ABSTRACT

THE BLOCKCHAIN SECURITY AND IDENTITY PROOFING

By Suresh Babu Yella

The idea of the blockchain, an open ledger maintained and extended by a peer-to-peer network as it adopts decentralized consensus mechanism to complete the transactions that make blockchain an expensive and difficult to attack. The distributed ledger of blockchain has found application in many fields, from the exchange, digital money, smart contracts, grocery to supply chain. It can also be worked to implement a solution for identities proofing to secure Identities in the real world. In this paper, we will cover some potential vulnerabilities with blockchain technology like 51% attack, Double spending Vulnerabilities in smart contracts and a solution to defend a system against any particular attack. Also, we will discuss how we can decentralize the identity systems using blockchain technology thus identities are protected from theft, data leaks, threats, and fraudulent activities. A node, identity proof verifier, will validate the identities can give individuals greater control over their personal information and Identity Proofing can satisfy Business KYC requirements, attestations and to integrate trusted 3rd parties, etc.

Table of Contents

List of Tables

List of Figures

Chapter I

Introduction

The blockchain is a concept that originated to avoid third-party involvement in any financial transaction in a whitepaper named Bitcoin: "A Peer-to-Peer *Electronic Cash* System" by Satoshi Nakamoto (2009). We will also be discussing the types of blockchain-based business needs, cryptography, and consensus, which mitigate the risk of fraud.

1.1 Cyber Threat Landscape and Security Challenges

Cybersecurity is a 20-year-old phenomenon, but in the past five years, it has become more challenging for defenders to protect themselves against emerging threats, such as zero-day exploits, crypto-ransomware, terabytes of DDoS attacks, multi-vector malware, and advanced social engineering.

1.2 Current threat landscape

In the new era of cyberspace, technology transformation has been a core factor for continuous security innovation and operations. In the world of connected vehicles, IoT, mobility, and the cloud, it opens up a focal point for cybercrime, targeted attacks, and industrial espionage. Once an attacker finds a vulnerability and determines how to access an application, they have everything they need to build an exploit for the application, and

so it is critical to develop strong vulnerability management. Remember, the effectiveness of vulnerability management depends on the organization's ability to keep up with emerging security threats and models.

1.3 Ransomware

Ransomware is malware in which information on a victim's computer is encrypted, and ransome is demanded before granting them access. Ransomware is one of the trending and high-return types of crime ware. The ransomware hosts the service over the dark web, which allows any buyer to create and modify the malware.

1.4 Distributed denial-of-service (DDoS) attacks

A DDoS attack is a malicious attack to disrupt the legit user traffic of a server by overwhelming it with a flood of traffic. DDoS differs from DoS by its distributed nature, attacking a target from several networks of compromised systems. These compromised computer systems are called bots, and a botnet refers to a group of such bots under the control of the same malicious actor.

1.5 Insider threats

Any form of threat can originate from inside an organization, and it's not just limited to an employee with malicious intent; it can even be contractors, former employees, board members, stockholders, or third-party entities.

1.5.1 Some more ways to define insider threats

Insider Threats defines an insider as a current or former employee, contractor, or business partner who meets the below criteria:

- Has or had authorized entry to an organization's network, data
- Has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, availability of the organization's information or information systems break.

1.6 Data Breaches

Data breaches may involve the leaking of sensitive corporate documents, technical blueprints, intellectual property, trade secrets, or even emails. This has always been massive in number and has an even bigger impact on businesses. Sophisticated attackers are capable of weaponizing malware highly tailored for the target, and they are also managing to deliver the malware silently.

Table 1. Several ways of data breaches.

Malicious attacks	Adversaries can launch a malware or malware-less attack, leveraging application vulnerabilities to exfiltrate sensitive information.
Weak security systems	Attackers have become more advanced and persistent in nature. Attackers can use stolen credentials to look like legitimate users in the network and hence bypass existing security systems such as firewalls, intrusion prevention system (IPS), and endpoint security.
Human error	As per a Verizon Data Breach investigation report in 2017, 88% of data breaches involve human error. Human error is something that all the organizations have to deal with.

Chapter II

Introducing Blockchain

In this chapter, the blockchain will be introduced with an insight into the technology and its business use cases. The blockchain is a concept that originated to avoid third-party involvement in any financial transaction in a whitepaper named *Bitcoin: A Peer-to-Peer Electronic Cash System,* by *Satoshi Nakamoto*. We will also be discussing the types of blockchain-based business needs, cryptography, and consensus, which mitigate the risk of fraud.

2.1 Fundamentals of the blockchain.

The blockchain is a decentralized database that keeps records of all transactions secure and in an append-only fashion.

2.2 Internet versus blockchain

The internet is a more-than-30-year-old technology with the purpose of sharing data over TCP/IP and the Open Systems Interconnection (OSI) model stack. From the birth of the internet, every novel technology had disrupted an existing technology, whether it's an email or the web, or even e-commerce. The internet is one of the powerful technologies and has been powerful enough to spread ideas to impact and create illusions for reality. In Figure 1, an overview of the Blockchain evolution.

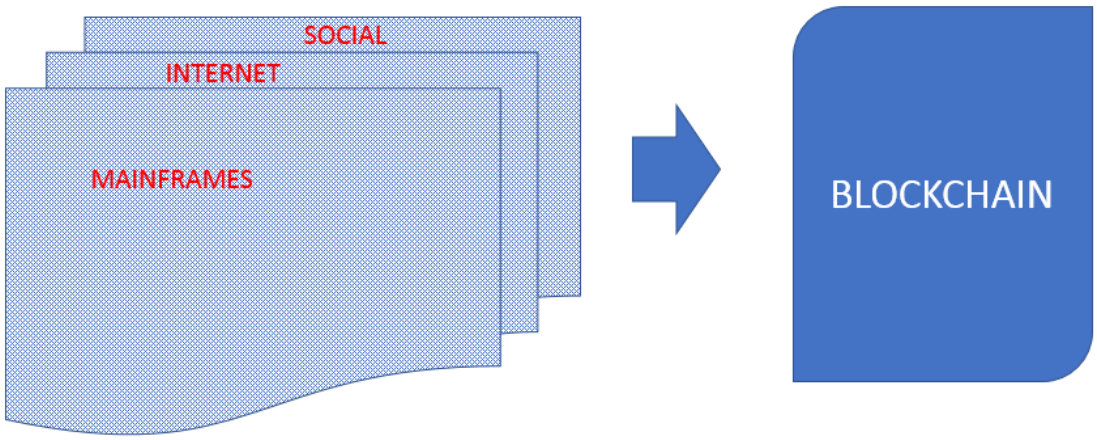

Figure 1. Internet evolution from Mainframes to Blockchain

2.3 Web app versus dApp

A web app is simply a web-based application, which is widely used in client-server models to serve users. However, a decentralized application (dApp) is an application that runs on a peer-to-peer network of machines.

The standard web application uses CSS, HTML, and JavaScript and it renders a frontend page. It fetches the information from a database through an API call. dApp's frontend uses the same technique to render the page, but instead of calling the API, dApp uses a smart contract, it connects to the blockchain.

2.4 How blockchain works

Let's understand the workings of the blockchain ledger in its simplest form. To understand the system in its generic form, it is important to use several states of blockchain and explore them further:

1. Transaction preparation: At this stage, party A creates a transaction that includes information including the public address of the receiver, a source digital signature, and a transaction message. Now, this transaction is made available to all the nodes in the blockchain.
2. Transaction verification: The blockchain nodes work in a trustless model, where each node (the machine running the blockchain client software) receives this transaction and verifies the digital signature with party A's public key. After successful verification, this authenticated transaction is parked in the ledger queue and waits until all the nodes successfully verify the same transaction.
3. Block generation: The queued transactions are arranged together, and a block is created by one of the nodes in the network. In the Bitcoin blockchain, Bitcoins are rewarded when a Bitcoin node, also known as a miner, creates a block by solving some mathematically complex problem.
4. Block validation: After a successful block generation, nodes in the network are processed for an iterative validation process where the majority of the nodes have to acquire consensus. There are four popular ways to achieve consensus.
    a. Proof of Work (PoW)
    b. Proof of Stack (PoS)
    c. Delegated Proof of Stack (DPoS).
    d. Practical Byzantine Fault Tolerance (PBFT).

Bitcoin uses PoW to achieve consensus; however, Ethereum uses PoS for consensus. This mechanism impacts financial aspects and ensures the security of all transaction operations.

5. Block chained: After a successful consensus mechanism, the blocks are verified and are added to the blockchain. Figure 2 shows states of the blockchain.

The building blocks of blockchain technology is built over a group of existing technologies that have been widely used across the industry. Let's go through each component of the blockchain.

2.4.1 Block

A distributed ledger is stored in a database and gets updated by each participant in the

blockchain network. A ledger is a series of units called blocks.

The network consists of a network of several independent machines named nodes. Unlike traditional databases that store entire information on a centralized database server, Blockchain nodes keep the copy of the entire database with an administrative role. Even if one node goes down, the information will remain available for the other nodes, as shown in the following diagram:

Figure 2. Peer to Peer Blockchain

The moment a node joins the blockchain network, it downloads the updated blockchain ledger. Each node is responsible for managing and updating its ledger with validated blocks. The node maintains the ledger and organizes it in the form of blocks connected to the hashing algorithm, as shown in the following diagram:

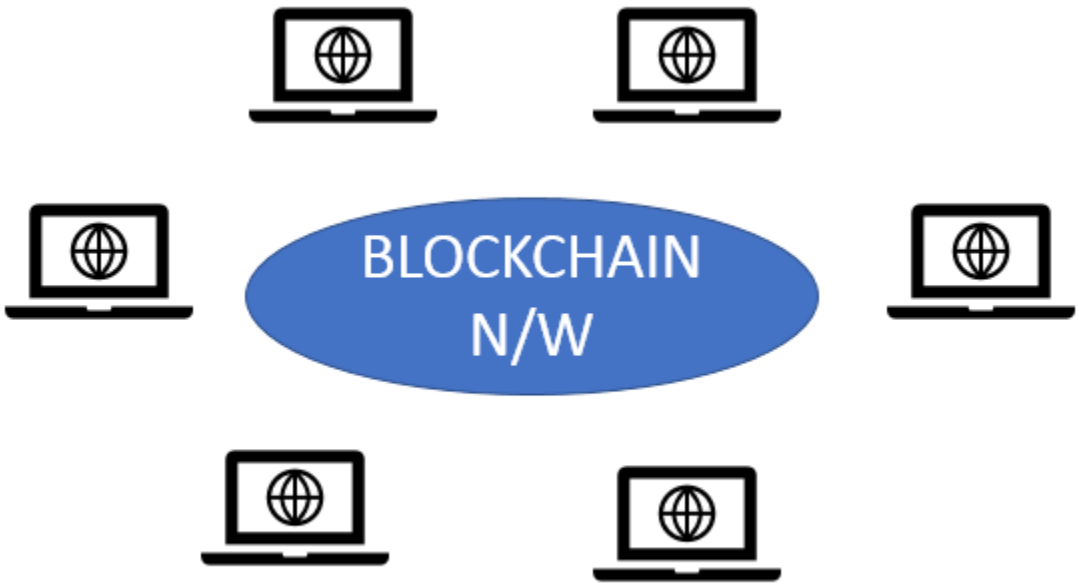

Figure 3. Blockchain Network

Multiple transactions are bundled together to form a block, and in its simplest form, it's a data structure. Every cryptocurrency has its own blockchain with its own customized properties. For example, a block in a Bitcoin blockchain is generated every 10 minutes, and the size of each block is 1 MB, whereas a block in an Ethereum

blockchain is generated every 12-14 seconds, and the size of each block is 2 KB. Take a look at the following diagram:

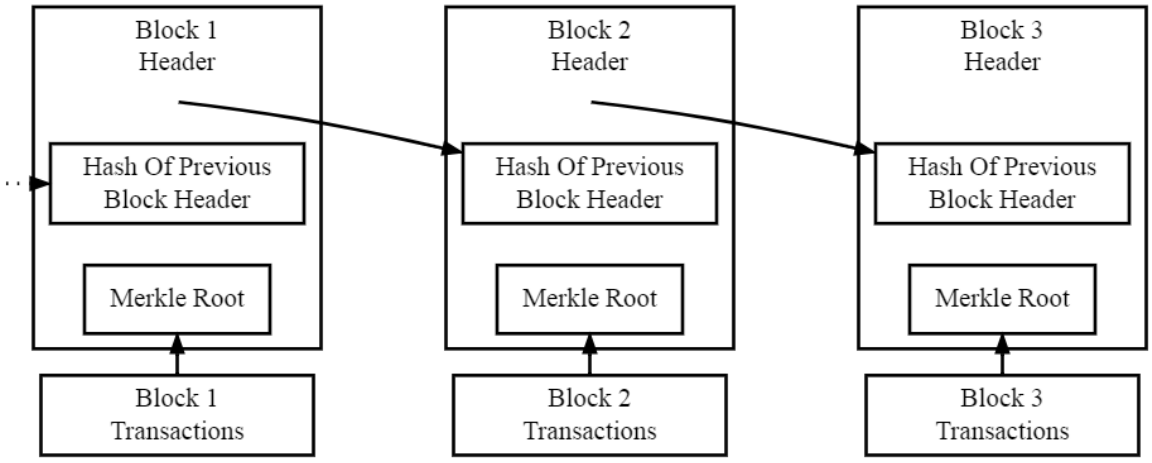

Figure 3. Simplified Blockchain
(modified from https://bitcoin.stackexchange.com/questions/35448/is-it-chain-of-headers-rather-than-a-chain-of-blocks. by David A. Harding)

Table 2. A block consists of a block header and a block body:

Block header	A block header helps us identify a specific block in the blockchain.
Version	It's a 4-byte field that's used to track software or protocol
Timestamp	This is a 4-byte field that indicates the creation time of the block in seconds.
Hash of the previous block	This is a 32-byte field that indicates the hash of the previous block in the chain.
Nonce	This is a 4-byte field that's used to track the PoW algorithm counter.
Hash of Merkle root	This is a 32-byte field that is a hash of the root of the Merkle tree of the block transaction.
Block body	This part of the block consists of a list of transactions. In the Bitcoin world, one block consists of more than 500 transactions on average. Each transaction has to be digitally signed; otherwise, it is treated as invalid.

In blockchain, a node arranges the entire ledger in the form of chronologically connected blocks. To ensure that the ledger remains tamper-proof, each block is made dependable on the previous block.

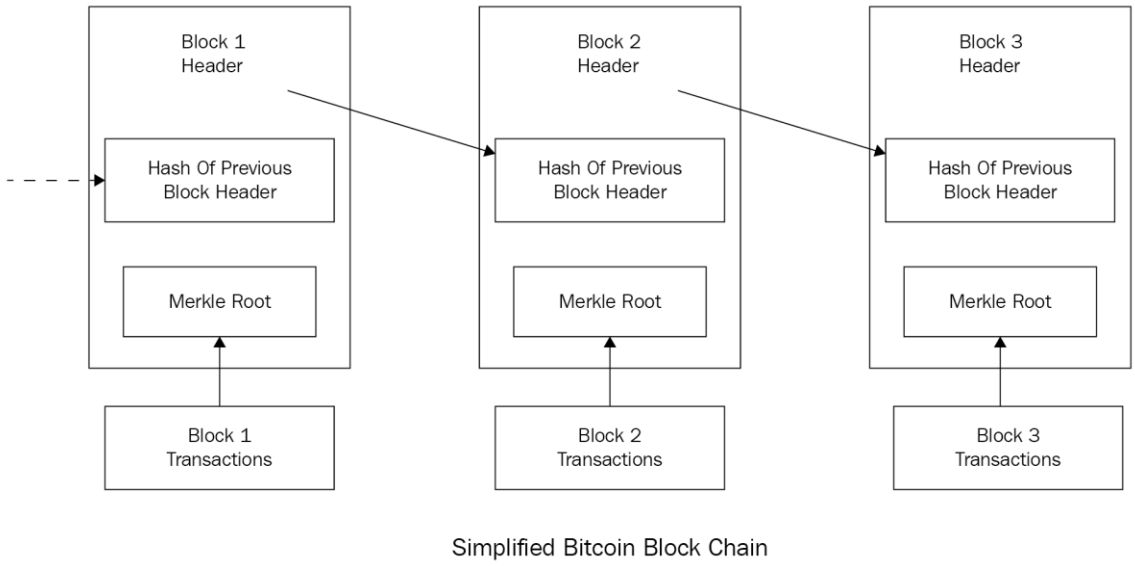

Figure 4. Bitcoin Block Chain
(modified from https://blockgeeks.com/guides/what-is-hashing/)

Every block points to the hash of the previous hash block, and this becomes the backbone of the blockchain's immutable system. Now, even if a block in between is altered or disturbed by any means, a hacker can never achieve the same blockchain as a small change in the block can result in a drastic change in the resulting hash. With thousands upon thousands of transactions in every block, it becomes extremely difficult to find one transaction that won't be time consuming and process-sensitive. To avoid this complex work, a comprehensive hash tree has been developed named the Merkle tree.

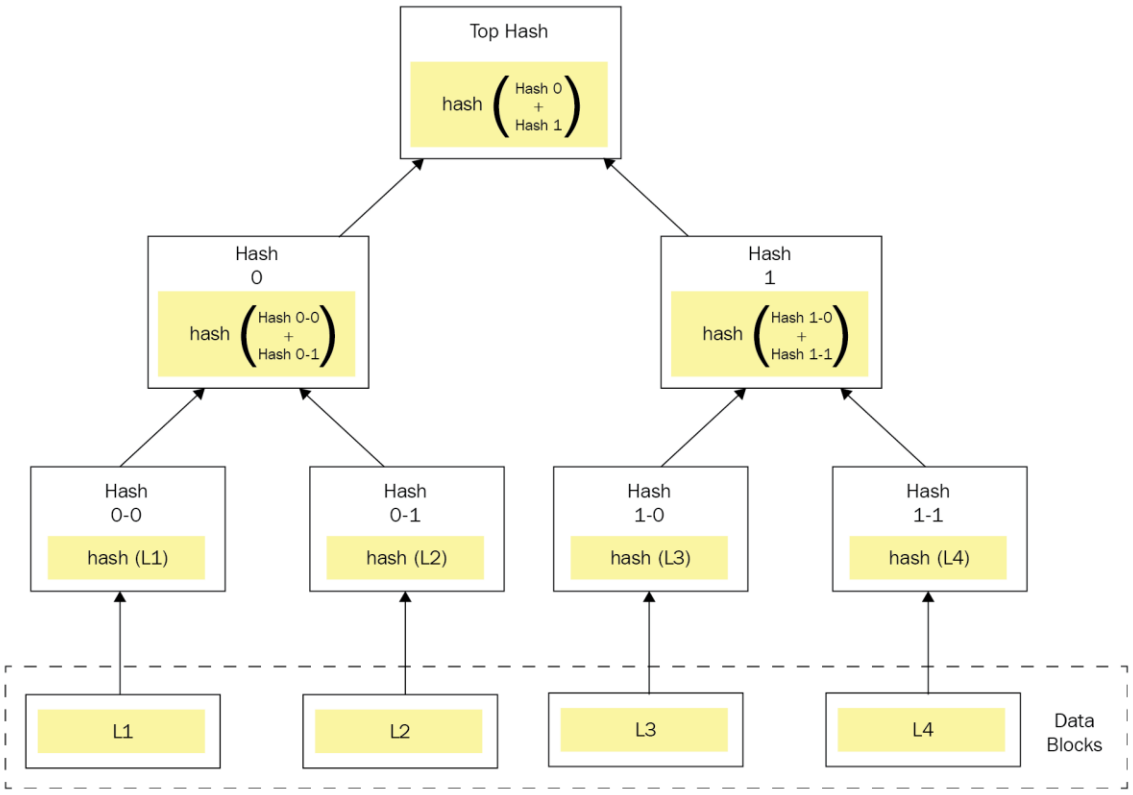

Figure 5. The Merkle tree
(modified from https://blockgeeks.com/guides/what-is-hashing/)

2.4.2 Consensus – the core of blockchain

The consensus is an integral component of the blockchain system and is responsible for achieving agreement in a distributed environment. The following are four methods that are used to achieve consensus with blockchain:

1. PoW: One of the most popular methods to achieve consensus in blockchain was invented by Satoshi Nakamoto, the founder of Bitcoin. In this type of consensus, fraud attempts are avoided based on the fundamentals of trusting a particular node that has been created to do the maximum computational work. The block owner, also known as a miner in the world of cryptocurrency, knows that having

powerful computational resources can achieve a better hash rate and the chance of getting rewarded with Bitcoin increases. A new transaction is broadcast to all the nodes in the network, and each node keeps listening to these transactions. Nodes that want to gain incentives through Bitcoin are known as miners, but they don't just listen, they collect transactions. Miners have to solve some complex mathematical problems with a PoW algorithm. The one who solves it first gets rewarded with Bitcoin. Finally, verified blocks are added to the blockchain of every miner. When a miner wins the block,

each block carries a set of bitcoins (BTC), which they then receive:

a. Jan 2009-Nov 2012: It was 50 BTC per block
b. Nov 2012-Jul 2016: It was 25 BTC per block
c. Jul 2016-Feb 2020: It is 12.5 BTC per block
d. Feb 2020-Sep 2023: It is going to be 6.25 BTC per block

2. PoS: This is another method to achieve consensus in the blockchain among nodes and to validate transactions. Unlike PoW, with PoS, the block generator will not be selected based on its current stack of wealth. Blocks are never rewarded in this mechanism, and the miner in PoS is called a forger.
3. DPoS: This is another consensus protocol and is known to be a faster and more efficient model. DPoS uses a democratic method to solve consensus problems. It takes around one second to elect the block generator in the network and confirm the transaction. This way, you don't just solve the consensus issue, but you also eliminate unwanted regulatory interference.
4. PBFT: Byzantine failure is the state of appearing both failed and functioning to

fault detection systems and showing a different pattern to different detectors. If some of the node members send inconsistent information to others about transactions, it may lead to a huge dilemma for an entire network. PBFT is a solution to protect the network against Byzantine faults.

Chapter III.

Blockchain on the CIA Security Triad

In this chapter, we will be discussing the fundamental approach to arranging the components of a native blockchain and Hyperledger in the form of *Confidentiality, Integrity, and Availability (CIA)* security triad model.

3.1 What is the CIA security triad?

CIA is a framework/model that's used to arrange a list of security controls and systems used by the information security (InfoSec) team. It is also called Availability, Integrity, and Confidentiality (AIC) security triad. The purpose of the triad is to deliver a standard framework to evaluate and deploy information security policies, independent of the underlying technology, network, or system.

3.1.1 Confidentiality

Confidentiality is a way to keep information hidden from unauthorized people. When information that has to be secret remains a secret, you achieve confidentiality.

3.1.2 Integrity

Integrity is a way to protect the modifying of information from unauthorized party. It is mandatory

compliance for every InfoSec body.

3.1.3 Availability

Availability refers to on-time and Realtime access to data. Availability can often be viewed as one of the most important parts of a successful information security

program. Ultimately end-users need to be able to perform job functions; by ensuring availability an organization is able to perform to the standards that an organization's stakeholders expect.

Chapter IV.

Deploying PKI-Based Identity with Blockchain

Organizations have deployed several ways to authenticate users, based on methods such as multi-factor authentication, one for each system/application, single sign-on (SSO) A public key infrastructure (PKI) is an open framework built to resolve trust factors between internet-connected users.

In this chapter, we will learn about the below topics: Public key infrastructure and Challenges of the existing PKI model.

4.1 PKI

Organizations may have hundreds of cloud-based applications to manage and maintain. Managing individual access control and authentication is a difficult daily task. When it comes to internet users and enormous web applications, it becomes difficult to trust individual websites, and users tend to lose their private and confidential information through them. A PKI provides a secure means of authenticating an individual's identity.

The PKI solves this problem by appending a trusted third party (TTP) between Bob and Alice. So, before they can start getting to know each other, they have to establish trust, and the TTP helps to accomplish that

4.2 Certificate

A certificate is an electronic ID that represents the identity of a user or a device interested in communicating over a network. The certificate basically ensures that only a

legitimate user can connect to the network. The following are the three main types of certificates:

- Secure Socket Layer (SSL) certificate: SSL server certificates are installed on the server hosting services, such as a web application, mail server, directory, or LDAP server. This certificate contains identifying information about the organization that owns the application. SSL certificates also contain a system public key. The subject of the certificate matches the hostname of the server. This certificate has to be signed by a trusted certificate authority. The primary hostname is listed as the Common Name in the subject field of the certificate. Client certificate: Client certificates are used to identify an internet user, a device, a gateway, or any other type of device. It is a digital credential that validates the identity of the client who owns the certificate. Today, many applications allow using certificates to authenticate users for a specific resource instead of a username and a password. Two users communicating over email will also use a client certificate to authenticate their respective identities.
- Code signing certificate: Code signing certificates are used to sign software running on the system. With millions of applications being downloaded by a user machine, it is important to verify the code; code signing certificates play an important role in this.
- Email certificate: The sender needs to identify which public key to use for any given recipient with the S/MIME protocol. The sender gets this information from an email certificates. Usually, the S/MIME protocol is used when email communication is deployed within the organization and with its own CA.

Chapter V.

Two-Factor Authentication with Blockchain

Every organization has hundreds of applications and databases, and its employees access them every day using their credentials (username and password). An attacker with such valid credentials can bypass existing security solutions, as they look like a legitimate user.

In this chapter, we will cover the below topics:

What is 2FA?

Blockchain for 2FA

5.1 What is 2FA?

2FA is an extra layer of security that's used to ensure that only the legitimate owner can access their account. In this method, the user will first enter a combination of a username and password, and, instead of directly getting into their account, the user will be required to provide other information.

Something that the user knows	This could be information such as a password, an answer to a secret question, or maybe a personal identification number
Something that the user has	This method includes the second level of authentication based on card details, through smartphones, other hardware, or a software token.
Something that the user is	This is one the most effective ways to verify the user on the second step, and this is accomplished with biometric

	data such as keystroke dynamics and mouse behavior.

5.2 Blockchain for 2FA

The blockchain is being hailed as one of the most revolutionary and disruptive technologies out there. Blockchain has been disrupting the cybersecurity solutions-based CIA security triad principle. 2FA has been critical in security measures for several years; however, attackers sometimes manage to compromise these systems. We will understand how blockchain can transform the 2FA system to achieve an improved security method.

5.3 Solution architecture

Being the latest technology, blockchain is still in its testing phase with several organizations. For this chapter, we will be using the Ethereum blockchain to turn up the 2FA system. Ethereum allows an application to be programmed with a smart contract. In the following diagram, the basic flow between the user, the web application, and the The Ethereum-based repository is depicted:

Chapter VI.

Deploying Blockchain-Based DDoS Protection

The internet is expanding dramatically in both the number of users and applications and their respective bandwidth. Over the past few years, a user has entered the world of internet, known as a smart device. It can be a refrigerator, a microwave, it can be as complex as a drone or
automated vehicle. These smart devices are also referred to Internet of Things (IoT) devices, monitoring the functionality and operations of connected utilities. Despite of enough use cases, attackers are making use of them to launch some massive cyber attacks called distributed denial-of-service (DDoS) attacks. In this chapter, you will learn about DDoS attacks and how blockchain can be more effective at defending organizations from such massive attack operations.

In this chapter, we will cover the following topics:

1. DDoS attacks
2. Types of DDoS attacks
3. Challenges with current DDoS protection solutions
4. How blockchain can transform existing DDoS protection platforms

5.1 DDoS attacks

A DDoS attack is a malicious attempt to disrupt legit traffic to a server by

overwhelming the target with a flood of requests from geographically dispersed systems. Now, let's first understand how a denial-of-service (DoS) attack works. During DoS attacks, the attackers bombard the target machine

5.2 Challenges with current DNS

Today, DNS has become the heart of the internet and organization's infrastructure. The DNS is a critical infrastructure that no organization can function without. However, despite increasing investment in network and information security, attackers manage to invade the network, and the DNS remains a vulnerable component in the network infrastructure that is often used as an attack vector. Firewalls leave port 53 open and never look inside each query. Let's look at one of the widely used DNS-based attacks:

5.3 DNS spoofing

When a DNS server's records are altered to redirect the traffic to the attacker's server, the DNS gets hijacked. This redirection of traffic allows the attacker to spread malware across the network. DNS spoofing can be carried out in one of the following three ways:

5.4 Blockchain-based DNS solution

Blockchain technology has the capabilities to transform several industries, and in this chapter, we are going to use it for managing a name server to overcome some of the most critical DNS challenges. DNSChain is one of the most active projects to transform the DNS framework and protect it from spoofing challenges.

DNSChain is a blockchain-based DNS software suite that replaces X.509 public key infrastructure (PKI) and delivers MITM proofs of authentication. It allows internet users to set a public DNSChain server for DNS queries and access that server with domains ending.

References

[1] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187.

[2] BLOCKCHAIN. (2018). Mix, 42(4), 10.

[3] Zachary Baynham-Herd. (2017). Technology: Enlist blockchain to boost conservation. Nature, 548(7669), 523-523.

[4] Underwood, S. (2016). Blockchain beyond bitcoin. Communications of the ACM, 59(11), 15-17.

[5] De Filippi, P., & Wright, A. (2018). Blockchain and the law: The rule of code.

[6] "Fishbone (Ishikawa) diagram," ASQ, 2016. [Online].

[7] Rawls, John. [https://books.google.com/books?id=kvpby7HtAe0C&pg=PA18 "A Theory of Justice"]. Harvard University Press, 1971, p. 18.