BLOCK CHAIN SECURITY PROJECT

AMRATH FATHIMA SHIFA N

KARTHIKA G

INTRODUCTION

Blockchain is a list of blocks. Each block comprises information such as transactions and a unique hash to identify each block. It is a distributed, decentralized ledger that is widely becoming popular these days.

.

What is Blockchain Security?

Security is managed in order to protect some vital information so that hackers or other unauthorized users do not get access to it. With the increasing dependency on Blockchain networks, Blockchain security has become a prime concern. Blockchain security is a risk management technique that aims to secure transactions and hence the whole blockchain network. It is usually implemented with the help of cybersecurity, authorized services, and ethical users.

Why Does Blockchain Require Security?

Blockchain is an immutable ledger with no involvement of third-party organization. It also uses cryptography to hide some details. So hackers find it almost impossible to tamper with the blocks. But there are some loopholes that allow the malicious users to perform malicious activities as blockchain networks are not immune to cyberattacks and fraud. Blockchain attacks are cyber attacks that can be done by outside malicious users as well as the users involved in the network.

ATTACKS

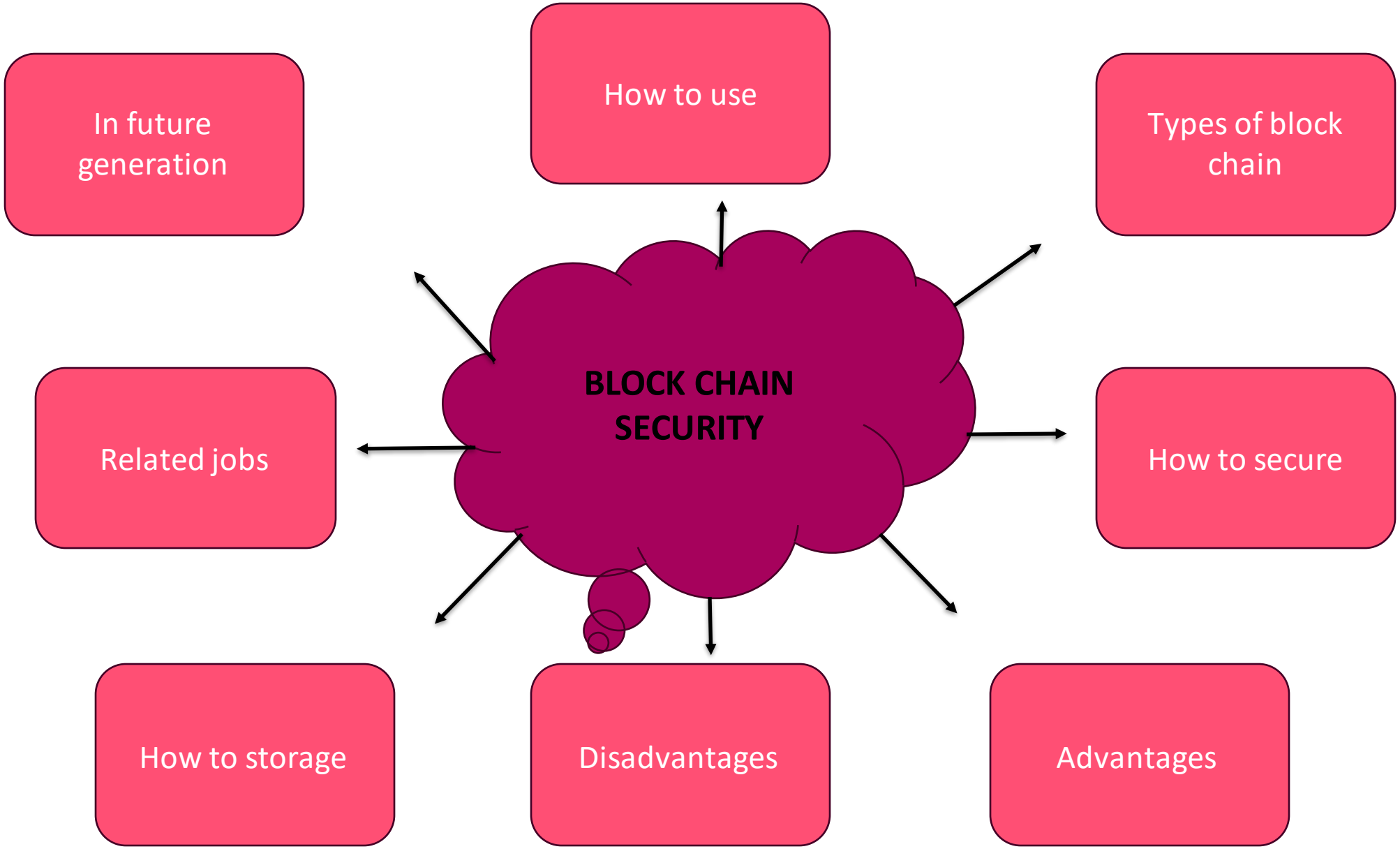
Some of the attacks are as follows:

- **Sybil Attack:** Hackers try to increase the traffic in the network like Sybil Attack. In this, the malicious user floods the network with unnecessary packets to create traffic in the network.
- **Eclipse Attack:** Hackers try to make duplicates of the node. This is an eclipse attack. The user eclipses(hides) the original node and broadcasts the fake node that was created by the hacker.
- **51% Attack:** Hackers try to control the network. They take control of 51% of the mining and this attack is known as 51%Attack.

Finney Attack: In the Finney attack, the hacker hides the original block and broadcasts the fake block. The transaction is performed. After that transaction for the original block is performed. So a case of double expenditure happens.

Attack Wallet: In this hackers try to attack users' wallets to perform unnecessary transactions.

So security is of prime concern in blockchain as millions and millions of transactions are involved and these are the reasons why Blockchain networks should be secured.


In future generation
How to use
Types of block chain
BLOCK CHAIN SECURITY
Related jobs
How to secure
How to storage
Disadvantages
Advantages

Types of block chain security

However, different use cases require different types of blockchain.

There are four main types of blockchain networks:

1. **public blockchains**
2. **private blockchains**
3. **consortium blockchains**
4. **hybrid blockchains.**

Each one of these platforms has its benefits, drawbacks and ideal uses.

1. Public blockchain

The first type of blockchain technology is public blockchain. This is where cryptocurrency like Bitcoin originated and helped to popularize distributed ledger technology (DLT). It removes the problems that come with centralization, including less security and transparency. DLT doesn't store information in any one place, instead distributing it across a peer-to-peer network. Its decentralized nature requires some method for verifying the authenticity of data. That method is a consensus algorithm whereby participants in the blockchain reach agreement on the current state of the ledger. Proof of work (PoW) and proof of stake (PoS) are two common consensus methods.

2. Private blockchain

A blockchain network that works in a restrictive environment like a closed network, or that is under the control of a single entity, is a private blockchain. While it operates like a public blockchain network in the sense that it uses peer-to-peer connections and decentralization, this type of blockchain is on a much smaller scale. Instead of just anyone being able to join and provide computing power, private blockchains typically are operated on a small network inside a company or organization. They're also known as permissioned blockchains or enterprise blockchains.

3. Hybrid blockchain

Sometimes, organizations will want the best of both worlds, and they'll use hybrid blockchain, a type of blockchain technology that combines elements of both private and public blockchain. It lets organizations set up a private, permission-based system alongside a public permissionless system, allowing them to control who can access specific data stored in the blockchain, and what data will be opened up publicly.

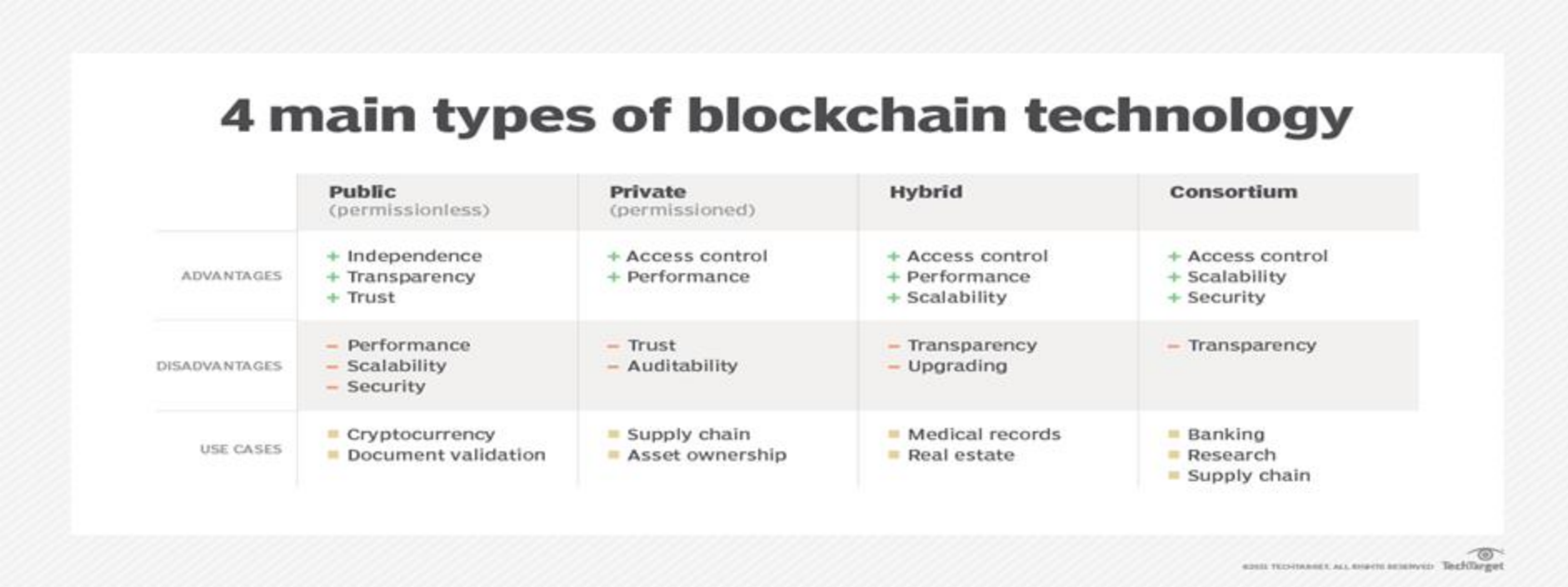
Typically, transactions and records in a hybrid blockchain are not made public but can be verified when needed, such as by allowing access through a smart contract. Confidential information is kept inside the network but is still verifiable. Even though a private entity may own the hybrid blockchain, it cannot alter transactions.

When a user joins a hybrid blockchain, they have full access to the network. The user's identity is protected from other users, unless they engage in a transaction. Then, their identity is revealed to the other party.

4. Consortium blockchain

The fourth type of blockchain, consortium blockchain, also known as a federated blockchain, is similar to a hybrid blockchain in that it has private and public blockchain features. But it's different in that multiple organizational members collaborate on a decentralized network. Essentially, a consortium blockchain is a private blockchain with limited access to a particular group, eliminating the risks that come with just one entity controlling the network on a private blockchain.

In a consortium blockchain, the consensus procedures are controlled by preset nodes. It has a validator node that initiates, receives and validates transactions. Member nodes can receive or initiate transactions.

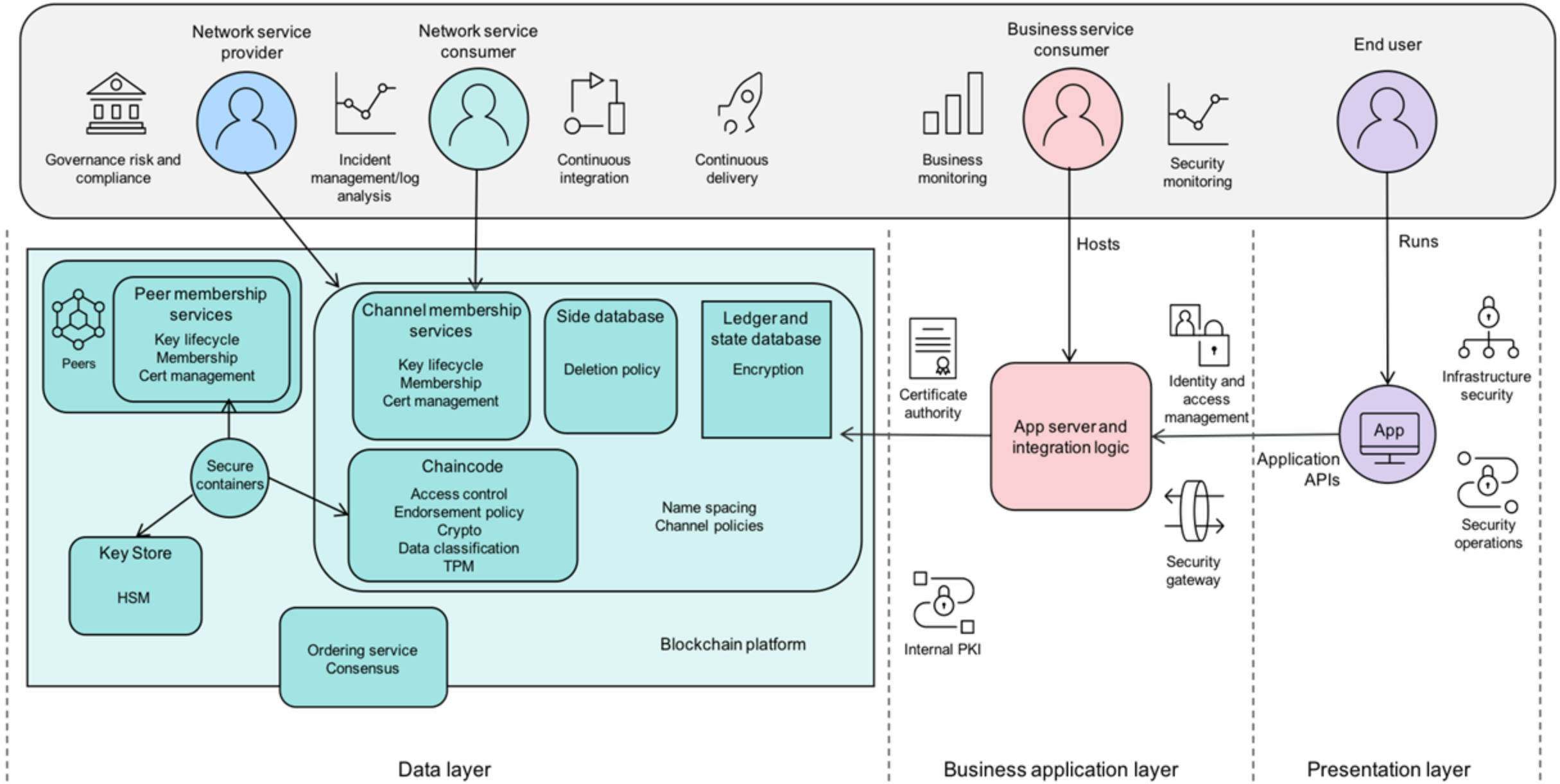


Best Practices For Building Secure Blockchain Solutions

Companies are using many ways to make a smooth secured network for users. But users also have some responsibility so that the whole system gets secured. Some of the ways are:

- **Use of Cold Wallet:** Cold Wallets do not connect to the Internet, therefore users can secure their private keys. The wallet is not prone to cyberattacks.
- **Secure the Internet:** Often hackers try to hack Wifi. Users must avoid public wifi networks at all costs as any hacker can use public networks and can use malware to steal valuable information.
- **Avoid Phishing:** Phishing attacks are common nowadays. Users should not click malicious advertisements. They should remove all the spam emails.
- **Password:** It is always advisable to use strong passwords with a combination of alphabets, numbers, and special characters. Passwords should be changed regularly.
- **Security of personal devices:** Personal devices should be up to date. The patches should be fixed and the latest antiviruses should be installed to protect from virus attacks.

- **Blockchain Penetration Testing:** Those who create blockchain networks should get penetration testing done by an ethical hacker to test the strength of the security blockchain networks and find vulnerabilities if present.
- **Secure keys:** Keys should be secured by the user. Strong cryptographic keys should be used Users should not share the keys with other users.
- **Use private permissioned blockchain:** Business entrepreneurs should use private permissioned blockchain. The permission is necessary as each user is verified before allowing them to enter the blockchain.


Network service provider
Network service consumer
Business service consumer
End user
Governance risk and compliance
Incident management/log analysis
Continuous integration
Continuous delivery
Business monitoring
Security monitoring
Hosts
Runs
Peers
Peer membership services
Key lifecycle
Membership
Cert management
Channel membership services
Key lifecycle
Membership
Cert management
Side database
Deletion policy
Ledger and state database
Encryption
Secure containers
Chaincode
Access control
Endorsement policy
Crypto
Data classification
TPM
Name spacing
Channel policies
Key Store
HSM
Ordering service
Consensus
Blockchain platform
Certificate authority
App server and integration logic
Identity and access management
Infrastructure security
App
Application APIs
Security operations
Security gateway
Internal PKI
Data layer
Business application layer
Presentation layer

Where is Blockchain Data Stored?

Blockchain data is stored on a decentralized public ledger. The data on the ledger is stored in chunks called blocks, which are chained together using cryptography.

- Every block has a unique cryptographic hash as an identifier along with the previous block in the blockchain.

  Each transaction inside a block is timestamped and added to the ledger with each block. Each new block records all transactions and adds them to the previous one. The data stored on Blockchain cannot be altered or removed from the blockchain as it would require alterations on every subsequent block.
- The miner who finds a solution for the proof-of-work puzzle (such as solving an equation by submitting correct answers) is rewarded with newly created bitcoins and has to add that block to the blockchain. But doing this takes time, so miners solve these puzzles using computer processors' power, resulting in competition to solve these puzzles first.

There are different storages to store data in the blockchain:

- **Hashing:** This is a cost-efficient way of storing the data in the blockchain. In this method, only the hash value of the data is stored in the blockchain. The raw data can be stored in the file system and the hash id of the blockchain will be attached to the raw data.
- **TiesDB:** This is an Ethereum-based decentralized application (dApps) to store non-financial data and search through their documents. This allows advanced search and document modifications.
- **BigChainDB:** This database allows developers and enterprises to deploy blockchain proofs-of-concept, platforms, and applications with a blockchain database. This offers immutable data storage, built-in-asset support, low latency, powerful query functionality, and high throughput, thus this is a database with blockchain characteristics.

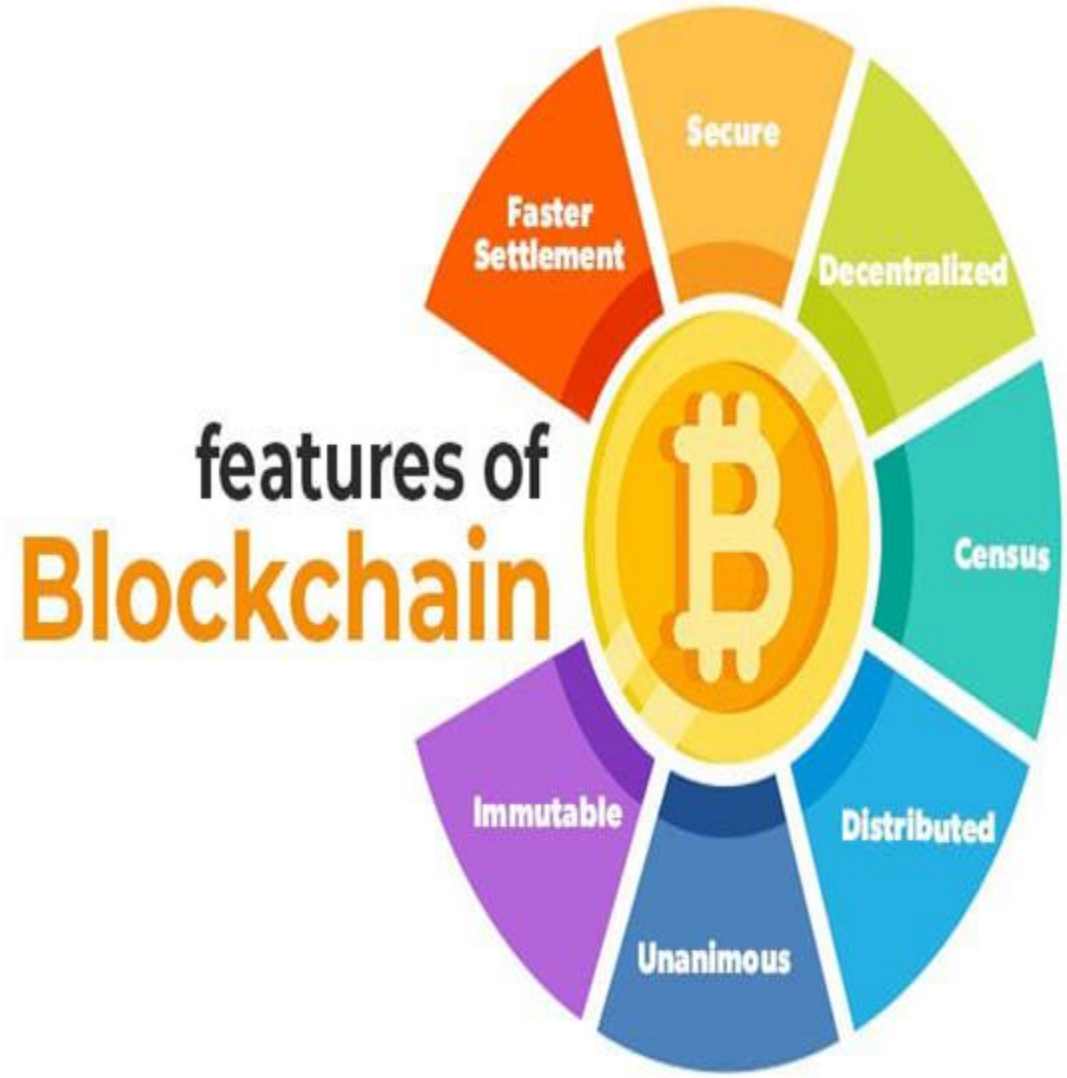
- **Distributed database:** Distribute databases like MongoDB, Apache, and Rethink DB can be used to store data. They are quick and versatile, but they are not Byzantine verified. This means any hacker can corrupt the entire information base as all the hubs of the information completely trust one another.
- **Decentralized cloud storage:** Decentralized cloud storages allow for the storage of static data where data is not stored on the company server but instead on the devices of the renters. This storage can be used online thus making them fast and efficient but they are costly too.
- **Interplanetary file system:** This is a blockchain technology that breaks up data into shards and stores them in multiple instances. It is a peer-to-peer solution where the files get downloaded only if the person needs them. Thus, this is the address-dependent storage solution.

Advantages and Disadvantages of Blockchain

FINANCE STRATEGISTS

LANGUAGES USED IN BLOCKCHAIN SECURITY

1. Solidity
2. Java
3. Python
4. C++
5. Ruby
6. Go
7. C#
8. Simplicity
9. Rholang
10. PHP



USES OF BLOCKCHAIN SECURITY

- Blockchain creates an unalterable record of transactions with end-to-end encryption to shut out fraud and unauthorized activity. Additionally, data on the blockchain is stored across a network of computers, making it nearly impossible to hack, unlike conventional systems that store one copy of the data on servers.
- In marketing, blockchain can be used to increase the security and transparency around the sharing of customer data, either between a customer and a company or between two companies. Blockchain can also be used to reduce fraud and other trust-related issues in digital ad buying.

FUTURE GENERATION IN BLOCKCHAIN SECURITY

- Blockchain will be used to verify firmware updates and patches and prevent unauthorized access or attempts to install malware.
- Smart contracts show users the potential to automate payments by using predetermined conditions and automatically reducing fraud by reducing human interference.

THANK YOU