هيئة الاتصالات وتقنية المعلومات
Communications & Information
Technology Commission

Guidelines for Blockchain Adoption

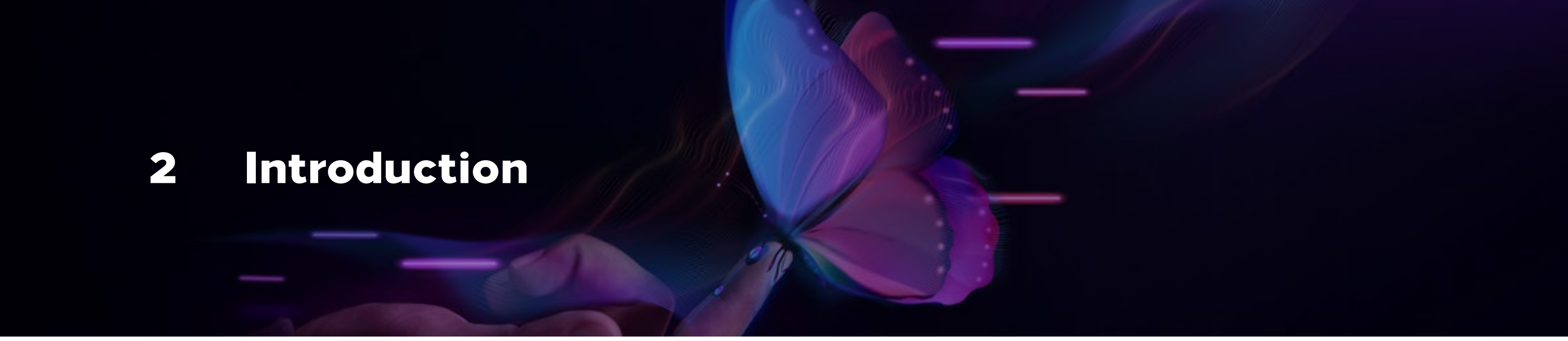
First Version
October 2022

CITC.GOV.SA

Table of Contents

1 Glossary

Asset	Anything of value that can be owned or controlled by a stakeholder.
Block	Data including hash of the previous block and zero or multiple transaction records. Each block is assigned a cryptographic hash.
Blockchain	A type of DLT in which transactions are grouped into “blocks” and each block is connected to the previous, forming a chain of blocks.
Consensus	A set of rules that nodes within a blockchain network have to follow in order to validate transactions and ensure consistent order of transactions among nodes.
Distributed Ledger Network	A Network of connected devives where each device has a copy of the ledger and smart contracts.
Distributed Ledger Technology (DLT)	Distributed Ledger Technology (DLT) refers to the technology used to enable the secure operation of a ledger that is distributed among multiple nodes. The nodes agree on and ensure consistency of ledger information using consensus.
Hash	The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.
Ledger	Transaction records.
Node / Participant	A device / device owner that participates in a DLT network by storing a copy of the ledger.
Smart Contract	A computer program that automatically executes relevant transactions when contract terms are met.
Token	A set of digital information within a Blockchain that confers rights for an asset to a particular stakeholder.
Transaction	Recording an event such as creating a new asset or transferring an asset between nodes.



2 Introduction

In accordance with the Communications and Information Technology Law, its Executive Regulations, and the organization of the Communications and Information Technology Commission (CITC), and what was stipulated in Item (Seventh) in Cabinet Resolution No. (292) dated 271441/4/ AH, the Communications and Information Technology Commission is the authority responsible for regulating the sector Communications and Information Technology in the Kingdom of Saudi Arabia (Kingdom).

Accordingly, and based on the CITC's strategy, and in the interest of CITC to enable the Blockchain market in the Kingdom, CITC has issued these guidelines to adopt best practices and executive and technical recommendations related to Blockchain technology.

2.1 Scope of Application

This document is a non-binding guideline intended to facilitate and support the adoption of Blockchain technology for:

- **Executives**

  Responsible for making decisions on the adoption of Blockchain technology including business and technical executives.

- **Solution and Software Architects**

  Responsible for making decisions on the design and development of Blockchain solutions from a technical perspective.

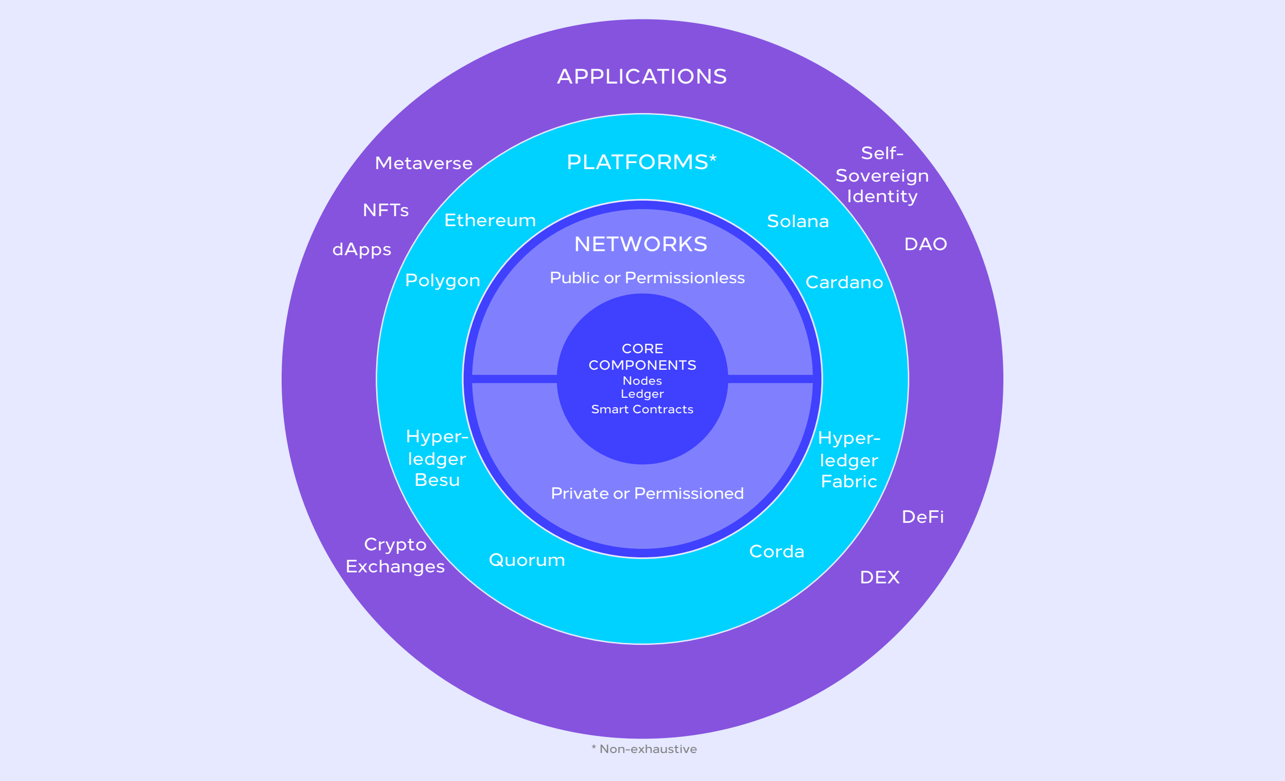
The guidelines in this docuement focused on the following areas:

- Providing general Blockchain guidance to foster adoption
- Help make informed architecture choices based on best practices
- Defining interoperability principles within one Blockchain network or between Blockchain networks
- Providing guidance for data privacy and security on Blockchain
- Introducing proper guidance for the governance of networks

2.2 A brief about Blockchain

Blockchain is one of the distributed ledger technologies that enables recording of immutable transactions in a ledger that is accessible only to members within the same network. Blockchain technology allows for building consensus and increase trust and transperancy since it can be used to access information in a secure peer-to-peer network without the need of an intermediary.

The below diagrams give an overview of the ecosystem, which contains networks, platforms and applications.



* Non-exhaustive

Figure 1: Blockchain Technology Landscape

And Figure 2: Blockchain Core Components below shows the core components of a Blockchain network, which include the connected nodes where each node contains a copy of the Blockchain ledger and smart contracts.

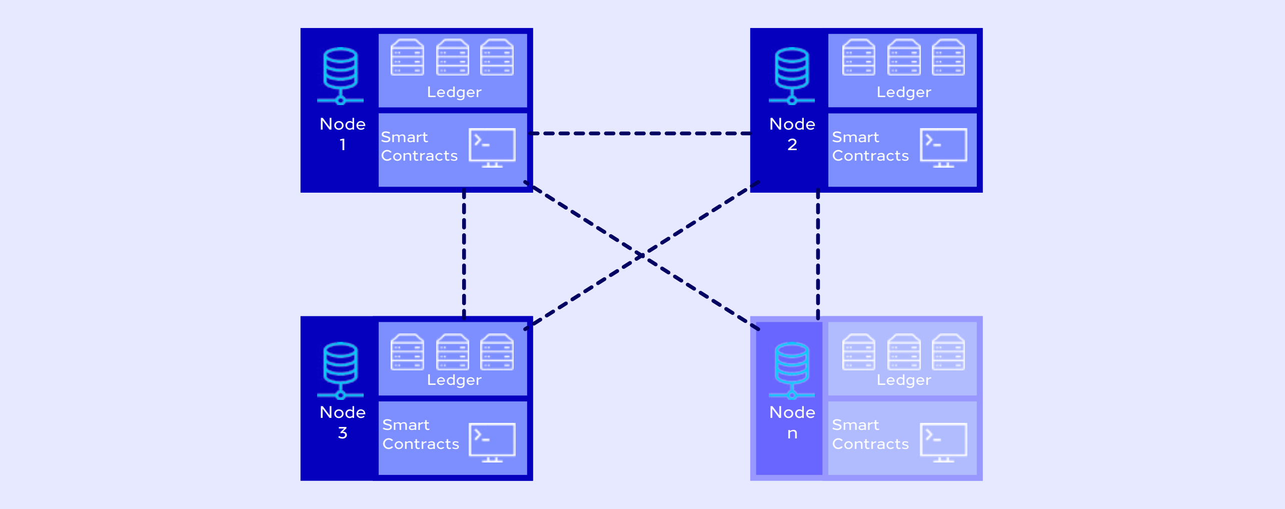


Figure 2: Blockchain Core Components – Nodes, Ledger and Smart Contracts

3 Related Laws and Regulations

Below is a list of the most related laws and regulations that may apply to Blockchain solutions with an emphasis on the need to check any updates to the mentioned documents or any newly issued documents.

	Document Title	Publisher	Scope of Application
1	Cloud Computing Regulatory Framework (CCRF)[1]	CITC	Cloud Blockchain services
2	Cybersecurity Regulatory Framework (CRF)[2]	CITC	Blockchain solutions
3	General Principle for Personal Data Protection[3]	CITC	Blockchain solutions that process personal information

[1] CCRF
https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx

[2] CRF
https://regulations.citc.gov.sa/ar/pages/published-document.aspx#/published-document

[3] General Principle for Personal Data Protection
https://www.citc.gov.sa/en/RulesandSystems/privacy/Pages/default.aspx

4 General Guidelines

This section aims to guide executives on the important decisions for adopting Blockchain.

4.1 Select the Right Blockchain Type

Choose the Blockchain type, considering the level of transparency, immutability, access level, scalability and permission management features desired

Blockchain networks can be categorised based on their accessibility and permission model into the following categories:

Public or Permissionless Blockchain Network

Public Blockchain networks are open to everyone to join the network and participate in the consensus process without requiring permission. Bitcoin and Ethereum are the most popular public Blockchain network examples.

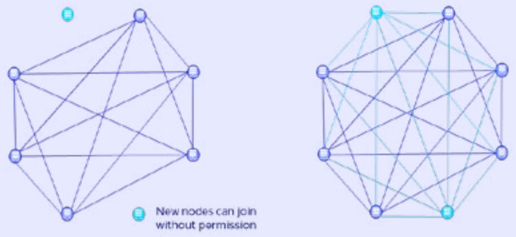


Figure 3: Public Blockchain

Private or Permissioned Blockchain Network

Private or Permissioned Blockchain networks can be owned by one or multiple entities that hold control over providing authority to new members either to only access the network or also to validate the transactions.

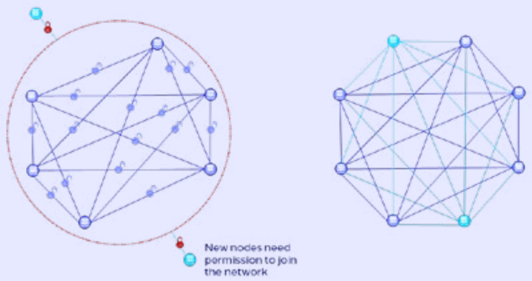


Figure 4: Private Blockchain

iven access to private blockchain networks is limited to authorised nodes, public blockchain is significantly more decentralised than private networks.Blockchain networks can be categorised based on their accessibility and permission model.

4.2 Assess the Existing Blockchain Network

Research the available networks and assess joining those networks instead of creating a new one

If there is a running network on the same planned use case that serves business requirements, then it is recommended to join the existing network instead of building a new one for the same purpose in order to have a faster time to market, including reduced efforts and financial costs.

Adoption of existing networks will also increases the number of network users and therefore makes the network more valuable and useful.

4.3 Implement Tokenisation

Tokenisation enables the representation of digital and physical assets on the Blockchain.

This guideline elaborates on suitable cases for using fungible or non-fungible tokens with examples of their standards.

Create Fungible Tokens

Adopt fungible token standards to represent assets that are not unique and could be exchanged in fractions

One example of the possible choice of fungible tokens over non-fungible tokens is inventory management, where a high number of the same products should be tracked. In this case, fungible tokens are helpful to represent the stock of a certain item and track its stock in real-time, allowing to eventually restock a certain item before stock-out. That is particularly helpful if a business partner is managing the stock for another company.

The most known standard in the fungible tokens is ERC-20[4], which serves as a standard protocol for the Ethereum Blockchain.

[4] EIP-20: Token Standard
https://eips.ethereum.org/EIPS/eip-20

Create Non-Fungible Tokens

Adopt non-fungible token standards to represent unique assets

Non-fungible tokens can be used to represent unique assets such as unique art pieces or limited edition products.

The most known standard for non-fungible tokens is ERC-721[5], which serves as a standard protocol for the Ethereum Blockchain.

[5] EIP-721: Non-Fungible Token Standard
https://eips.ethereum.org/EIPS/eip-721

5 Architecture Guidelines

This section aims to guide executives and architects regarding the architectural decisions for designing a Blockchain solution.

5.1 Select a Suitable Architecture Model for Blockchain Application

Select the more appropriate architecture for a Blockchain application according to the use case requirements, governance model and level of security or privacy required

Blockchain applications can be either decentralised or centralised like traditional web applications.

Traditional web applications are usually composed of the following:

- **Front-end** including the user interface
- **Back-end system** including business logic triggered by the user interface
- **Database,** including data transacted by the back-end and data used to execute business logic

The following diagram represents the workflow from the front-end to Blockchain through the back-end and database. It is noteworthy that the back-end system and database in such architecture are centralised and thus could represent a single point of failure for the application.

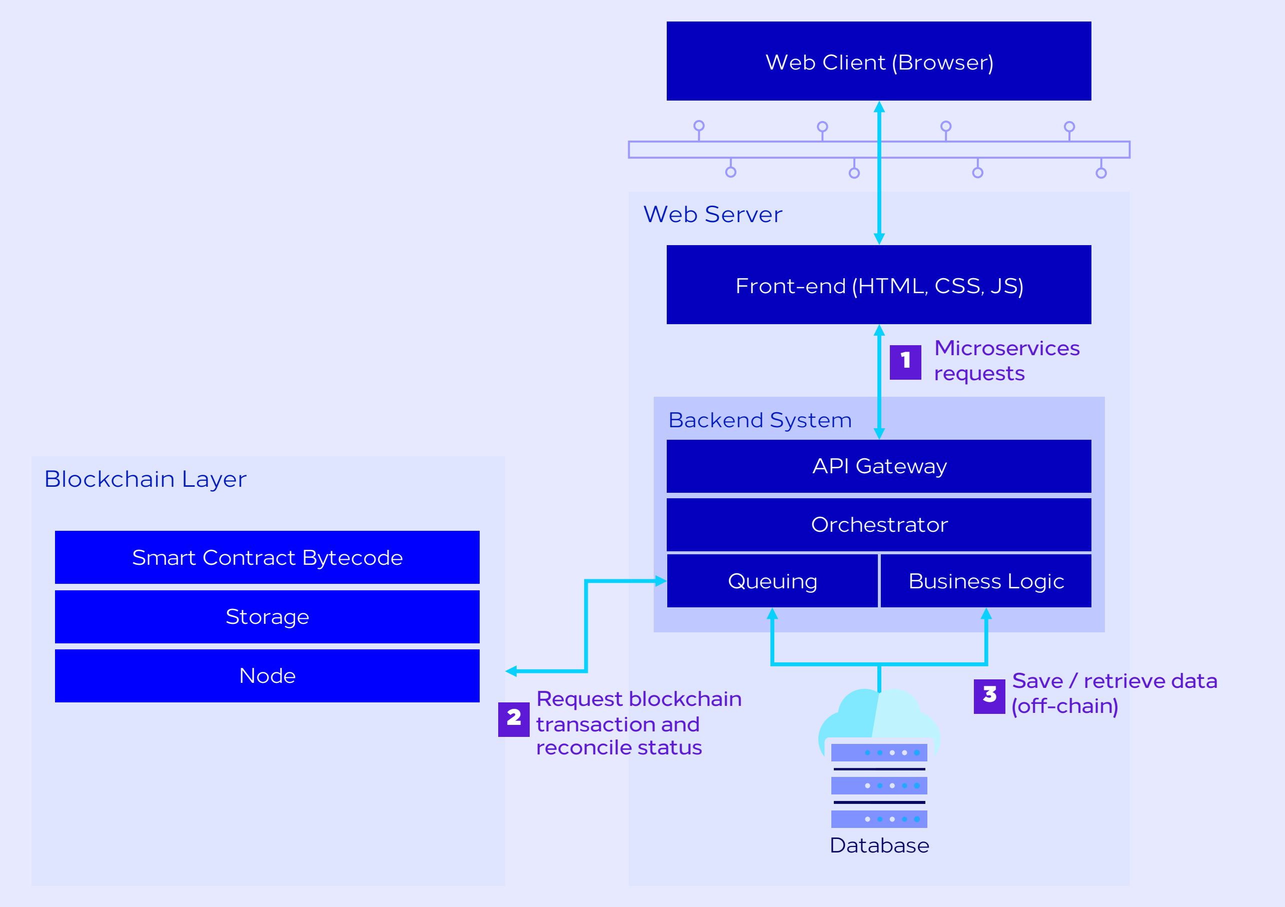


Figure 1: Blockchain Application Architecture - Centralised

While Decentralised applications (dApps) are digital applications or programs that live and execute on a Blockchain or peer-to-peer network instead of a single computer. Anf dApps are composed of the following:

- **Front-end** including the user interface
- **Back-end** system including smart contracts

The following diagram represents the workflow in dApps where the user interface is querying the Blockchain directly without any centralised back-end system in the middle, making the application more fault-tolerant. Thus, it is recommended to use dApps when user experience and decentralization are prioritized.

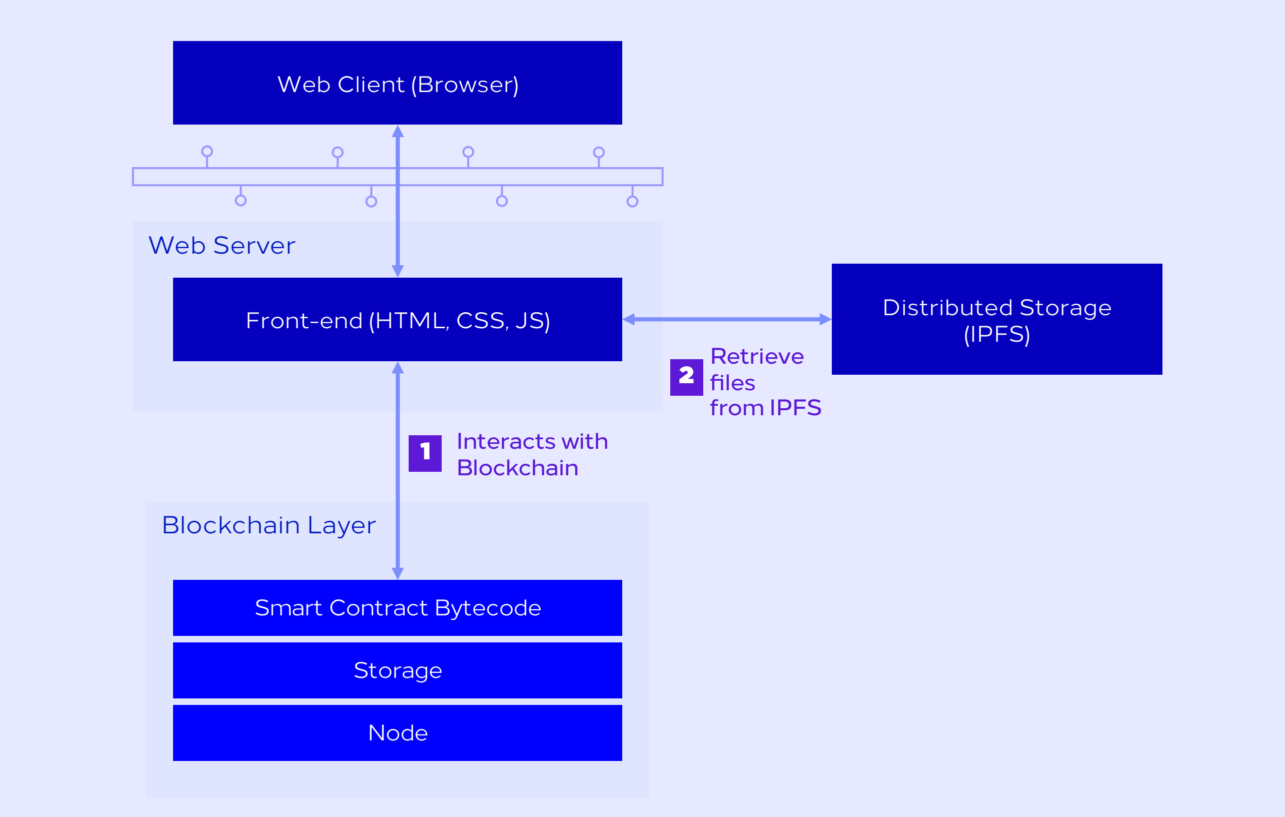

Web Client (Browser)
Web Server
Front-end (HTML, CSS, JS)
Distributed Storage (IPFS)
2 Retrieve files from IPFS
1 Interacts with Blockchain
Blockchain Layer
Smart Contract Bytecode
Storage
Node

Figure 2: Blockchain Application Architecture - Decentralised

5.2 Manage Performance through Enterprise Components

Decouple the business logic from the Blockchain nodes in Blockchain applications

Blockchain platforms have a maximum throughput – transactions per second. The throughput is affected by the block size and the consensus algorithm used on the network. For example, the throughput when using PoS is higher than the PoW.

The architecture of any application built on those platforms also affects productivity. When the business logic is separated from the nodes, productivity will be positively impacted. For example, in centralized web applications, it is recommended to adopt queueueing mechanisms to sort and manage transactions in order to avoid overloading nodes too many requests at once, which may cause network downtime.

The following diagram illustrates the integration of private blockchain networks with traditional application components:

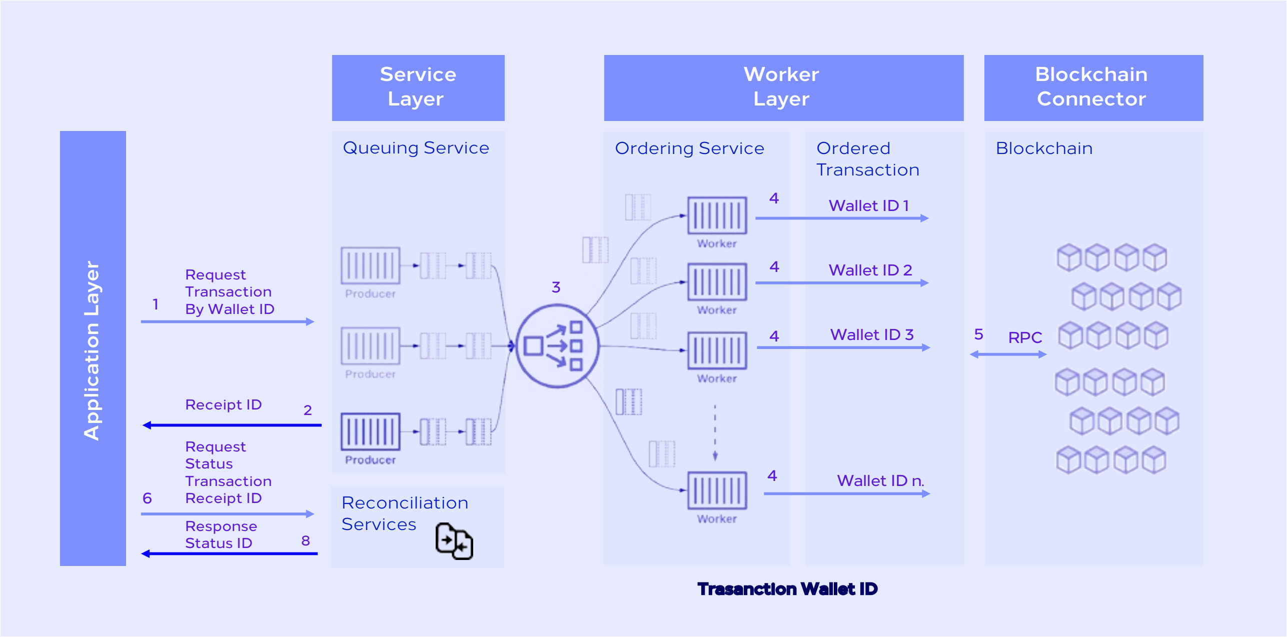


Figure 3: Transaction submission flow through the use of queuing service

Figure 9 highlights the use of a **Queuing Service** that receives requests from the application, **Ordering Service** that orders the received requests and then sends them into the Blockchain on a wallet-basis, with nonce properly managed to avoid failures. The reconciliation is then done by the **Queuing Service,** which returns for each receipt ID the status of the transaction (In pending, done) to the client. For instance, when using the above flow in a public Blockchain like Ethereum to send multiple transactions from the same wallet, data loss or for latencies to get transaction confirmation will be limited.

6 Interoperability Guidelines

This section aims to guide executives and architects with best practices to increase interoperability of Blockchain solution components and multi-chain and multi-cloud compatibility.

6.1 Use OpenSource Technologies

Include open-source technologies into solution architecture, if applicable

Adopting open-source components is critical for developing Blockchain applications that follow the leading standards and, at the same time, can be evolved without expensive maintenance and evolution costs. The use of open source components also facilitates access to blockchain applications and promotes reusage. This applies to all parts of blockchain applications, from the blockchain platform to the front-end.

6.2 Build Applications for Multi-Chain Compatibility

Design Blockchain applications to be Blockchain-agnostic to enable multi-chain compatibility

Blockchain has changed the paradigm of applications, removing all the business logic from back-end systems and promoting direct integration of the front-end with the Blockchain. Therefore, it is essential to design software applications in a way that they can follow the evolution of technology by enabling migrating the application between Blockchains or integrating new Blockchains to the application without the need for severe refactoring.

And if the used Blockchain platform does not provide multi-chain compatibility, it is recommended to build an intermediary back-end system to enable that compatibility. It is recommended also to build a common data model to facilitate the compatibility between Blockchains. (For details, refer to guideline 9.3).

Another possible way of handling multi-chain compatibility is using solutions that enable data interoperability across Blockchain. However, the following are important considerations before using such solutions:

- Ensure reliability and security of Blockchains before integrating, as bridging assets between networks could lead to data leakage in the process.[6]

[6] Cross Chain Bridges Security https://thedefiant.io/vitalik-eth-cross-chain-bridges-security/

Assess appropriately and thoroughly to prevent issues that could arise from the reliability as such solutions are still in development phases.

6.3 Design Applications for Multi-Cloud Compatibility

Design Blockchain applications to be cloud-agnostic

Using microservices architecture and containers facilitates multi-cloud compatibility, because containers support the fast deployment of applications between different cloud service providers. Containers also can be used to isolated application layers in order to achieve resource efficiency, simplified deployment, and faster boot times wherever possible.

Multi-cloud compatibility can be also achieved also through open-source cloud-agnostic libraries and components. (For details, refer to guideline 6.1).

7 Data Privacy Guidelines

This section aims to guide architects with best practices to maintain data privacy in Blockchain solutions.

7.1 Store Data On-Chain or Off-Chain Based on Privacy Requirements

When selecting storage alternatives, consider the size and sensitivity of the data

It is recommended to avoid storing the following data on-chain:

- Large-size data; as the Blockchain storage in smart contracts could be limited
- Sensitive data; as it might require deletion due to the immutable nature of the ledger

However, it is essential to put security measures for off-chain data to ensure restrictions on access and visibility of the data: those measures depend on the storage choice.

Data should be stored on-chain when there is a need to keep detailed track of the data, with the opportunity to retrieve it from the network. In addition, on-chain storing simplifies the system by reducing the infrastructure needs.

Examples of off-chain data storage can relate to sensitive documents containing patient data. On-chain data storage can be used to record information about the production steps in a manufacturing company's value chain.

7.2 Connect Off-Chain Data: Oracles

Use decentralised oracles to connect off-chain data in a reliable and decentralised way

Oracles are a middleware between Blockchain networks and real-world external data (i.e., weather data). Off-chain oracles query APIs and periodically publish response data as transactions on the Blockchain, making the data reliable. [7] For example, oracles can be used to register on-chain updates of a product's price to automate purchase via a smart contract when the price reaches a specific threshold.

[7] Oracles, Ethereum
https://ethereum.org/en/developers/docs/oracles/

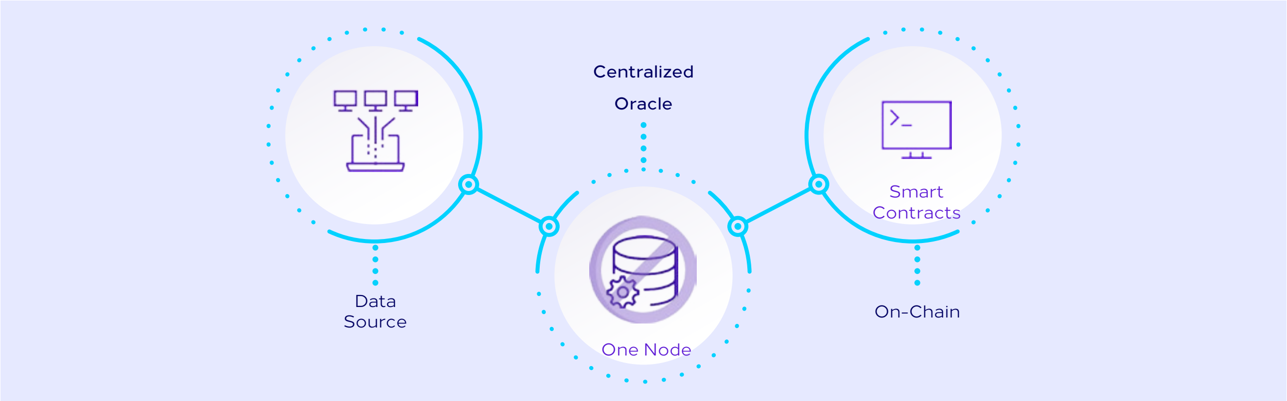


Figure 4: Centralised Oracle

Figure 7 above shows how centralised oracles works. However, the main challange with centralized oracles relates to security. If the data source is hacked, the data security is at risk. Therefore, it is recommended to use decentralised oracles that draw data from multiple data sources. Thus, using decentralised oracles because it is less exposed to such security risk.

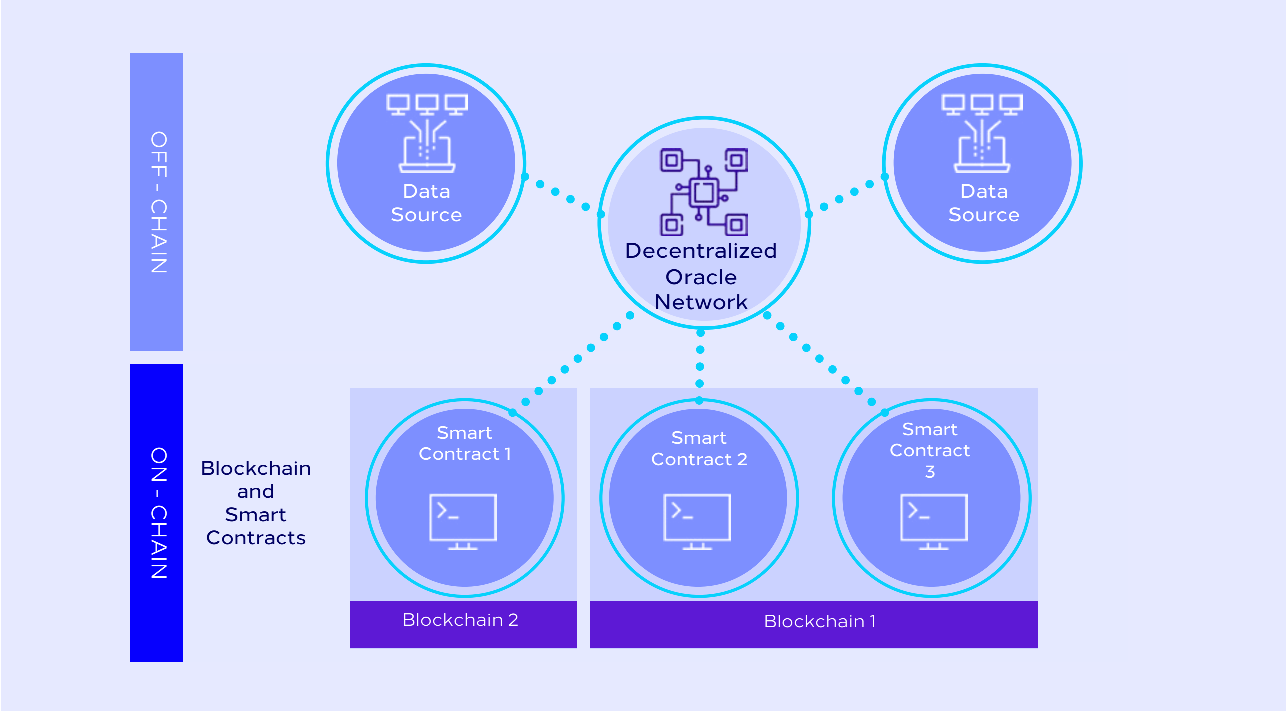


Figure 5: Decentralised Oracles

7.2 Use Distributed Storage

Use distributed storage when there is a need for immutability in storing files or information and when the data needs to be distributed among multiple network peers

When storing data off-chain, distributed storage is one of the suitable options to store data such as proof receipts, reference notarised objects or a large quantity of data through IoT for bypassing Blockchain challanges of scalability and high transaction costs if storing data on-chain.

One example of distributed storage is IPFS, which is a protocol for storing and sharing content data among users in a peer-to-peer network.

7.3 Manage Data Confidentiality on the Blockchain

Use secure and reliable hashing algorithms

Data encryption by hashing algorithms is a way of maintaining data integrity and confidentiality in the blockchain, by storing data off-chain (e.g., in distributed storage), while hash of that data is only stored on-chain.

- When hashing data, it is recommended to use algorithms that have the following features:
- Being an industry-standard trusted by leading public-sector and technology agencies.

  Wide adoption in Blockchain solutions.
- Advantage of recognisability as any change in the input will result in a completely different output.

SHA256 is an example of such algorithms. Other than SHA256, keccak256 is getting traction on Blockchain as it is the built-in hashing algorithm for Ethereum, while SHA3 is starting to be considered the new SHA256. However, it is important to review and evaluate encryption algorithms to ensure its efficiency and avoid using broken algorithms that are no longer effective.

There are also other ways to keep data confidentiality, such as encrypting transactions with zero-knowledge proof (ZKP) which enables one party (the validator) to confirm the correctness of specific information to another party (the auditor) without disclosing that information.

8 Security Guidelines

This section aims to guide architects with best practices to increase Blockchain security.

8.1 Size the Blockchain Network Appropriately

Appropriately size the number of nodes of the network and implement appropriate high-availability strategies

Depending on the consensus algorithm, there will be a need to ensure the availability of a certain number of active nodes in proportion to the total number of nodes in the network.

For example, for Byzantine Fault Tolerance algorithms, the number of active nodes should be greater than 23/ of the total number of nodes of the network to execute the consensus algorithm properly.

8.2 Identify Blockchain Users

Leverage user wallets to ensure identification, authenticity and transaction data integrity

Wallets allow users to submit transactions on the blockchain (i.e. trade cryptocurrencies and tokens) by signing those transactions in the wallet. Digital signatures, which are used to encrypt transactions, are computational schemes divided into two parts: the algorithm for creating the signature, which utilises a private key to sign the message, and an algorithm for verifying the signature, which uses the public key. Private keys are in the only control of the individuals and can be thought of as a password. In contrast, public keys work as a public address and can be tied up to decentralised identity and used to be identified by service providers.

The following diagram represents the relation between Private Key, Public Key and Wallet Address.

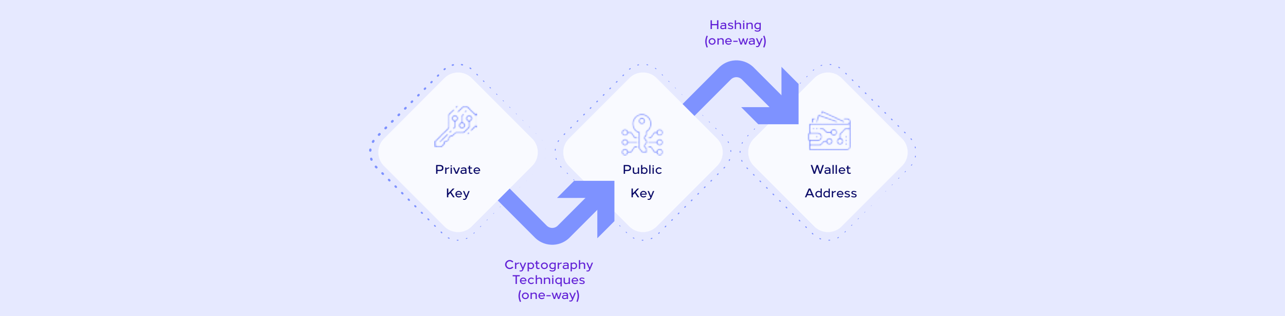


Figure 6: Use of cryptography and hashing for wallet address

If users sign their messages through their private keys, they can rightfully attest and prove their identity without revealing their private keys.

8.3 Review Blockchain Smart Contracts

Execute smart contract reviews as part of the Blockchain development lifecycles

Through the ongoing development in Blockchain technology, new bugs and security risks are expected to be discovered. Thus, it is essential to be up to date with the best security practices in smart contract development.

Following are some of the recommended practices to minimise the security risks of the smart contracts: [8]

- Ensure proper testing before deploying in a production environment.
- Assure error and vulnerability handling.
- Minimise (or, if possible, avoid) external calls as they might introduce a potential threat.
- Prioritise clarity and simplicity of smart contracts to decrease the possibility of errors.

[8] Ethereum Smart Contract Best Practices
https://consensys.github.io/smart-contract-best-practices/development-recommendations/

9 Governance Guidelines

Blockchain networks can be owned by one or multiple government and private organisations. Hence multiple owners can participate in how the solution is designed and operated. Thus, it is crucial to have clear governance that defines an allocation of power, risks and responsibilities among network participants.

This section aims to provide executives with the governance considerations to maximise the benefit of blockchain solutions.

9.1 Network Governance

Create a governance framework and, if possible, automatically enforce compliance to the framework

Governance frameworks are the bridge between technical implementations and real-world business, legal, and social requirements. Governance frameworks are the set of business, legal, and technical rules for how a network will be used to achieve its goal. The network owners should define, agree on and document a governance framework that includes the following, without limitation:

- Procedure for decision making and dispute resolution.
- Roles and responsibilities of network members, including the responsibility of assuring adherence to the governance framework among members.
- Policies and rules for joining, disjoining or interacting with the blockchain network.
- Funding and revenue generation model (if any).
- Rules for Intellectual Property access and use.
- Applicable standards and regulations.
- Data Governance. More details in guideline [9.2 Data Governance].
- Audit Governance. More details in guideline [9.3 Audit Governance].

However, as network owners grow, the governance framework should be reevaluated.

It is also recommended to create a testing environment or pilot use case to test compliance of the blockchain solution against the governance framework.

The diagram below is a high-level view of how organisations can test compliance with governance framework rules. The Governance off-chain verifies the compliance of governance framework rules manually or through external systems. However, rules can be shared and automated used on-chain Governance exploiting the capabilities of smart contracts.

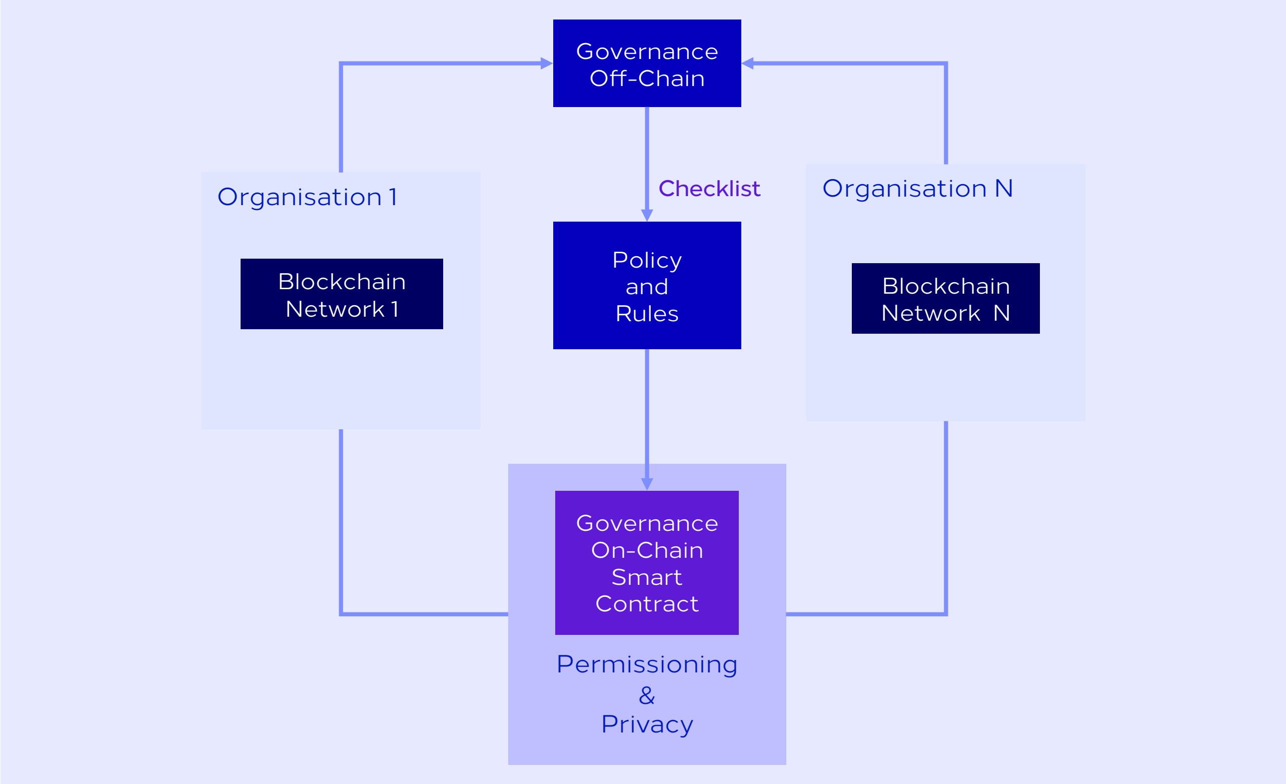


Figure 7: Distributed governance system as a potential governance model

9.2 Audit Governance

Define audit process and responsibility at the level of a Blockchain network as part of the general network governance framework

The governance framework should define how the audit process will be conducted. On the other hand, Blockchain can be used specifically for the auditing process due to its immutability feature. Further, blockchain smart contracts can be used to automate the audit process with real-time trusted results. The automation of the auditing process will increase efficiency by eliminating the need to wait to execute a manual audit process.

The governance framework for each blockchain network should also clearly define who is responsible for auditing, be it one or multiple organisations. The auditing responsibility is to ensure compliance of the blockchain network against governance framework rules, including the related standards and regulations.

9.3 Data Governance

Create a data governance framework as part of the general network governance framework

Blockchain data can be exchanged with multiple applications. Thus, a data governance framework should be created to identify policies and rules for sourcing, storing and using data.

The data governance frameworks ensure data privacy, integrity and security. The framework also ensures compliance against the enclosing governance framework, including applicable regulations.

It is also recommended to define a common data model as part of the data governance frameworks to facilitate integration with the blockchain network and maximise interoperability.

The data governance auditor that controls data usage should be separated from the data producer to assure data autonomy and fair regulation.

Governance should obligate data owners to comply with the governance framework. And if data is attributed to an IoT device or AI model rather than the organisation's database, the owner is the organisation managing the node which communicates with such device or model.

CITC

هيئة الاتصالات وتقنية المعلومات
Communications & Information
Technology Commission