BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Semiconductor Science and Information Devices
https://ojs.bilpublishing.com/index.php/ssid

ARTICLE

The Role of Blockchain in Cyber Security

Dylan Rafferty Kevin Curran*

School of Computing, Engineering & Intelligent Systems, Ulster University, UK

ARTICLE INFO

Article history
Received: 26 April 2021
Accepted: 19 May 2021
Published Online: 21 May 2021

Keywords:
Blockchain
Cybersecurity
Distributed ledgers
Bitcoin
Cryptocurrencies

ABSTRACT

Cyber security breaches are on the rise globally. Due to the introduction of legislation like the EU's General Data Protection Regulation (GDPR), companies are now subject to further financial penalties if they fail to meet requirements in protecting user information. In 2018, 75% of CEOs and board members considered cyber security and technology acquisitions among their top priorities, and blockchain based solutions were among the most considered options. Blockchain is a decentralised structure that offers multiple security benefits over traditional, centralised network architectures. These two approaches are compared in this chapter in areas such as data storage, the Internet of Things (IoT) and Domain Name System (DNS) in order to determine blockchain's potential in the future of cyber security.

1. Introduction

Blockchain as a technology entered the public consciousness in 2008, with the release of the whitepaper "Bitcoin: A Peer to Peer Electronic Cash System". The paper outlined an approach to online payments which was purely peer-to-peer, without the involvement of a financial institution [1]. This approach would be powered by blockchain, which over the last decade has developed into a ground-breaking technology with the potential to impact industries outside of finance such as manufacturing, education and cyber security. To define what blockchain is, the example of a ledger can be used. Fundamentally, a blockchain is a collection of transaction records, each between a set of two parties (see Figure 1). However, the key attribute in this case is that information is distributed – not copied – among a combination of computers linked to each other. There is no central server or authority that determines the correct version of events to the rest of the network [2].

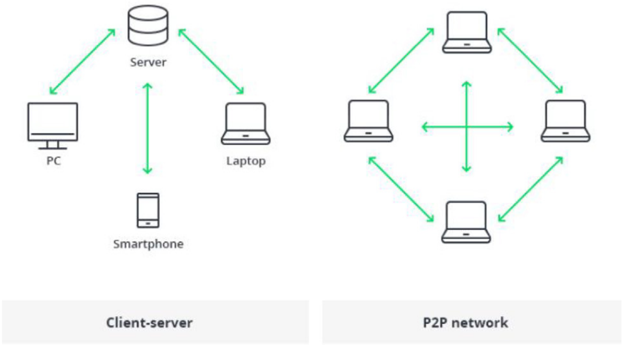


Figure 1. Database vs Blockchain Architecture [2]

Traditional architecture on the world wide web uses

*Corresponding Author:
Kevin Curran,
School of Computing, Engineering & Intelligent Systems, Ulster University, UK;
Email: kj.curran@ulster.ac.uk*

DOI: https://doi.org/10.30564/ssid.v3i1.3153

the client-server model, in which a central server contains all relevant information. This is intended to ease the process of updating it and communicating changes to all connected computers. By comparison, blockchain is decentralised – each computer on the network is responsible for ensuring that the collection of records is correct and in order. To alter data, the whole network must agree that the alteration is valid. With the use of a consensus protocol (common ruleset for verifying new additions) and financial incentive (reward for users who accurately verify additions), data stored in a blockchain are trustworthy and much less vulnerable to manipulation[2]. There are multiple key components in blockchain to consider. These will be defined in order to provide context to its potential applications in cyber security [2]

•**Node:** A single computer in the peer-to-peer network. Each node contains a copy of the entire blockchain ledger.

•**Transaction:** The smallest part of any blockchain. Contains a record of information.

•**Block:** A data structure containing multiple transactions. Blocks are distributed to all nodes in the network.

•**Chain:** A specific sequence of blocks.

•**Miners:** A sub-section of nodes which verify blocks before adding them to the wider blockchain structure (verification can be rewarded financially). Once added, a miner node will broadcast the updated blockchain to the rest of the network.

•**Consensus (Consensus Protocol):** A ruleset which must be followed to enact blockchain operations.

Figure 2 lays out how these components interact with each other in order to process a transaction.

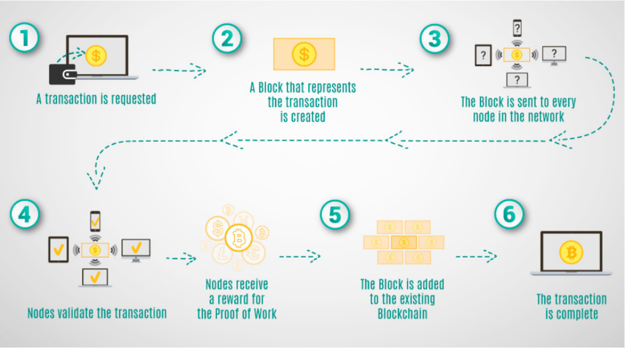

1
A transaction is requested
2
A Block that represents the transaction is created
3
The Block is sent to every node in the network
4
Nodes validate the transaction
Nodes receive a reward for the Proof of Work
5
The Block is added to the existing Blockchain
6
The transaction is complete

Figure 2. Transactions in a blockchain

To observe the security benefits of blockchain, one can analyse blocks. Each block contains specific data, a hash for itself and a hash for the previous block. These hashes are generated via cryptographic algorithm and are in-part derived from the first block in a chain. If a single block is changed illegitimately, then the following blocks are recognised as containing incorrect information, rendering the whole chain invalid [2]. A possible countermeasure would be to simply change all blocks so that each hash reference in the chain is valid. However, in the creation of any new block, proof-of-work (PoW) must be done by a miner node in order to validate the block. For a single block in a Bitcoin network, this process requires 10 minutes on average. On top of this, each node in the network receives a full copy of the blockchain and any new nodes created in it. Each of these nodes checks the new block to verify if it is correct, and only after this process will the block be added to every node's local blockchain. Finally, all nodes jointly create a consensus protocol between them, so they all follow the same rules in determining the validity of the blockchain.

In summary, the information within a blockchain network is extremely secure and logistically difficult to tamper with. To do so would require not just tampering with target blocks, but all blocks surrounding them, as well as re-calculating proof-of-work for these. Such an attack would also require control of more than 50% of nodes in order to secure consensus [2]. The strength of blockchain comes from its decentralised nature and intensive verification process. It is a secure means of containing data and therefore has potential in the realm of cyber security. Most cases analysed here will be future-facing, as blockchain's role in security is still in the formative stages. The following sections will analyse its potential use in different scenarios, the merit of these approaches compared to traditional methods, and whether any drawbacks are significant enough to warrant hesitation in technology companies.

2. Possible Applications to Cyber Security

2.1 NASA and Addressing Industry-Specific Needs

An example of a major entity actively considering blockchain in security practices is NASA. NASA released a report identifying risks present in the adoption of Automatic Dependent Surveillance-Broadcast (ADS-B) by the U.S. Federal Aviation Agency (FAA). These risks include spoofing, denial of service attacks and more [3]. An interesting observation in NASA's proposal is the idea that the most popular forms of blockchain networks (e.g. Ethereum) are designed for monetary applications, and so are not ideal for other use-cases. While non-monetary functions may be achieved, the implementations often lack flexibility and consistency due to platform limitations. Considering this, they pursued a more compatible blockchain foundation developed by the Linux Foundation known as "Hyperledger Fabric [3]. Features that motivated its use in addressing air traffic surveillance vulnerabilities include

DOI: https://doi.org/10.30564/ssid.v3i1.3153

permissioned membership, private channels, smart contracts (Detailed later) and open-source code that may be modified to further meet air traffic surveillance needs [3].

Smart contracts are noted as one of the pillars of this solution. In principle, smart contracts operate on an "If-then" premise that Smart contract code is uploaded to the blockchain and contract terms and code can be viewed publicly on the network. In addition, when terms in the contract are met, the associated code executes. For example, releasing a digital key to user X if user X sends 5 BTC (Bitcoin) to user Y [4]. Part of NASA's solution involves creating subnets (channels) and associated private ledgers, enabled by the unique architecture of Hyperledger Fabric. This allows for confidential transactions between approved members of the network. For a client to join a restricted channel, they send a request which is routed to it. A smart contract is then triggered which reviews the client's eligibility, the result of which is then verified and updated in the channel's ledger [3]. A notable outcome of this approach is that communications can be limited between approved members of the network. For instance, aircraft status (latitude, longitude, speed etc.) may be kept in a private channel, while less sensitive information (flight ID, origin, destination etc) can be published to all approved peers in the network [3]. An additional benefit is that authentication is automated via the use of smart contracts. Overall, a useful lesson to take from this proposal is that the most popular forms of Blockchain network are not necessarily the best for every use-case. Where frameworks like Ethereum are effective in the area of financial technology ("Fintech"), commercial enterprise problems are better solved with more flexible frameworks such as Hyperledger Fabric. The open source nature of Hyperledger Fabric also allows for further tailoring, allowing NASA to utilise the unique security benefits of Blockchain while not being restricted according to its traditional use in finance.

2.2 Data Storage

Many companies operate with a centralised storage system for saving customer and business data. This is a long-running logistical weakness, as evidenced by major scandals such as the Equifax security breach in which the data of millions of customers were compromised. Aside from the clear implications for public relations, the company was left vulnerable to lawsuits and therefore direct financial damage [5]. A step toward addressing risk is to de-centralise data storage so that an attack on one system does not compromise every single data record. To this end, blockchain-based storage solutions have been developed and are increasing in popularity [5].

According to Xiaoyang He, founder of Lambda (decentralised storage network): "*Blockchain has the technological underpinnings to ensure better data security… Breaking into an individual block to steal some recorded information is virtually impossible at this point. Altering or in any other way hampering with a string of data entered to a blockchain-ledger is even less likely.*" [6]. Xiaoyang argues two points of strength – The low likelihood of data breaches, and an even lower likelihood of data modification. Before analysing these, an architecture overview is required. Figure 1 compares traditional storage methods with that of blockchain:

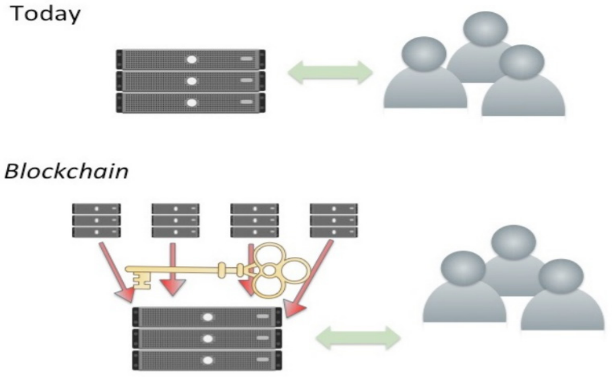


Figure 3. Comparing traditional and blockchain database structures [7]

As Figure 3 makes apparent, the traditional method of data storage is centralised. If the main server is attacked, the entire data set can be compromised – In this sense, there is a single point of failure (SPOF) in the system which can lead to damaging consequences. Additionally, due to centralisation, the owner of the server has full control over the data within it. Convention in modern service markets is not to modify customer data (e.g. Sent e-mails) without the customer's consent, but this is largely a contract built upon market forces and not enforced by any specific architecture. Another example of this weakness is in the field of research, where important papers may be modified or deleted with no trace.

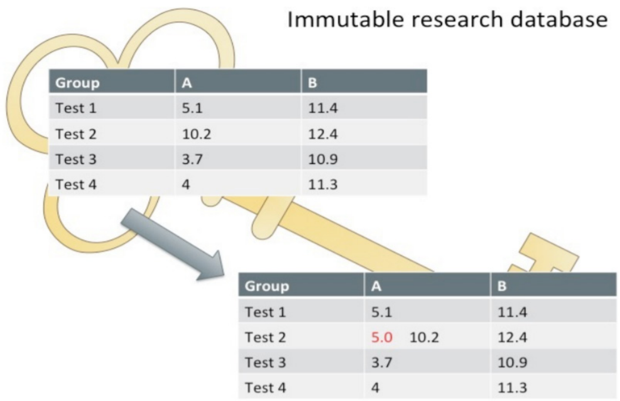
By comparison, blockchain is decentralised, distributed, transparent and immutable:

•**Decentralised:** No SPOF. A running service is not reliant upon any single computer for its continued function or integrity, so attacks on said computer are not damaging to data stored on the network.

•**Distributed:** The database exists across multiple computers. The entire database may be replicated on each machine, or it may be split across the machines.

•**Transparent:** Calculations made to produce data results are public and verifiable. Traditional hosting solutions may simply update the result (for example, in research, the impact factor of a journal), requiring trust between the publisher and users. Instead, blockchain can show how a result was generated and uploaded to the network, improving accountability of the data's "owners".

•**Immutable:** In the context of blockchain, immutability refers to the fact that data cannot be changed without leaving a trace (Figure 4). Old versions of the dataset are available for recovery and cannot be removed. This acts a deterrent against unauthorised modifications, such as ones potentially made by rogue employees in a service company [7].



Immutable research database

Group	A	B
Test 1	5.1	11.4
Test 2	10.2	12.4
Test 3	3.7	10.9
Test 4	4	11.3

Group	A	B
Test 1	5.1	11.4
Test 2	5.0 10.2	12.4
Test 3	3.7	10.9
Test 4	4	11.3

Figure 4. Immutability in a blockchain database [7]

With these attributes in mind, this report can now address Xiaoyang's two main arguments. In terms of stealing information, as noted previously there are Blockchain frameworks available which can restrict sensitive information to private networks or ledgers. Blockchain systems can also be taken off the internet or cloud and placed in a local and encrypted environment. At this stage, most routes of access for any attacker are removed. However, due to the decentralised and distributed nature of blockchain, even if a node is compromised it can be shut down and removed from the network before damage is done [8]. Assuming an attacker does however gain access to the network and reads information contained within a block, Mr He's point of data alteration being "even less likely" is valid. As noted in the Introduction section of this report, unauthorised data modification requires time, processing power and hardware. A single block being changed requires the blocks around it to be changed too, including all associated processing and validation for PoW. Additionally, for the changes to be verified and implemented by the whole network, the attacker must control of more than 50% of its nodes. Considering these points, the logistical challenge in modifying data without a trace would be immense, especially when attacking large-scale enterprise systems.

Further to his second argument, deterrents against the attackers themselves must be considered. One such example is their anonymity and the fact that its compromise can lead to prosecution (for example, under the UK's Computer Misuse Act 1990) [9]. The immutability aspect of blockchain contributes to this deterrent, allowing for any data modifications to be identified. Further, blockchain security also allows organisations to make data records traceable, exposing the identity of whoever modifies them [8].

The advantages of blockchain as a storage solution have been established. However, there are two reasons why organisations may hesitate at its implementation.

1)In January 2019, a major blockchain security breach occurred on the Ethereum platform. An attacker gained control of half of the network, and utilising its processing power, was able to rewrite transaction history. As a result, cryptocurrency (typically immune to forgery) was duplicated and sent to the attacker. While attacks on this scale are likely to be expensive (due to the processing power required), they are possible given adequate financial reward [10]. In this sense, blockchain networks are not immune to breaches, but they are logistically more difficult to execute when compared to attacks on centralised systems.

2)Due to the nature of adding blocks of data to a blockchain and syncing the updated ledger across the network, the rate of data addition can be slow and may not meet the requirements of larger organisations that require rapid input. However, solutions are emerging to this problem (for example, Microsoft's Confidential Consortium Framework (CoCo) which can throughput thousands of blocks per second as opposed to Bitcoin's rate of ten) [11].

Overall, blockchain addresses many problems raised by conventional forms of data storage, such as SPOF, lack of data transparency, unauthorised data modification with no trace and relative cost-effectiveness of attacks. In these ways, data stored on a blockchain network are more secure. Additionally, decentralised solutions are gaining in popularity and market competition is likely to present more options in this area as time progresses [12]. Whilst attackers are beginning to make an occasional breach in to blockchain systems [10], these are rare and expensive to execute. As more organisations consider blockchain a critical priority and begin to invest in it [13], it is likely that additional frameworks with further security measures will be introduced, just as they have been developed for centralised storage solutions over time. In the same vein, while blockchain networks suffer from slower data throughput on average, this is a problem that is being addressed over time by major companies like Microsoft[11]. This report argues that the fundamental merits of blockchain in storage security are strong, and it is likely to be

DOI: https://doi.org/10.30564/ssid.v3i1.3153

utilised by organisations that wish to protect their data into the next decade.

2.3 Internet of Things

The internet of things (IoT) is a term to describe how non-living objects (e.g. Webcams, thermostats, doorbells…) are connected to the internet, and interact with their respective networks to automate processes for humans [14]. The advent of home utilities having internet connectivity potentially creates much value for consumers. Despite this, industry growth and user adoption have been slow. A major reason for this is widespread concern over security, exacerbated by headline news stories such as baby monitor feeds being accessed by hackers. Currently, the IoT ecosystem is mainly reliant on cloud servers [15]. Figure 5 showcases the infrastructure of this model:

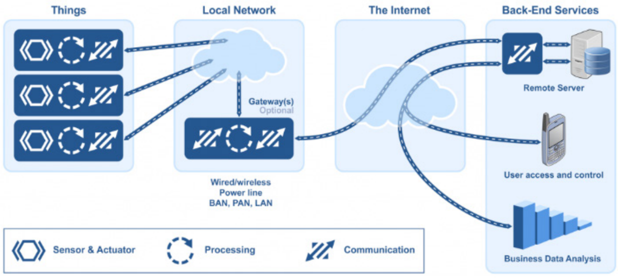


Figure 5. Traditional IoT centralised-cloud model [16]

As illustrated in Figure 5, things (devices) connect to a local network. In many commercial cases, a connection from the device then continues through a gateway to the internet, and eventually to a centralised cloud service which allows the user to access and control their device. The service owner will also be able to monitor its usage at this stage, collecting analytics to inform organisational decisions.

There are two major security challenges associated with this model:

1)**Single Point of Failure (SPOF)**

Multiple devices are connected to the central cloud service at any one time. These devices are likely to range in age and quality of built-in security. If a single device is insecure, it can be targeted as a “gateway” toward attacking the entire network. Possible ramifications include denial of service attacks, data theft and remote hijacking of other devices. In this sense, each device is a potential bottleneck to the security and integrity of the wider network.

2)**Manipulation of Collected Data**

Organisations can monitor and aggregate information delivered from devices in order to inform decision-making. They may also do this in order to inform other entities, such as regulatory bodies, about their operations. However, apart from external attacks, there are cases where data may be tampered with by the organisations themselves in order to avoid higher costs (related to regulation or prosecution). In these cases, assuming the central cloud service is under their control, they can unilaterally modify collected records without alerting other stakeholders. This is a security issue that can negatively impact parties reliant on said organisation (for example, customers relying on safety statistics collected by a water company) [15].

In order to address SPOF, the commercial supply chain involved in creating IoT devices can be considered. The supply chain could adopt blockchain, and due to the network’s public availability, devices could be traced back to their raw materials in order to determine which of them is vulnerable to a security breach. At this point, affected devices could be identified for recall and cut off from the network. Additionally, to protect against man-in-the-middle or replay attacks made against a device, blockchain signs each transaction using cryptography and verifies each signature. This would ensure that any message is actually the one sent by the originating device[15]. For Manipulation of Collected Data, external attackers face a major logistical challenge in changing information saved on the network. If one node’s blockchain updates are hacked, they are rejected by the wider network. If an organisation intends to maliciously change the data it is supposed to be honestly recording, this cannot be achieved with a single actor. Instead, the entire network must agree on the changes implemented. Due to immutability, there is likely to be a trace of any such change. It is also important to note that a blockchain storage network fed by IoT sensors can be an automated system, which along with the base strengths of blockchain in verification and shared governance protocols, further limits the possibility of human actors interfering in the accurate storage of data[17].

Overall, the themes in IoT security align closely with those in storage security, mainly due to the use of centralised structures and the vulnerabilities caused by them. Blockchain’s decentralised and autonomous capabilities can help address these. Additionally, as the IoT grows larger, the consensus-driven aspect of blockchain security will increase in strength due to a single attacker having less relative influence. This is a desirable outcome compared to traditional architecture, where running costs increase instead [15].

Blockchain’s ability to verify transactions with cryptography helps protect against attacks on devices, and its possible application in the supply chains which produce these devices can further guarantee a secure Internet of Things and improve public confidence in the market [15].

DOI: https://doi.org/10.30564/ssid.v3i1.3153

Regarding implementation today however, there are multiple challenges:

1)IoT devices are typically resource limited. Yet, mining (establishing PoW) is resource intensive.

2)Mining is time consuming, yet low latency is desired in most IoT applications.

3)Blockchain protocols can create additional overhead traffic, which may be incompatible with bandwidth-limited devices.

4)Blockchain network performance scales poorly with the number of nodes, and IoT networks are expected to have many nodes [18].

In the short term, these challenges are likely to still exist and impede the adoption of blockchain in the IoT. However, alternative light-weight frameworks that eliminate overhead while maintaining security benefits are actively being researched [18] and could be available for use by IoT companies soon. If this comes to pass, and these hurdles can be overcome, the IoT market can begin experiencing exponential growth as consumer security concerns are addressed by the new infrastructure.

2.4 Domain Name System

Domain Name System (DNS) is a way for users to connect to a network service such as the web. The left side of Figure 6 (from "End User") articulates the traditional architecture and process involved.

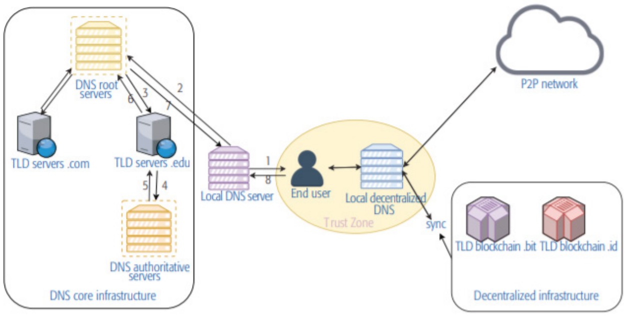


Figure 6. Centralised (Left) and decentralised (Right) DNS Structures (Karaarslan and Adiguzel, 2018)

The key attribute of this setup is that it is centralised, like many other non-blockchain methods. The user determines an IP address from a domain name by interacting with the local DNS server. If the local server already knows the address (e.g. It is cached) then it responds directly to the user. Otherwise, the root servers and top-level domain (TLD) servers will be queried for a specific authoritative server based on the given domain name. At this point the local DNS server requests the corresponding IP address and delivers it to the user [19].

There are four notable vulnerabilities in the existing centralised solution for DNS:

1)**Distributed Denial of Service (DDoS) attacks**

This kind of attack occurs when a server (such as DNS) is flooded with internet traffic in order to disable it. This can result in a loss of service for users. Mitigating this risk in the context of centralised infrastructure is difficult and expensive, requiring an increased number of servers and anti-DDoS mechanisms.

2)**Server damage caused by cyber attack / Shutdown of DNS servers by authorities or disasters**

If these events occur, legacy solutions can do relatively little to mitigate them. The user must manually change DNS in order to re-gain access to web services.

3)**Alteration of DNS records on server**

This problem can be addressed by the addition of security measures and a monitoring process to the server, but success can vary based on the admin or security professional involved.

4)**Attack on user to change DNS address mid-session**

In this attack, the user's traffic is re-routed to a server they did not intend to contact. This can lead the user to malicious sites, resulting in consequences such as data theft or viruses. The difficulty in addressing this is moderate, requiring end-to-end implementation of the DNS Security Extensions (DNSSEC) protocol in order to verify that the correct DNS address is being reached [19,20].

3. Weaknesses of Blockchain

The architecture of a blockchain-based decentralised solution is set out on the right side of Figure 6 and is largely immune to the vulnerabilities present in a traditional centralised DNS structure. The user asks the decentralised DNS server for the domain list it serves, which is stored locally (for example, bit and .id). The server connects to a peer-to-peer network of other blockchain-based DNS nodes, utilising this to sync its domain records [19].

We analyse all four vulnerabilities and why blockchain can mitigate against them:

1)**DDoS**

A blockchain DNS network would be decentralised, and as a result many nodes would need to be disrupted in order to take down the entire system and disrupt service [21]. Additionally, the larger the network, the more secure it becomes [19].

2)**DNS Server Damage or Shutdown by External Actors**

Due to DNS records being replicated across many nodes, shutting down one server will not affect service as the rest of the network will still be active.

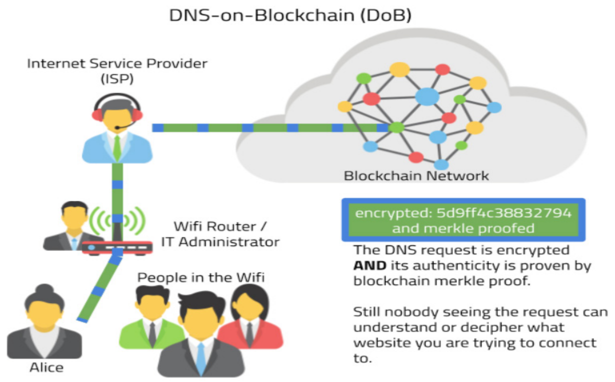
DOI: https://doi.org/10.30564/ssid.v3i1.3153

3)**Alteration of DNS records**

Such a change on one server would require the change to be applied to the whole network, therefore requiring network-wide consensus. This relates to the attribute of immutability referenced in earlier cases.

4)**DNS Address Hijack**

Blockchain removes the need to contact a central authority in order to obtain DNS data. Instead, domain owners store their domain information directly on the blockchain with a cryptographic signature, and only the respective owners can change this information. Due to cryptographic signature techniques, the user can be sure that the DNS data they receive from a corresponding block are valid. The DNS request is encrypted and so attackers cannot easily intercept it [22].


DNS-on-Blockchain (DoB)
Internet Service Provider (ISP)
Blockchain Network
encrypted: 5d9ff4c38832794 and merkle proofed
Wifi Router / IT Administrator
People in the Wifi
Alice

The DNS request is encrypted **AND** its authenticity is proven by blockchain merkle proof.

Still nobody seeing the request can understand or decipher what website you are trying to connect to.

Figure 7. Web access in a DNS-on-Blockchain structure [22]

Another security weakness DNS-on-Blockchain could improve would be in the realm of digital certificates. When visiting a website, one's browser verifies its authenticity by checking the certificate associated with it. Digital certificates are issued to websites by several certificate authorities, and if an authority is hacked, it can begin distributing false certificates which can lead users to malicious imposter websites. Instead, if website names are managed on the tamper-resistant blockchain, then the need for certificate authorities is removed because simply accessing the correct domain name is a secure process in itself and guarantees that the connection is legitimate [10]. While such vulnerabilities can be protected against, there are also disadvantages to blockchain's implementation. For instance, as the network increases in scale, security may increase [22] but response times may slow down in turn [19] which can impact user access to the web. Additionally, if an organisation believes a domain with their name is being held in bad faith, a blockchain system with no central "decision-maker" will make it difficult to resolve such legal disputes [10]. This may be a hurdle to organisations opting to participate in any decentralised DNS system, and so some "centralisation" may still be required.

There are already blockchain-based Internet of Things (IoT) frameworks that include layers of access to keep out unauthorised devices from the network. Some enable IoT devices to send data to blockchain ledgers for inclusion in shared transactions with tamper-resistant records. It also validates the transaction through secure contracts. A potential barrier to blockchain and IoT is that most IoT devices have a limited memory size and limited battery life along with restricted processors. Traditional 'heavy' cryptography is difficult to deploy on a typical sensor hence the deployment of many insecure IoT devices. As such, IoT devices are more vulnerable to the '51 percent attack' where hackers control 51 percent of the processing power in the blockchain. This also raises a more important point in that IoT devices may simply be too underpowered to be part of the blockchain. The blockchain does require participating nodes to perform relatively complex computations in a 'proof of work'. It is necessary for integrity of data. Blockchain has the potential to enable the IoT to finally provide true machine-to-machine interactions with automated price negotiations through smart contracts taking human preferences into consideration. This allows us to fulfil the final vision for a true IoT blockchain framework, which is IoT nodes verifying the validity of other IoT transactions without relying on a centralised authority, such as an IoT device monitoring soil conditions validating payments to the local water supply utility based on moisture readings. As time goes on, these application areas will increase for society and industry, allowing the industry to move blockchain far beyond the coin.

4. Conclusions and Future Developments

We identified that traditional centralised architecture carries common weaknesses across multiple sectors. This is especially noteworthy given that most industries today rely on centralised solutions. These weaknesses include SPOF, vulnerability to data tampering and vulnerability to attacks such as denial of service. Blockchain, utilising attributes such as its distributed nature, transparency and resistance to tampering offers a fundamentally different but much more secure method of delivering cyber security. Under blockchain, a single attacker has much less relative influence over a network and so must leverage a significantly larger set of resources in order to pose any kind of threat. The risk of DDoS attacks against DNS systems could be significantly reduced if domain owners collectively agreed to register themselves and their domains on a common DNS blockchain network. The Internet of Things, particularly individual devices in the home, would be secure and resistant to man-in-the-middle attacks if

DOI: https://doi.org/10.30564/ssid.v3i1.3153

blockchain was leveraged in that field. In terms of data storage, risk of untraceable tampering and data loss would be essentially removed under a blockchain method. These are just some of the problems currently experienced by services today that could be effectively mitigated by blockchain integration.

Barriers to adoption include much higher power consumption overall, slower data throughput and potential hesitation by larger organisations that would lose influence under blockchain-based networks. However, investment in blockchain by companies is increasing year-on-year, and with that comes the increased possibility of new blockchain frameworks designed to overcome such hurdles to adoption. While blockchain is not appropriate for replacing every single centralised system, and is not a "magic wand", it could bring large benefit to specific areas such as the ones outlined in this report. In this sense, blockchain is likely to cause at least some disruption to the technology industry, and in the end will at least co-exist with centralised architecture in other fields.

References

[1] Nakamato, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [online] p.1. Available at: https://bitcoin.org/bitcoin.pdf [Accessed 10 Nov. 2019].

[2] Lastovetska, A. (2019). Blockchain Architecture Basics: Components, Structure, Benefits & Creation. [online] Available at: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture [Accessed 10 Nov. 2019].

[3] Reisman, R. (2019). Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy. [online] pp. 1, 7-9. Available at: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190000022.pdf [Accessed 10 Nov. 2019].

[4] Rosic, A. (2016). Smart Contracts: The Blockchain Technology That Will Replace Lawyers. [online] Available at: https://blockgeeks.com/guides/smart-contracts/ [Accessed 10 Nov. 2019].

[5] Arnold, A. (2019). 4 Promising Use Cases of Blockchain in Cyber Security. [online] Available at: https://www.forbes.com/sites/andrewarnold/2019/01/30/4-promising-use-cases-of-blockchain-in-cybersecurity/#7b0f8b1b3ac3 [Accessed 10 Nov. 2019].

[6] Glenn, A. (2018). Equifax: Anatomy of a Security Breach. [online] p.1. Available at: https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=1429&context=honors-theses [Accessed 10 Nov. 2019].

[7] Bartling, S. and Fecher, B. (2016). Could Blockchain provide the technical fix to solve science's reproducibility crisis? [pdf] pp. 1-3. Available at: https://pdfs.semanticscholar.org/55d1/2f48e2b446bbc1501eac0d-1f60c7f04a22e5.pdf [Accessed 10 Nov. 2019].

[8] DataFloq, (2019). Is Blockchain the Answer to Healthcare Data Breaches? [online] Available at: https://datafloq.com/read/blockchain-answer-health-care-data-breaches/6104 [Accessed 10 Nov. 2019].

[9] CPS, (2019). Cybercrime - prosecution guidance. [online] Available at: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance [Accessed 10 Nov. 2019].

[10] Orcutt, M. (2019a). Once hailed as unhackable, blockchains are now getting hacked. [online] Available at: https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ [Accessed 10 Nov. 2019].

[11] O'Dowd, E. (2018). Cloud-Based Healthcare Blockchain Improves Efficacy, Control. [online] Available at: https://hitinfrastructure.com/news/cloud-based-healthcare-blockchain-improves-efficacy-control?utm_source=datafloq&utm_medium=ref&utm_campaign=datafloq [Accessed 10 Nov. 2019].

[12] Arnold, A. (2018). The Current Take On IoT Security: Are We Getting Closer To A Safe Ecosystem? [online] Available at: https://www.forbes.com/sites/andrewarnold/2018/10/15/the-current-take-on-iot-security-are-we-getting-closer-to-a-safe-ecosystem/#272a0623862e [Accessed 10 Nov. 2019].

[13] Deloitte (2019). Deloitte's 2019 Global Blockchain Survey. p.3. Available at: https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf [Accessed 10 Nov. 2019].

[14] Jindal, F., Jamar, R. and Churi, P. (2018). Future and Challenges of Internet of Things. International Journal of Computer Science & Information Technology (IJCSIT), [online] 10(2), p. 13. Available at: http://aircconline.com/ijcsit/V10N2/10218ijcsit02.pdf [Accessed 10 Nov. 2019].

[15] Kshetri, N. (2017). Can Blockchain Strengthen the Internet of Things? [online] New York: IEEE Computer Society, Pages used. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8012302 [Accessed 10 Nov. 2019].

[16] Micrium, (2019). How to Think about the Internet of Things (IoT). [online] Available at: https://www.micrium.com/iot/devices/ [Accessed 10 Nov. 2019].

[17] Cheng, S., Daub, M., Domeyer, A. and Lundqvist, M. (2017). Using blockchain to improve data management in the public sector [online] Available at:

https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector [Accessed 10 Nov. 2019].

[18] Dorri, A., Kanhere, S. and Jurdak, R. (2016). Blockchain in Internet of Things: Challenges and Solutions. [online] pp. 1-2, Available at: https://arxiv.org/ftp/arxiv/papers/1608/1608.05187.pdf [Accessed 10 Nov. 2019].

[19] Karaarslan, E. and Adiguzel, E. (2018). Blockchain Based DNS and PKI Solutions. [pdf] pp. 52-54, 57. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8515149&tag=1 [Accessed 10 Nov. 2019].

[20] ICANN. (2019). DNSSEC – What Is It and Why Is It Important? [online] Available at: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en [Accessed 10 Nov. 2019].

[21] Griffin, M. (2016). New Blockchain DNS System would put an end to DDoS attacks. [online]. Available at: https://www.311institute.com/new-blockchain-dns-system-would-put-an-end-to-ddos-attacks/ [Accessed 10 Nov. 2019].

[22] Lai, P. (2019). Why DNS on the Blockchain is the next step after DNS over HTTPS [online] Available at: https://diode.io/distributed-infrastructure/Why-DNS-on-Blockchain-is-the-next-step-after-DNS-over-HTTPS-19231/ [Accessed 10 Nov. 2019].

DOI: https://doi.org/10.30564/ssid.v3i1.3153