simplest in its conception. It consists of taking successful projects and arranging them in such a way that they work in an ideal flow. In other words, it is the creation of nodes that participate collaboratively in a large resilient network of file exchanges as in BitTorrent, using hash tables as explained in [19] about Kadmelia, and versioning the contents like Git. Everything self-certified by the network itself.

Storj, the before-mentioned IPFS, DECENT or BlockCDN are some of the initiatives that are based on the distribution of contents that Blockchain offers to create new horizons in the CDN ecosystem. These solutions take advantage of storage times, downloads or bandwidth to boost their businesses. This means that the creators of these systems, with very different market viewpoints, are able to encourage users to adopt the network that each one promotes. These networks are focused on the needs of the user and reward participants for maintaining the network, without the need for a trusted third party to intervene to control all of them.

This is how the concept of "distribution" is being reinvented in the Content Distribution Networks. Content transparency and user privacy begin a new path together.

5. Blockchain for threat intelligence

Another interesting use case for blockchain is threat intelligence. As written in [20], threat intelligence is an advanced process which involves gathering valuable insights including mechanisms, context, indicators, actionable advice and implications about an emerging or existing cyberthreat. Threat intelligence processes must be adapted to a company ecosystem to integrate it properly.

One of the issues related to threat intelligent these days is that companies usually spend a lot of time researching the same threats, while others are unnoticed. As a consequence, new tendencies emerge, being now crucial to be able to share information between different interested parties. Following this principle, different companies are able to share information about threats to benefit each other. In the end, a distributed ledger of shared information is the ultimate goal of the threat intelligence philosophy.

Decentralization in the threat management ecosystem is not new at all. Previous works, as [21], study decentralization strategies applied to threat intelligence use cases. Others, like [22], propose a shared infrastructure to implement a threat intelligence solution. With decentralization, a single view of data and information shared concepts, blockchain comes into mind. Synchronization between different parties is also a crucial requirement, which is naturally made by blockchain due to its peer-to-peer-oriented architecture, as stated before.

When discussing the application of blockchain for threat intelligence use cases, Smart Contracts are a good asset too. For clarification, a Smart Contract is a computer program shared between nodes in a network that can be executed by all of them with a deterministic output. This piece of code allows us to verify, enforce or perform specific actions that can be audited so everyone knows the logical flow of the system. In other words, everyone is aware of the system functioning and is enforced to comply with it. Furthermore, the consensus is presented as a mechanism to guarantee synchronization between all the nodes. The aforementioned Smart Contracts enable high-level computations far from traditional distributed architectures focused on only-sharing information. In addition, we can ever think more philosophically and say blockchain is a more futuristic solution due to the fact that it allows us to create networks controlled by no-one, but verifiable by everyone.

As an example, specifically focusing on healthy ecosystems, a European initiative is trying to implement a blockchain-based Threat Management platform, which is the SPHINX Project [23]. In this project, health IoT devices within different medical centers share information about different threats ideally affecting the same ecosystem. Different components, within the scope of the same project, read from the same registry, so all of them have a single view of the data. This is one step forward in decentralization and information sharing solving a very specific problem applied to a very specific scenario. Focusing on the blockchain infrastructure, it acts as a BaaS (Blockchain as a Service), whose nodes are in different medical centers and the different IoT devices act as the users of this shared platform. This is a very clear example of how we can use Blockchain to solve a threat management problem in a wise way.

On the other hand, when it comes to other general cybersecurity solutions, blockchain can add some additional value to the traditional systems. For example, a very interesting use case is the distributed intrusion detection systems. However, these distributed intrusion detection systems are far from being fully secure as shown in [24], where the authors study the vulnerabilities that affect these systems. Blockchain can work as a distributed intrusion detection system, as shown in [25], avoiding the need to trust in third parties. It can also be very useful to detect some zero-days attacks in industrial environments by doing what

we have named "log comparison", which basically consists of comparing different logs from different devices against the ones stored in a Blockchain infrastructure. When an attacker breaks into a system, one of the first things he usually does is to delete every proof of his presence, so he usually tries to delete every log which can link him with a particular incident. By having a trusted anti-tampering infrastructure, we can detect almost in real-time if a system has been compromised or not just comparing the logs in the system with the ones stored in the Blockchain, which are immutable "by design". It is important to mention that Blockchain grows very fast in disk, but storing just simple information, like log hashes, for example, we can easily overcome this issue.

No just focusing on pure threat intelligent, rather than monitoring activities, there are some studies which apply blockchain to enhance logging systems. One of the first examples is [26], written by some members of the University of La Sapienza in Rome and the University of Southampton, tries to find a solution to the European project Sunfish based on a distributed database which provides integrity and stability to the data, analyses the advantages and disadvantages of using this tool by implementing cloud computing. Nokia Bell Labs published a small report [27] in which it proposes to make use of private and permissioned blockchains instead of public ones to manage the logs, in this case, it focused on information related to banks. As mentioned in the paragraph before, storing logs can be problematic. As a consequence, working with hashes is wiser, because it is always possible to get the integrity of the data without affecting blockchain the disk usage excessively.

To sum up, blockchain comes up when sharing information between different parties is a matter. Whether if we want to identify the issuers of this information or if we want to anonymize them, different blockchain technologies can help us to achieve these requirements.

6. Conclusions

As we have read, blockchain is much more than just cryptocurrencies. It is possible to build a vast number of use cases by using blockchain as a trusted infrastructure due to its security properties. In this document, we have shown several of these use cases, all of them security-related may be unknown for the reader and different from the now-trendy cryptocurrencies trading.

As far as we dig into the blockchain technology, we become more aware of its possibilities, ranging a huge spectrum of functionalities and covering various use cases in different fields, such as industry, health, finances... although this document has enlightened only the ones concerning the security field.

However, the future is continuously changing, and blockchain technologies are not the panacea for every problem in the world. The emergence of the so-called blockless technologies is a challenge for the blockchain technology itself, because they present a different way to achieve almost the same security requirements of the blockchain technologies, but trying to overcome its issues, such as latency and fees. The subsequent years will decide which ones of these technologies take advantage of the rest of them, but the decision does not seem to be easy.

Acknowledgements

This work was performed with the financial support of the ELKARTEK 2018 (CyberPrest project, KK-2018/00076) research program from the Basque

Government. At the same time, this content is the product of a joint effort of a group of people belonging to the Tecnalia Blockchain and Cybersecurity Research Group and it is the result of our experiences in researching, developing and applying blockchain to different sectors. We want to thank the community of hard-working developers involved in foundations and technologies like Hyperledger or Ethereum, among others, allowing us to collaboratively improve and develop new blockchain-based solutions to reach a better world.

Author details

Oscar Lage*, Santiago de Diego, Borja Urkizu, Eneko Gómez and Iván Gutiérrez
TECNALIA, Parque Científico y Tecnológico de Bizkaia, Derio, Spain

*Address all correspondence to: oscar.lage@tecnalia.com

References

[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available from: http://bitcoin.org/bitcoin.pdf

[2] Innerbichler J, Damjanovic-Behrendt V. Federated Byzantine Agreement to Ensure Trustworthiness of Digital Manufacturing Platforms. 2018. pp. 111-116. DOI: 10.1145/3211933.3211953

[3] Fan X, Chai Q. Roll-DPoS: A Randomized Delegated Proof of Stake Scheme for Scalable Blockchain-Based Internet of Things Systems. 2018. pp. 482-484. DOI: 10.1145/3286978.3287023

[4] NRI. Survey on blockchain technologies and related services [Tech. Rep.]. 2015. Available from: http://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf

[5] Zheng Z, Xie S, Dai H, Chen X, Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017. DOI: 10.1109/BigDataCongress.2017.85

[6] "Webcam Maker Takes FTC's Heat for Internet-of-Things Security Failure" [Internet]. 2013. Available from: https://www.technewsworld.com/story/78891.html

[7] Hilton S. "Dyn Analysis Summary Of Friday October 21 Attack." 2016. In: Oracle Dyn Company News. Oct 26. Available from: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[8] Chacos B. Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline. 2016. In: PCWorld [Accessed: 22 October 2016]

[9] Bonderud D. Eight Crazy Hacks: The Worst and Weirdest Data Breaches of 2015 [Internet]. 2015. IBM SecurityIntelligence December 9, 2015. Available from: https://securityintelligence.com/eight-crazy-hacks-the-worst-and-weirdest-data-breaches-of-2015/ [Accessed: 05 March 2019]

[10] "Stonefly: First Blockchain Technology Backup" [Commercial tool]. Available from: https://stonefly.com/blockchain-backup

[11] Lee B, Lee JH. Blockchain-based secure firmware update for embedded devices in an internet of things environment. The Journal of Supercomputing. 2017;**73**(3):1152-1167

[12] Boudguiga A, Bouzerna N, Granboulan L, Olivereau A, Quesnel F, Roger A, et al. Towards better availability and accountability for iot updates by means of a blockchain. In: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 50-58). IEEE; 2017

[13] Benet J. "Ipfs-content addressed, versioned, p2p file system". 2014. arXiv preprint arXiv:1407.3561

[14] Lamport L, Shostak R, Pease M. The byzantine generals problem. ACM Transactions on Programming Languages and Systems. 1982;**4**(3): 382-401. DOI: 10.1145/357172.357176. Archived from the original on 13 June 2018

[15] Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems. 2002;**20**(4):398-461

[16] Domenico T, Trunfio P. Toward a synergy between p2p and grids. IEEE Internet Computing. 2003;**7**(4):96-95

[17] Cohenv B. Incentives build robustness in BitTorrent. In: Workshop

on Economics of Peer-to-Peer Systems. Vol. 6. 2003

[18] Shinde PS, Ardhapurkar SB. Cyber security analysis using vulnerability assessment and penetration testing. In: 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave). IEEE; 2016

[19] Maymounkov P, Mazieres D. Kademlia: A peer-to-peer information system based on the xor metric. In: International Workshop on Peer-to-Peer Systems. Berlin, Heidelberg: Springer; 2002

[20] Shahare R. "Blockchain, for Threat Intelligence Maybe?" [Internet]. 2019. Available from: https://www.cpomagazine.com/cyber-security/blockchain-for-threat-intelligence-maybe/

[21] Burger EW, Goodman MD, Kampanakis P, Zhu KA. Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. 2014. pp. 51-60. DOI: 10.1145/2663876.2663883

[22] Wagner C, Dulaunoy A, Wagener G, Iklody A. MISP -the Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. 2016. DOI: 10.1145/2994539.2994542

[23] "SPHINX - A Universal Cyber Security Toolkit for Health-Care Industry". 2018. Available from: https://cordis.europa.eu/project/rcn/220226/factsheet/en [Accessed: January 2019]

[24] Li W, Meng Y, Kwok LF, Ip HHS. PMFA: Toward passive message fingerprint attacks on challenge-based collaborative intrusion detection networks. 2016;**9955**:433-449. DOI: 10.1007/978-3-319-46298-1_28

[25] Meng W, Tischhauser EW, Wang Q, Wang Y, Han J. When intrusion detection meets blockchain technology: A review. In: IEEE Access. Vol. 6. 2018. pp. 10179-10188. DOI: 10.1109/ACCESS.2018.2799854

[26] Gaetani E, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V. "Blockchain-based database to ensure data integrity in cloud computing environments". 2017. Available from: eprints.soton.ac.uk

[27] Shekhtman LM, Waisbard E. Securing log files through blockchain technology. In: Proceedings of the 11th ACM International Systems and Storage Conference (SYSTOR '18). New York, NY, USA: ACM; 2018. pp. 131-131