Cyber Security in the Blockchain

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

UPU-WAPD:Philatelic Webinar December 14, 2021

Crypto & Hybrid Stamps ,What future for philately ?

Presented by: Hayet Yahyaoui

Cyber Security Analyst

yahyaoui.hayet@ansi.tn

WADP World Association for the Development of Philately

UPU UNIVERSAL POSTAL UNION

tunCERT Tunisian Computer Emergency ResponseTeam

Plan

- Intoduction to the Blockchain.
- Blockchain Cyberattacks and fraud.
- Best practices and recommendations.

What is a blockchain?

Blockchain is defined as an open ledger offers :

- Decentralization to the parties.
- Transparency.
- Immutability.
- And Security.

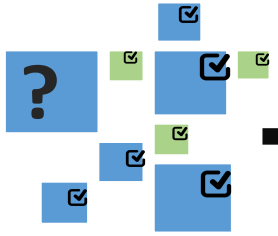
It has many features including being open, distributed, ledger, P2P, and permanent.

How Does a Blockchain Work?

1 A user requests for a transaction

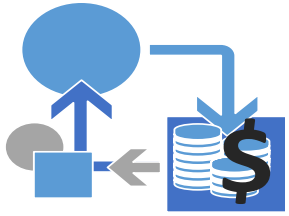
2 A block representing the transaction is created

3 The block is broadcasted To all the nodes of the network



4 All the nodes validate The block and the transaction

5 The block is added to the chaine



6 The transaction gets Verified and executed

Tokenization the Key element of a blockchain

- In the blockchain ecosystem, tokens are assets that allow information and value to be transferred, stored, and verified in an efficient and secure manner. These crypto tokens can take many forms, and can be programmed with unique characteristics that expand their use cases.
- There are four main types: Payment tokens, Utility tokens, Security tokens and the Non-fungible tokens (NFTs).

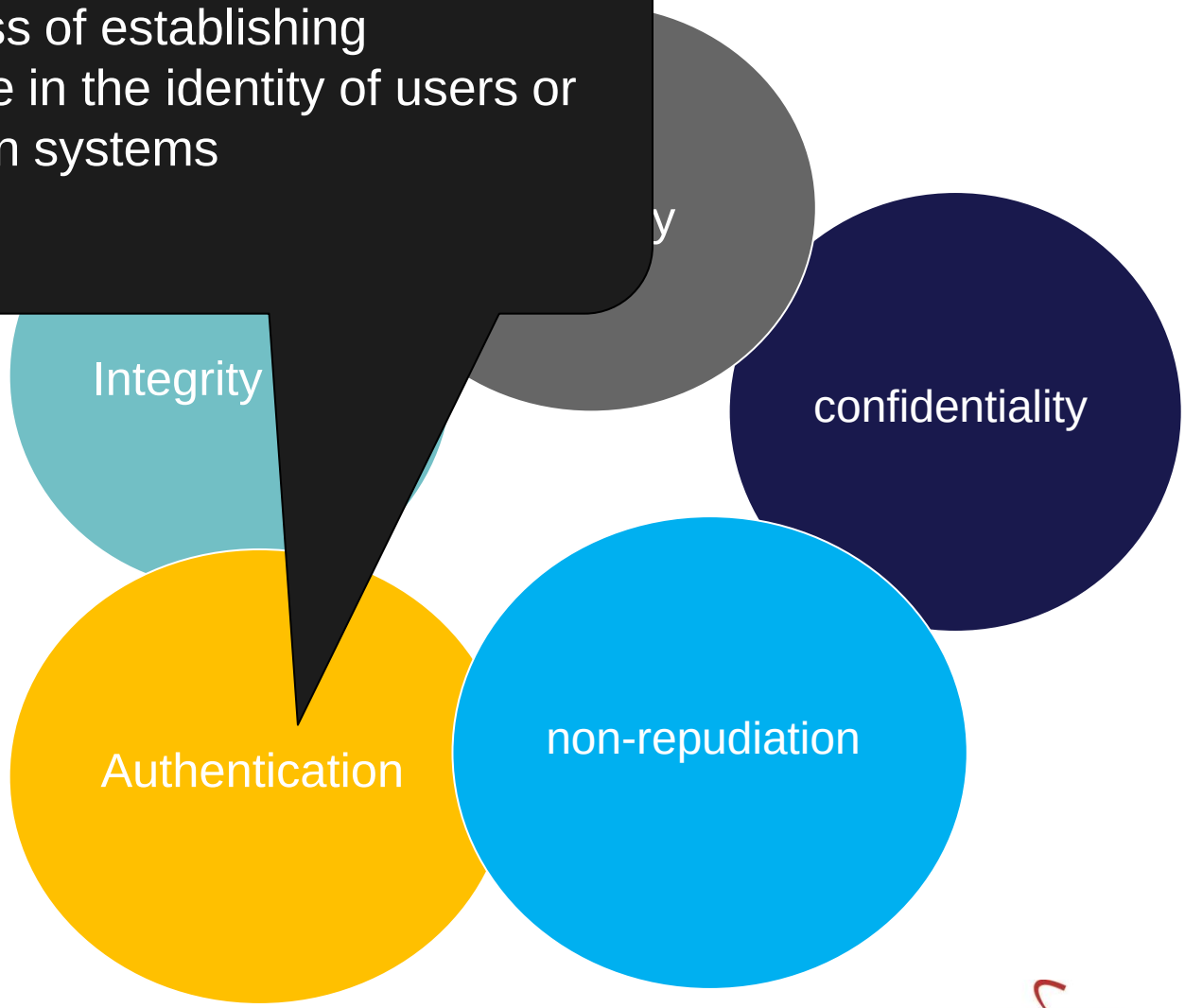
NFTs (Non-fungible tokens)

Non-fungible tokens (NFTs):

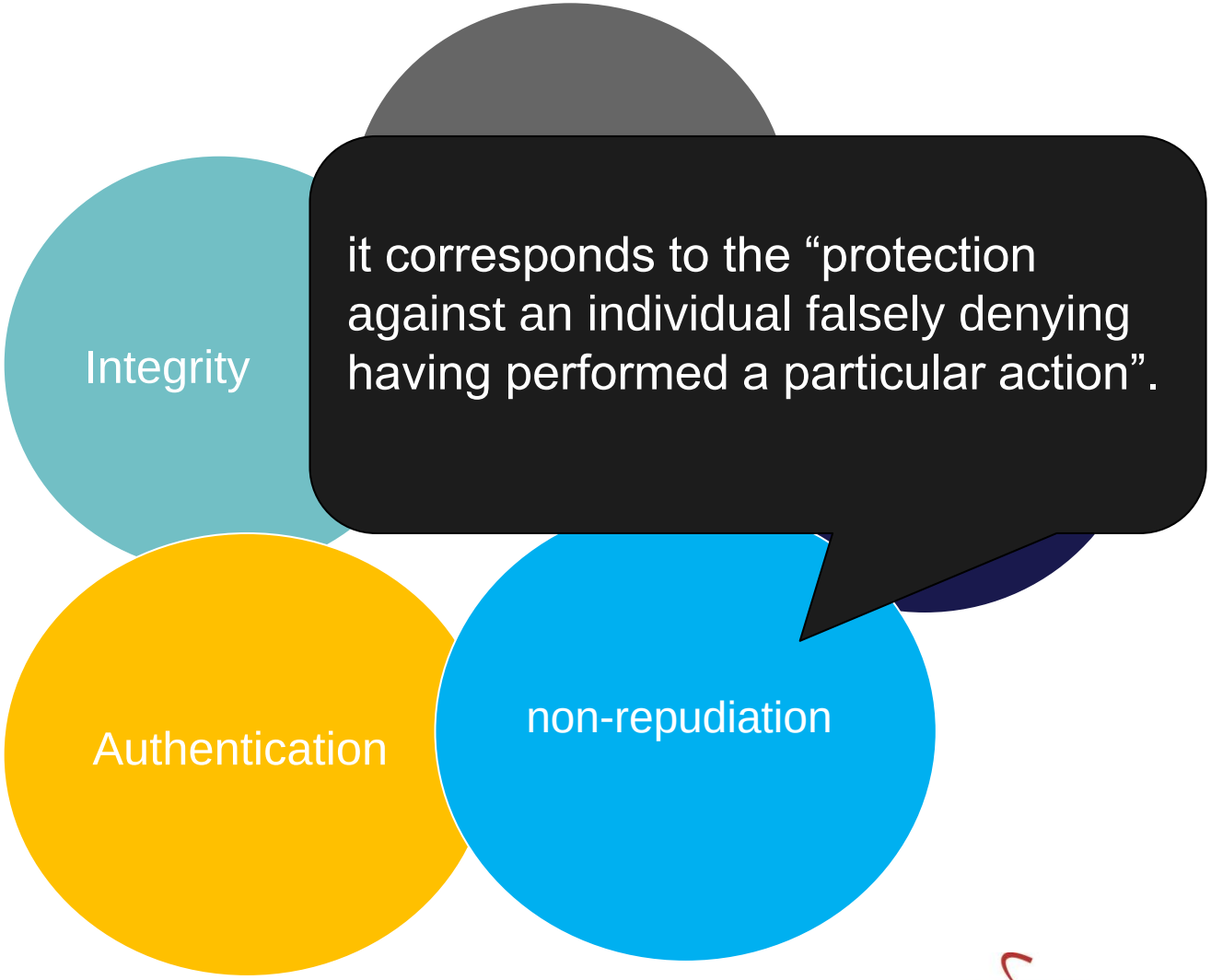
- They are blockchain-based tokens that each represent a unique asset like, piece of art, digital content, or media.
- The artwork/stamps, etc., can also become the NFT itself.
- An NFT can be thought of as an irrevocable digital certificate of ownership and authenticity for a given asset, whether digital or physical.
- Non-fungible tokens (NFTs) are designed to be **cryptographically verifiable**, **unique or scarce** and **easily transferable**.
- Example of NFTs: the NFT Stamps (STAMPSDAQ is one of the leading projects on the market that stands for exactly these NFT values.)

Cyber Security goals

the process of establishing confidence in the identity of users or information systems



Cyber Security goals



Cyber Security goals

Cyber Security goals

Cyber Security goals

Blockchain Cyberattacks and fraud

- How fraudsters attack blockchain technology ?
- Hackers and fraudsters threaten blockchains in five primary ways:
  - Botnets.
  - Phishing.
  - Routing.
  - Sybil.
  - 51% attacks.

Blockchain Cyberattacks and fraud

The five Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology:

1. User wallet attacks.
2. Transaction verification mechanism attacks.
3. Mining pool attacks.
4. Blockchain network attacks.
5. Smart contract attacks.

Blockchain Cyberattacks and fraud

1. User wallet attacks

They are concerned about the way humans interact with blockchain.

The vulnerabilities can include:

- Digital signature vulnerability.
- Hash function vulnerability.
- Mining malware.
- Vulnerability of addresses.
- Software flaws.

Blockchain Cyberattacks and fraud

Example of attack:

- Cryptocurrency mining botnets are making millions for their creators by secretly infecting various devices across the globe.
- Early this February, more than half a million computing devices were hijacked by a cryptocurrency miner botnet called Smominru, forcing the various devices to mine nearly 9,000 Monero cryptocoins without the knowledge of the devices' owners, according to technology portal ZDNet.

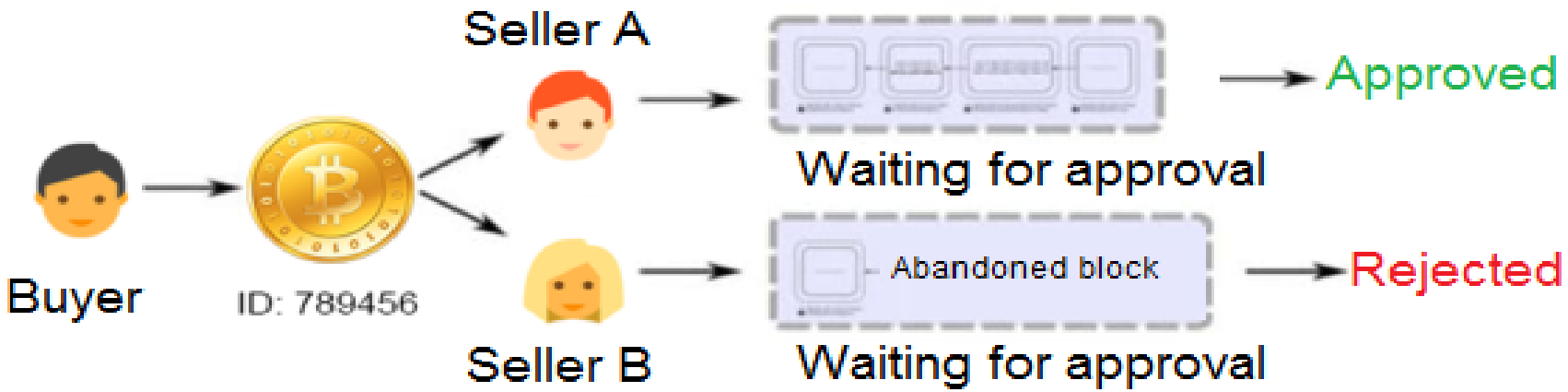
Blockchain Cyberattacks and fraud

2. Transaction verification mechanism attacks

- Blockchains confirm transactions only after all nodes in the network are in agreement. Until a block with a transaction is verified, the transaction is classified as unverified.

- However, verification takes a certain amount of time, which creates a perfect vector for cyberattacks.

Blockchain Cyberattacks and fraud

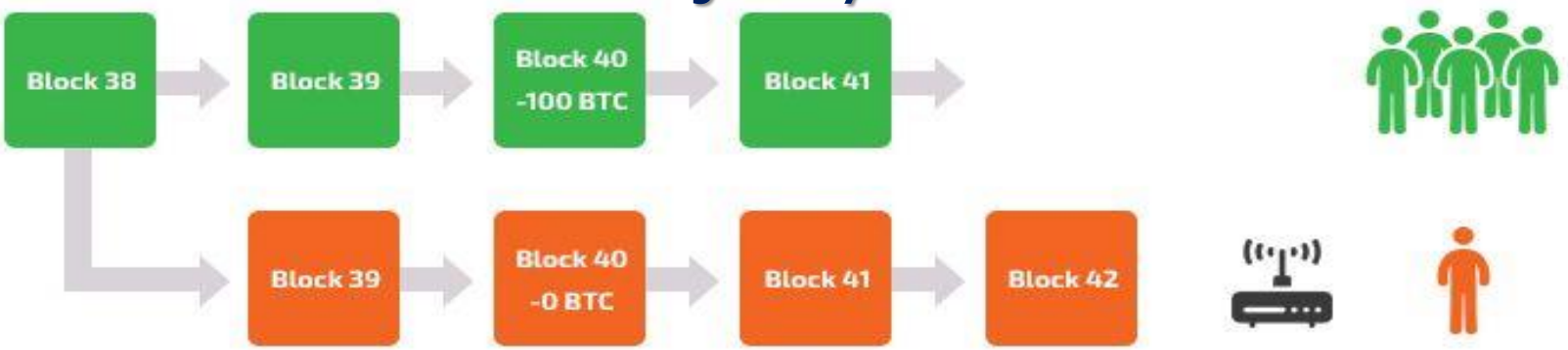


Double-spending attacks

A common blockchain attack exploiting the transaction verification mechanism. All transactions on a blockchain need to be verified by users in order to be recognized as valid, which takes time. Attackers can use this delay to their advantage and trick the system into using the same coins or tokens in more than one transaction.

Blockchain Cyberattacks and fraud

51% or majority attacks



A majority attack is possible when a hacker gets control of 51% of the network hash rate and creates an alternative fork that finally takes precedence over existing forks.

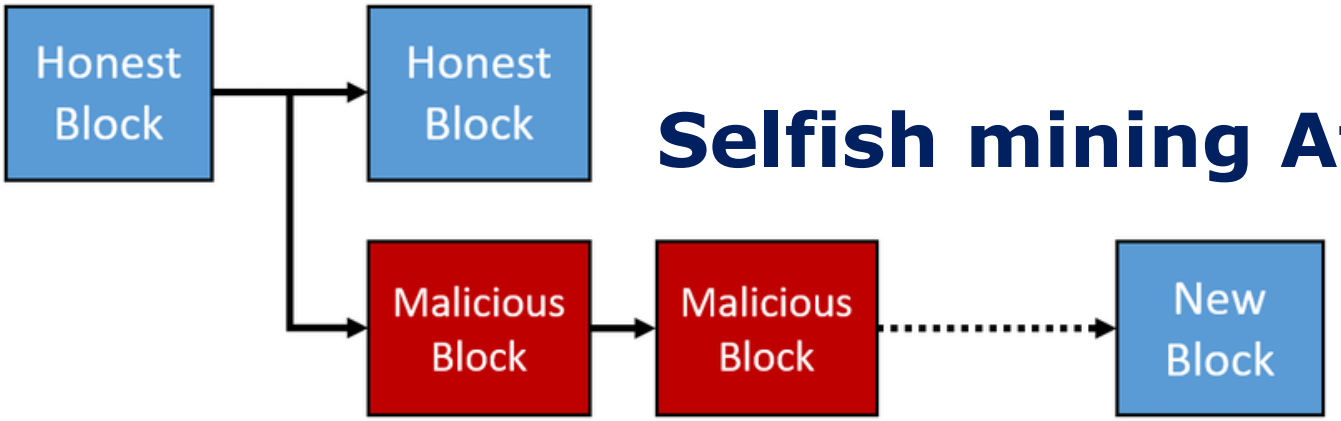
The recent 51% attack on Ethereum Classic (ETC) that happened in August 2020 resulted in approximately $5.6 million worth of the ETC cryptocurrency being double-spent.

Blockchain Cyberattacks and fraud

3. Mining pool attacks

- Mining pools use "shares" to track the activities of each miner. Attackers can apply different tactics to gain more shares, as they will receive a larger portion of the reward.

Blockchain Cyberattacks and fraud



Selfish mining Attack

Example of attack:

Selfish mining refers to the attempts of malicious miners to increase their share of the reward by not broadcasting mined blocks to the network for some time and then releasing several blocks at once, making other miners lose their blocks.

Blockchain Cyberattacks and fraud

4. Blockchain network attacks

- A blockchain network includes nodes that create and run transactions and provide other services. For instance, the Bitcoin network is formed by nodes that send and receive transactions and miners that add approved transactions to blocks.
- Cybercriminals look for network vulnerabilities and exploit them.

Blockchain Cyberattacks and fraud

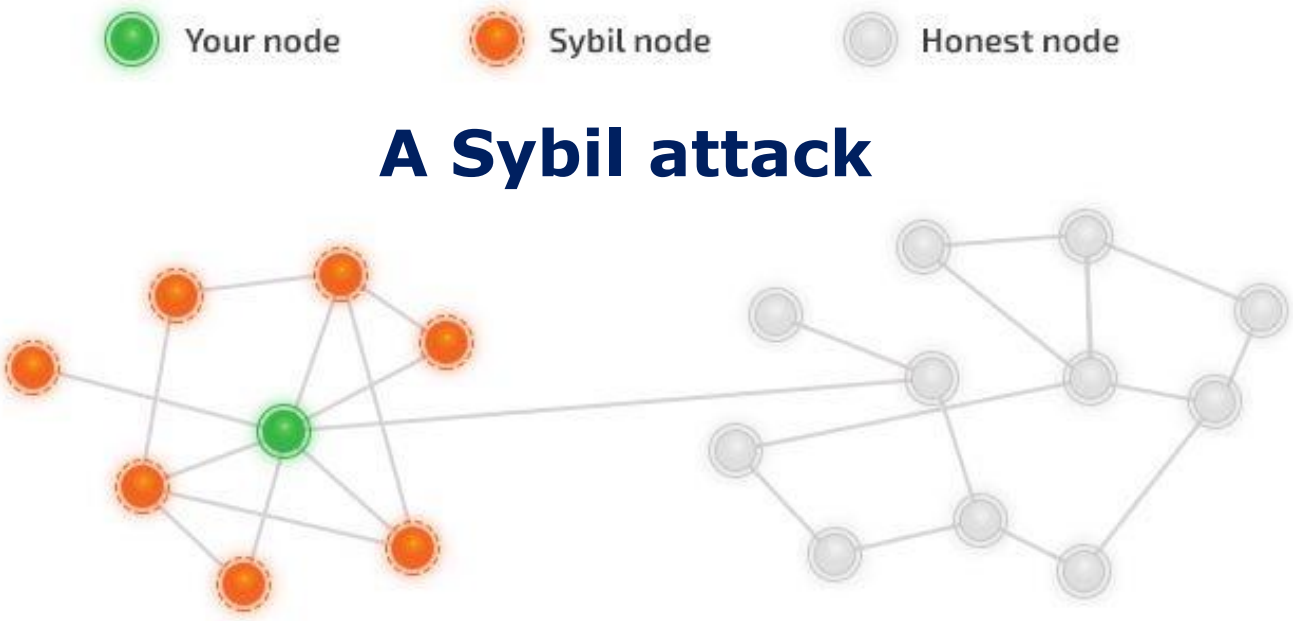
Example of attack:

- Distributed denial of service (DDoS) attacks .

They are hard to execute on a blockchain network, but they're possible.When attacking a blockchain network using DDoS, hackers intend to bring down a server by consuming all its processing resources with numerous requests. DDoS attackers aim to disconnect a network's mining pools, e-wallets, crypto exchanges, and other financial services.

- A blockchain can also be hacked with DDoS at its application layer using DDoS botnets.

Blockchain Cyberattacks and fraud



The following measures can be effective: increasing the cost of creating a new identity, requiring some type of trust for joining the network, or determining user power based on reputation.

Blockchain Cyberattacks and fraud

5. Smart contract attacks

- The main blockchain security issues associated with smart contracts relate to:
  - Bugs in source code.
  - A network's virtual machine.
  - The runtime environment for smart contracts.

Blockchain Cyberattacks and fraud

- If a smart contract has vulnerabilities in its source code, it poses a risk to parties that sign the contract.

Example of attack

Bugs discovered in an Ethereum contract cost its owners $80 million in 2016. One of the common vulnerabilities in Solidity opens up a possibility to delegate control to untrusted functions from other smart contracts, known as a reentrancy attack. During this attack, contract A calls a function from contract B that has an undefined behavior. In turn, contract B can call a function from contract A and use it for malicious purposes.

Best practices and recommendations

Best practices and recommendations

- Develop a risk model that can address all business, governance, technology and process risks.
- Evaluate the threats to the blockchain solution and create a threat model.
- Define the security controls that mitigate the risks and threats based on the following three categories:
  - Enforce security controls that are unique to blockchain.
  - Apply conventional security controls.
  - Enforce business controls for blockchain.

Best practices and recommendations

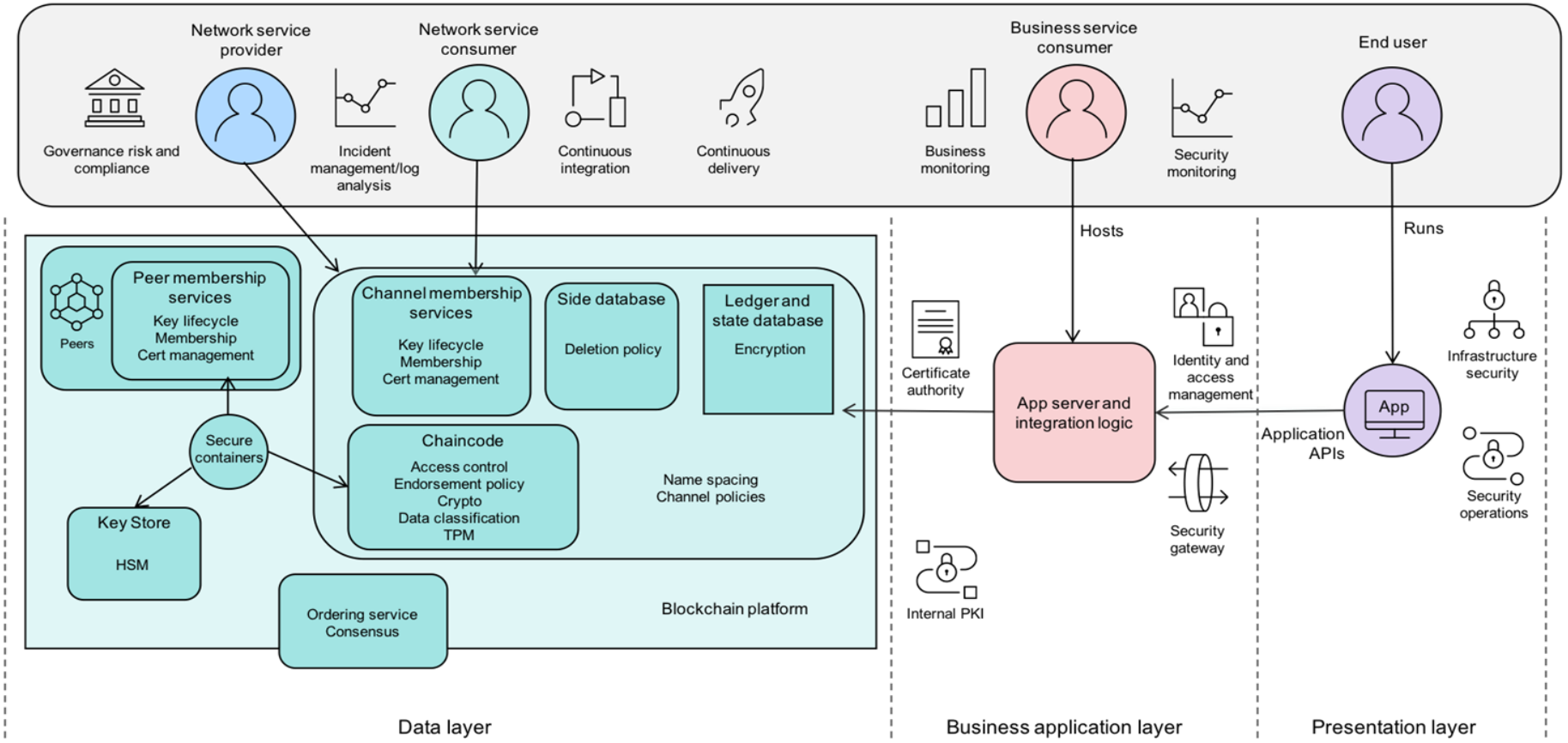
- Adopt and apply safety standards.
- Apply appropriate approval policies based on commercial contracts.
- Apply identity and access controls to access the solution and blockchain data.
- Enforce access control in smart contracts.
- Secure internal and external communication .

Best practices and recommendations

- Protect applications from vulnerabilities and protect data.
- Protect API-based transactions.
- Apply Hardware Security Modules (HSMs).
- Use a privileged access management solution (PAMs).
- Make good use of the secret store for applications and privileged access.
- Take a data classification approach to protect data / information.

Best practices and recommendations

Blockchain security reference architecture



tunCERT
Tunisian Computer Emergency ResponseTeam

References

- https://www.investopedia.com/tech/what-botnet-mining
- https://www.ibm.com/topics/blockchain-security
- https://www.investopedia.com/non-fungible-tokens-nft-5115211
- https://inblog.in/What-is-Double-Spending-How-Does-Bitcoin-handle-it-Ii1AKICQlo
- https://blog.goodaudience.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474
- https://coincentral.com/sybil-attack-blockchain
- https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors
- https://www.techgropse.com/blog/secure-blockchain-technology
- https://medium.com/geekculture/crypto-stamps-the-next-nft-hype-c9250cea1097

THANK YOU