|  |
| --- |
| Group 12 |
| Blockchain-based PKI (BB-PKI) |
| Cybersecurity – IT Technology |
| Brandon McPherson  10-15-2021 |

Contents

[Introduction 2](#_Toc85299358)

[Public Key Infrastructure 2](#_Toc85299359)

[What is the Public Key Infrastructure? 2](#_Toc85299360)

[PKI in Use 2](#_Toc85299361)

[Issues with PKI 3](#_Toc85299362)

[Blockchain 4](#_Toc85299363)

[What is Blockchain 4](#_Toc85299364)

[What Blockchain-based PKI will fix 5](#_Toc85299365)

[My Thoughts 5](#_Toc85299366)

[References: 6](#_Toc85299367)

# Introduction

As businesses begin to adopt cloud computing, moving away from the traditional centralized computing model, the typical user base now has the ability to access enterprise systems and exchange corporate data from their personal devices without the requirements of a VPN or using corporate assigned devices. The ease of accessing these systems have also increased with the likes of mobile devices such as tablets and smart phones over a cellular network and will continue to increase as 5G is rolled out. This presents a problem as these BYOD devices won’t have a corporate assigned digital certificate which the Public Key Infrastructure requires in order to encrypt data transmissions and establish trusts between different networks. Sure, a cloud service (whether this is AWS or Azure) will have their own Certificate Authority (CA) and their own digital certificate to hand out but the end user accessing these systems will not have a digital certificate assigned by a company from whom they represent. As we move towards a decentralized computing model, a new method is needed to improve the security of these devices. First, we need to understand how the public key Infrastructure works.

# Public Key Infrastructure

## What is the Public Key Infrastructure?

The Public Key Infrastructure (PKI) has been around for years and binds multiple technologies together to create trust and secure data exchanges over the internet (Brien Posey, September 15, 2005, TechRepublic). As the Internet is a public space allowing any computer to communicate with other computer networks, much like other internet service protocols (such as DNS) PKI is what allows different networks to communicate securely and provide evidence that the data is coming from the intended source. The technology behind PKI is based on distributing digital certificates to clients and between these digital exchanges are different levels of trust authorities. Digital Certificates are signed using a hash, contents encrypted via a private key (kept by the owner or CA) and a public key to decrypt the contents of the data and other metadata.

The Certificate Authority (CA) is responsible for auditing, issuing and revoking digital certificates. Some corporations will host their own CA which a security technician will be responsible to maintain the companies’ public keys, the Certificate Revocation List (CRL) and Auditing. A Registered Authority (RA) who verifies digital certificate requests. In layman’s term, identification of data exchange on the internet is similar to how we use passports in the real world (Josh Fruhlinger, 29 May 2020 CSO Online)

## PKI in Use

To understand how PKI is used, let’s briefly look at a digital certificate and the handling of them. This is a digital certificate from the RMIT University website:

Graphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

Digital Certificate from RMIT website, Images captured using Greenshot software from my computer.

Here we can see the Issuer (CA) which is QuoVadis Global, the Validation dates, the Signature hash algorithm used (sha256), the certification path, certificate polices and other meta data under the details tab.

A picture containing timeline

Description automatically generated

Image has been taken from Wikipedia article (<https://en.wikipedia.org/wiki/Public_key_infrastructure>)

The above image Illustrates how certificates are handed out amongst the different governing bodies on the PKI. A user applies for a digital certificate with the Registered Authority (RA), The RA will confirm the user’s identity and pass over to the Certificate Authority (CA) to issue a digital certificate. The Validation Authority (VA) verifies the status on the digital certificate and updates it if necessary. Not mentioned in the graph is the Certificate Revocation Lists (CRL) which the CA manages. These are where all the revoked digital certificates are stored (Dr. Herong Yang, 2021, PKI Tutorials – Herong’s Tutorial Examples). PKI can get quite complex when adding more trusted authority levels and these are generally used for reseller CAs such as VeriSign or GlobalSign.

Outside of communications to a Web Servers, there are other ways in which PKI can be involved, such as securing communication to a database server, encrypted email communications, used with window’s domain networks, securing Internet of things (IoT) devices, physical access cards for building access (Josh Fruhlinger, 29 May 2020 CSO Online).

## Issues with PKI

Public Key Infrastructure has helped keep networks secure for years but it doesn’t come without its flaws. In short, PKI uses many different components which increases the attack surface and can be prone to user error. CA’s can be hosted internally, depending on how the company manages their IT Infrastructure, which means an administrator (a human) maintains their private and public keys, management of the Certificate revocation list (CRL) and maintains the CA server itself (Roger A. Grimes, 30 June 2015, CSO Australia). This becomes a concern when users begin to access their work on an unmanaged BYOD device, operating on their private network with no VPN Tunneling back to a corporate network.

This is just an example of a company handling their own CA server internally but there has been known evidence of CA resellers mishandling their digital certificates. One example is with GlobalSign who manage to take down a portion of the internet, sites that went offline include Wikipedia, Dropbox, and Financial Times (Bob Cromwell, 2021).

# Blockchain

## What is Blockchain

**What does it do? (600 words)** *What is the state of the art of this new technology? What can be done now? What is likely to be done soon? (Say in the next 3 years)? What technical or other developments make this possible?* Blockchain is decentralized, operating as a peer-to-peer (P2P) network. The core of the technology is performing transactions between multiple participating computers (nodes) that store the data in a distributed manner. Each computer participating in the blockchain will have its own copy which is updated whenever a new transaction is completed, this creates a new block of data (hence the name). The blocks within the blockchain will include the data, the Hash and the Hash of the previous block. Depending on the type of blockchain you can store any value, whether this is user data (document or file), money or even a digital certificate. The block also contains metadata which could contain the identity of the user or transaction logs (Tania H, Jan 04, 2018, RubyGarage).

Blockchain gained popularity with its first widely used digital currency, Bitcoin. Blockchain made it possible for these cryptocurrencies to exist as the system itself acts as a public ledger that captures transaction history. Coupled with the hashing algorithm used, this system is impossible to crack. The beauty of blockchain is in its decentralized computing, the file (depending on the blockchain) will update every 10 minutes to all the nodes which offers a level or redundancy. The other benefit is only being able to write new data on a blockchain. Through the hash file algorithm that this technology offers, you cannot update or crack the previous saved blocks as this will change the hash and that piece of data becomes invalid (Token Metrics, July 23, 2021, Intro to Blockchain and Cryptocurrencies | an Ultimate Guide). Below are graphs on how the hashing mechanism works within a blockchain.

Hash intact:

A picture containing icon

Description automatically generated

Image used from  6 Tania H, Jan 04, 2018, RubyGarage (<https://rubygarage.org/blog/how-blockchain-works>)

Hash changed – chain broken:

A picture containing timeline

Description automatically generated

Image used from  6 Tania H, Jan 04, 2018, RubyGarage (<https://rubygarage.org/blog/how-blockchain-works>)

Another feature that blockchain contains is proof-of-work (PoW) which acts as a consensus. Proof-of-work is how a cryptocurrency mines and adds to the blockchain, this is achieved by solving mathematical problems which is how the new block is added to the blockchain. The nodes in a blockchain are referred to miners and the process for solving these mathematical problems called mining (Bybit Learn, December 8, 2020, What is proof of work (PoW in Blockchain?).

As blockchain has developed through cryptocurrencies, it has become increasingly noticed for its potential for decentralized data storage. This will cater for the emerging IoT devices and data exchanges from BYOD devices to cloud systems (Nexus, University of Michigan Engineering, October 20, 2020). Proof-of-work (PoW) offers a timestamp mechanism in which the nodes on the network solve computational puzzles to create the next block and push over the network and add to the blockchain (Bybit Learn, December 8, 2020, What is proof of work (PoW in Blockchain?). This mechanism will prevent denial of service attacks due to the scope of the peer-2-peer model that blockchain works on. The only downside to PoW is the sheer computing power that is required to mine the blocks and what is concerning is other countries are contending with mining crypto which is using the earth’s resources (statista, 2021). Despite the usage of blockchain for cryptocurrencies, the technology itself will transform industries such as supply chains, retails, manufacturing, financial services and even security.

## What Blockchain-based PKI will fix

As Blockchain technology is used more outside of the cryptocurrency space, we will begin to see the Public Key Infrastructure running on blockchain. As of this point in time, the technology is still in development, but it will resolve several issues that we see with PKI. One of these issues would be the need for a Certificate Authority (CA), with Blockchain Integrity and Auditing built into the technology there is no longer a need for a 3rd party to oversee the handling of certificates and public keys. This is simply because of how Blockchain works, which is a distributed ledger which saves meta-data based on transaction history. However, in this context for PKI, it would be digital certificates and public keys (Andrii Fedotov, January 24,2019, Hackernoon).

This will also take the burden off IT administrators having to host an on-premises CA and eliminate user error with mishandling keys, server maintenance or malicious attacks to their CA servers. As the PKI model was built to support the older centralized model which companies are increasingly moving away from due to cloud computing, mobile devices, and BYOD devices. Blockchain is built for peer-2-peer communications which is distributed and supports the current trend for companies moving towards cloud systems. Because Blockchain is distributed, there is built-in redundancy as multiple nodes over the network are downloading the new blocks via Proof-of-work (PoW) (Remme, Jan 27, 2020).

The only downside to blockchain is that there’s no governing control, this is due to the nature of the technology working as a peer-2-peer model, however there is great trust within the code that drives blockchain. As Satoshi Nakamoto writes: “*The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they’ll generate the longest chain and outpace attackers*.” (Satoshi Nakamoto, October 31, 2001 Bitcoin: a Peer-to-Peer Electronic Cash System whitepaper) As long as this is the case, blockchain-based PKI will be revolutionary within the cyber security space.

# My Thoughts

Currently for work, I use my personal computer when working from home and most of our users in our organization do the same, this creates a challenge for our organization to keep these devices secure. However, BYOD devices are becoming increasingly popular and sure, you can enrol the computer or mobile device into a Mobile Device Management (MDM) system, but users do not want their companies’ IT team to be able to monitor their activity on their personal computer. As it stands, there are not many measures preventing a user’s access to cloud systems. Users prefer to use devices that they’re more familiar with (i.e their personal computer), whether it is because of their preferred OS, higher specs, or configurations etc. At least with blockchain-based PKI, this would cover some of these implications. Aside from blockchain-based PKI, there are other security vulnerabilities but what is important to note here is that if you are representing a company then there needs to be evidence that the data came from the device that represents your company, this will increase integrity and confidence within organizations and the vendors that they conduct business with.

Another benefit of this technology is no longer needing to administrate an on-premises CA server. None of the IT technicians on my team are trained security professionals and have to depend on a managed service provider (MSP) to look after some of these systems. As technicians looking after a customer, there have been cases of half completed work, “band-aid” fixes or simple mistakes like powering the server back on after an update. Although they have the expertise and skills required to operate these specialized systems, they can lack the care and attention that an employer of the company network provides. So far, this hasn’t been the case for our CA server but if it did, the repercussions could be catastrophic for our company.

On a broader level, blockchain will increase secure data transmission over the internet and reduce the level of human errors from CAs. Although without CAs, there is a level of concern as to who monitors the identity. Unless you are part of that blockchain, it will be very difficult for an ethical hacker to prevent criminal activity to occur due to the security and lack of overarching authority.

# References:

1. Brien Posey, September 15, 2005, TechRepublic ([A beginner's guide to Public Key Infrastructure - TechRepublic](https://www.techrepublic.com/article/a-beginners-guide-to-public-key-infrastructure/))
2. Josh Fruhlinger, 29 May 2020 CSO Online ([What is PKI? And how it secures just about everything online | CSO Online](https://www.csoonline.com/article/3400836/what-is-pki-and-how-it-secures-just-about-everything-online.html))
3. Dr. Herong Yang, 2021, PKI Tutorials – Herong’s Tutorial Examples (<https://www.herongyang.com/PKI/Introduction-What-Is-PKI-Public-Key-Infrastructure.html>)
4. Bob Cromwell, 2021 ([Massive Failures of Public-Key Infrastructure (PKI) (cromwell-intl.com)](https://cromwell-intl.com/cybersecurity/pki-failures.html))
5. Roger A. Grimes, 30 June 2015, CSO Australia (<https://www.csoonline.com/article/2942072/4-fatal-problems-with-pki.html>)
6. Tania H, Jan 04, 2018, RubyGarage (<https://rubygarage.org/blog/how-blockchain-works>)
7. Token Metrics, July 23, 2021, Intro to Blockchain and Cryptocurrencies | an Ultimate Guide (<https://blog.tokenmetrics.com/intro-to-blockchain-and-cryptocurrencies/>)
8. Bybit Learn, December 8, 2020, What is proof of work (PoW in Blockchain?) (<https://learn.bybit.com/blockchain/what-is-proof-of-work-in-blockchain/>)
9. Nexus, University of Michigan Engineering, October 20, 2020 (<https://digitalskills.engin.umich.edu/fintech/top-five-emerging-blockchain-technologies/>)
10. Andrii Fedotov, January 24, 2019, Hackernoon (<https://hackernoon.com/distributed-pki-development-and-use-cases-a828287a2e67>)
11. Remme, Jan 27, 2020 (<https://remme.io/blog/how-blockchain-addresses-public-key-infrastructure-shortcomings>)
12. Satoshi Nakamoto, October 31, 2001 Bitcoin: a Peer-to-Peer Electronic Cash System whitepaper ([bitcoin.pdf (satoshinakamoto.me)](http://satoshinakamoto.me/bitcoin.pdf))
13. Statista (<https://www.statista.com/statistics/1200477/bitcoin-mining-by-country/>)