NATIONAL VIRTUAL ASSETS EDUCATION MANUAL

National Virtual Assets Literacy Initiative (NaVALI)

Intermediate Knowledge in Virtual Assets

NATIONAL VIRTUAL ASSETS
LITERACY INITIATIVE (NaVALI)

Empowering Ghana for the Digital Future

By
Joseph Antwi Baafi (Ph.D), Eric Effah Sarkodie (Ph.D),
Pearl Syream Kumah (Ph.D)

Manual Title
National Virtual Assets Education Manual

Programme Name
National Virtual Assets Literacy Initiative

Intermediate Knowledge in Virtual Assets

Disclaimer

This manual is provided for education and public awareness only. The purpose is to help people understand digital money, virtual assets, related risks, and safety practices in a clear and neutral way. This manual is not meant to encourage, promote, advertise, or persuade anyone to use virtual assets or any digital money platforms. It does not give financial advice, investment advice, or instructions to make profit. Examples, stories, and scenarios used in this manual are for learning purposes only. They are not recommendations to take action or to use any specific application, service, or product. Users are responsible for their own decisions. Anyone choosing to use digital money or virtual assets should do so carefully, follow the law, and seek guidance from trusted and qualified sources where necessary. Regulations, rules, and platforms may change over time. Readers are encouraged to rely on official information from recognized authorities and service providers. There will not be any statutory compensation by the Bank of Ghana or the Securities and Exchange Commission in case of any loss. Some Sentences and images used were generated with the help of Artificial Intelligence (AI).

By

Joseph Antwi Baafi (Ph.D), Eric Effah Sarkodie (Ph.D),
Pearl Seyam Kumah (Ph.D)

Printed in Ghana

Main Authors

Joseph Antwi Baafi (Ph.D)[1], Eric Effah Sarkodie (Ph.D)[1], Pearl Seyram Kumah (Ph.D)[2]

[1]Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development, Faculty of Business Education, Department of Economics
[2]Lead, Virtual Assets Regulation, Bank of Ghana

Contributors

Prof. Nii Narku Quaynor, Ghana Dot Com
Del Titus Bawuah, Web 3 Africa Group
Frank Sekyere Tawiah, CFA

Cover Design by: Evans Oppong

ISBN: 978-9988-41-655-3

First Edition: March 2026

Publishers: Bank of Ghana
The Bank Square
42 Castle Road
Ridge, Accra
P. O. Box GP 2674, Accra – Ghana

Dedication

This manual is dedicated to the Government of Ghana.

Acknowledgement

We express sincere appreciation to the Bank of Ghana Virtual Asset Team for their guidance, technical input, and steady support during the preparation of this manual. We are grateful to Elhanan Owureku Asare, Kwadwo Darko Botwe, Tahiru Alhassan, Caleb Akuffo Dampare, Esther Abbey, Sophia Amo-Gotfried, and Reginald Isaac Quaynor for their time, insights, and commitment to strengthening the quality and relevance of the material.

We also acknowledge the valuable contributions of the Securities and Exchange Commission Virtual Asset Team. Special thanks go to Thompson Mensah, Foster Nani, Richard Dusi, McNamara Peter-Brown, and Emmanuel Darko for their feedback, professional perspectives, and support, which enhanced the clarity and practical focus of the manual.

This manual has significantly benefited from the collective experience and dedication of all those mentioned, and their contributions are deeply appreciated.

TABLE OF CONTENTS

Preface

This manual was prepared as part of a national effort to improve understanding of virtual assets and related digital financial tools in Ghana. Rapid technological change continues to affect how value is stored, transferred, and protected. These changes influence households, businesses, public institutions, and the wider financial system. Precise and accurate knowledge has therefore become essential for safety, trust, and informed decision-making. The National Virtual Assets Literacy Initiative addresses this need by presenting key ideas in a structured, accessible format. The manual explains core concepts, operational processes, risks, and regulatory considerations associated with virtual assets. The content is educational and focuses on awareness, protection, and responsible engagement rather than on promotion or advocacy.

This book is designed for a broad audience, including professionals, regulators, educators, and members of the public at different education levels. Technical language is kept simple and supported by illustrations, examples, and practical scenarios drawn from everyday experience. Repetition of safety messages is intentional, since protection against loss, fraud, and misuse remains a central priority.

Particular attention is given to the Ghanaian context. Legal and institutional roles are explained with reference to national frameworks and supervisory mandates. This approach supports consistent interpretation and helps readers know where to seek guidance, verification, or support when questions arise.

The authors acknowledge the Bank of Ghana and the Securities and Exchange Commission's leadership in commissioning this work and their commitment to public education and consumer protection. The manual reflects collaboration with key stakeholders who share a common goal of strengthening digital financial awareness while safeguarding the public interest.

We hope this manual serves as a practical reference for training, discussion, and ongoing learning. By enhancing understanding and promoting careful habits, the book seeks to reduce harm, support informed judgment, and cultivate a more resilient financial environment as Ghana continues to adopt digital innovation.

Foreword

This manual forms part of a nationwide public education effort to guide all communities through the ongoing changes in how money is stored, sent, and received. Phones and simple digital tools are now part of daily life for many people. These changes bring convenience and wider access, but they also introduce new risks, confusion, and opportunities for abuse. This programme exists to ensure people understand these changes in a precise, careful, and practical way, without pressure to adopt any digital system.

The primary audience for this manual relies mainly on spoken explanation, pictures, and practical demonstrations. Many participants have limited reading ability, and some are using digital tools for the first time. This group faces greater exposure to scams, false promises, impersonation, and misleading information, especially in environments where digital money and virtual asset services are discussed without proper guidance. This manual is intentionally designed to reduce those risks by using simple language, repeated safety messages, and everyday examples drawn from real life.

Strong emphasis is placed on protection and caution. The training prioritises learning how to keep money safe, protect phones and PINs, recognise suspicious behaviour, and pause and seek advice before taking action. Participants are guided to question offers of quick profit, avoid strangers who ask for personal details, and rely on trusted people and official channels when unsure. The goal is not to build confidence in technology itself, but to construct careful habits and awareness that reduce harm.

This manual reflects a firm commitment to inclusion within the national education effort. No one is excluded due to literacy level, age, location, or background. Through pictures, storytelling, demonstrations, repetition, and group discussion, the programme supports practical

understanding and shared learning. The overall aim is to strengthen awareness, reduce losses, and provide clear guidance on where to seek help, especially for those most vulnerable to digital and financial harm.

Johnson Pandit Asiamah (PhD)
Governor, Bank of Ghana.

Introductory Remarks

This National Virtual Asset Literacy Initiative (NaVALI) training material has been co-developed by the Bank of Ghana and the Securities and Exchange Commission and carefully selected knowledge partners to support the effective implementation of the NaVALI initiative.

The manual is intended for financial regulators, law enforcement, and other relevant state institutions; financial institutions (FIs); designated non-financial businesses and professions (DNFBPs); and consumers of financial services in Ghana. By enhancing technical knowledge and practical competencies, institutional capacity and general risk awareness, the initiative contributes to evidence-based policymaking, adequate supervision, and the responsible adoption of innovation in line with Ghana's legal and regulatory architecture.

I commend the Bank of Ghana, the Securities and Exchange Commission, the Ministry of Finance, and all knowledge partners for their contributions in developing this manual. I encourage all participants to engage fully with the training and awareness sessions and apply their insights in their respective endeavours. The strength and resilience of Ghana's financial system in the digital age will depend on our collective commitment to innovation that is well-governed, risk-aware, and firmly anchored in public interest. This training marks an important milestone in positioning Ghana as a trusted and forward-looking hub for digital finance in Africa.

James Kwame Awedzi (PhD)
Director-General
Securities and Exchange Commission

How to Use This Manual

This manual is designed to guide learners through the basic concepts of digital money and virtual assets in a clear, simple way. It is suitable for individuals at all levels of education.

i. *Follow the order of sections*

The manual is arranged in a logical sequence. Users should begin with the first section and proceed step by step, as each section builds on earlier ideas.

ii. *Focus on examples and illustrations*

Examples and short stories are included to explain how digital money and/or virtual assets work in everyday situations. Readers should relate these examples to their own daily activities.

iii. *Encourage discussion and clarification*

In group settings, facilitators should encourage discussion after each section. Learners should be encouraged to ask questions whenever something is not understood.

iv. *Apply learning through practice*

Practical demonstrations and role-play activities should be carried out using small amounts of money. This supports understanding and reduces the risk of errors.

v. *Emphasise safety guidance*

Safety instructions are provided throughout the manual. These should be highlighted and repeated, as they are essential for protecting users and their funds.

vi. *Use scenarios for assessment*

Scenario-based questions are included to assess understanding. Facilitators should use these to confirm learning before moving to the next section.

vii. *Refer to support and reporting information*

The manual includes guidance on where to seek help and how to report problems. Learners should be made aware of these channels and encouraged to use them when necessary.

This manual should be used as a reference during training sessions and as a guide for safe day-to-day use of digital money and virtual assets.

PROGRAMME OVERVIEW

1. Introduction

Ghana is experiencing rapid digital growth. New payment systems, cross-border financial tools, online service platforms, and emerging digital markets are reshaping daily transactions and professional practice. These changes bring new opportunities but also pose risks for consumers, institutions, and the broader economy. The nationwide virtual assets education programme responds to this moment. The programme supports a national objective to strengthen understanding across all sectors. It equips professionals with the knowledge needed to understand new tools, safeguard the public, and guide responsible growth.

Virtual assets influence how value moves across borders, how businesses raise funds, and how citizens interact with financial services. They affect how fraud occurs, how data flows, and how supervision takes place. Ghana's financial sector, legal system, security institutions, and regulatory bodies must understand these tools to make informed judgments. Virtual assets also affect sectors such as health, engineering, and education through data management, digital identity, and secure records. A shared baseline of knowledge supports consistency and sound decision-making across public and private roles.

Greater national literacy in virtual assets strengthens governance through more precise policy interpretation and improved oversight. Finance professionals gain stronger skills for assessing risk and evaluating digital products. Security agencies improve readiness for crime detection and evidence management. Compliance officers and regulators benefit from sharper tools for monitoring platforms and verifying authorisation. Professional groups across all fields strengthen their readiness for digital transformation. The broader economy stands to gain from a workforce that understands both the promise and the

limits of virtual assets, supporting a balanced approach to innovation that protects citizens and preserves trust.

2. Target Group Description

This manual is designed for individuals with a solid formal education and structured training. Members of this group work in office-based, service, and technical environments where written instructions, procedures, and guidelines are part of daily activities. They are familiar with forms, records, basic reports, and digital tools used for administration, service delivery, and coordination. They follow established processes, apply rules in practical situations, and are expected to carry out tasks accurately and responsibly. This group benefits from clear explanations, step-by-step guidance, and practical examples that relate directly to work and everyday transactions. The manual supports their need for operational understanding, safe decision-making, and awareness of risks linked to virtual assets, without requiring advanced technical depth.

3. Learning Philosophy

The learning approach for this group is structured, practical, and aligned with formal work environments. Participants are familiar with written guidance, procedures, and rules, so learning builds on these strengths by presenting content in a precise sequence that moves from concepts to application.

The manual emphasises operational understanding. Each topic explains not only what virtual assets are, but how they affect tasks, decisions, and responsibilities in everyday work and service settings. Concepts are introduced with definitions, followed by examples that reflect everyday situations.

Case-based learning supports this philosophy. Scenarios drawn from real-life contexts help participants apply rules, identify risks, and choose appropriate actions. This strengthens judgment and reinforces correct procedures without requiring advanced technical expertise.

Policy and guidance interpretation is treated as a practical skill. Participants are guided on how to read instructions, notices, and rules carefully, understand their scope, and apply them correctly. This supports compliance, accountability, and consistency in decision-making.

The learning process values clarity and caution. The goal is not speed or experimentation, but informed participation, risk awareness, and responsible use. By the end of the programme, participants should feel prepared to handle virtual asset–related situations thoughtfully, follow approved processes, and seek the proper support when issues arise.

4. Programme Learning Outcomes

The aim is to achieve the following

i. To increase awareness of the risks associated with the use of virtual assets

ii. Enable informed, lawful, and appropriate participation in virtual assets

iii. Route activity to licensed channels

iv . Boost regulatory readiness and institutional capacity, and

v. Source feedback for incorporation into regulatory frameworks

Module 1

Module Title - Virtual Assets: Concepts and Context

Module Purpose: Establish a neutral, technically sound foundation on virtual assets and underlying ledger technologies, clarifying scope, terminology and practical relevance without promotion or discouragement.

Module Learning Outcomes

i. Articulate core concepts and terminology in a clear, policy-neutral manner
ii. Differentiate major virtual assets categories at a conceptual level
iii. Describe, in principle, how distributed ledgers function and why that matters for users and markets
iv. Identify realistic application areas versus common misconceptions or overstated claims

Divide the programme into modules.

SECTION 1: Introduction to Virtual Assets and Ecosystem

What Are Virtual Assets

Virtual assets are digital forms of value that exist and move through online systems. They are not physical cash that can be touched or held. Instead, they are stored electronically and accessed using phones, computers, or other digital devices. They are typically secured cryptographically and run on a blockchain or distributed ledger technology.

People use virtual assets to transfer value, make payments, or represent ownership of certain digital items. When a virtual asset is sent, the value moves through a digital network rather than passing directly from from one person to another. This enables speed and convenience, but it also requires users to understand how these systems work to stay safe.

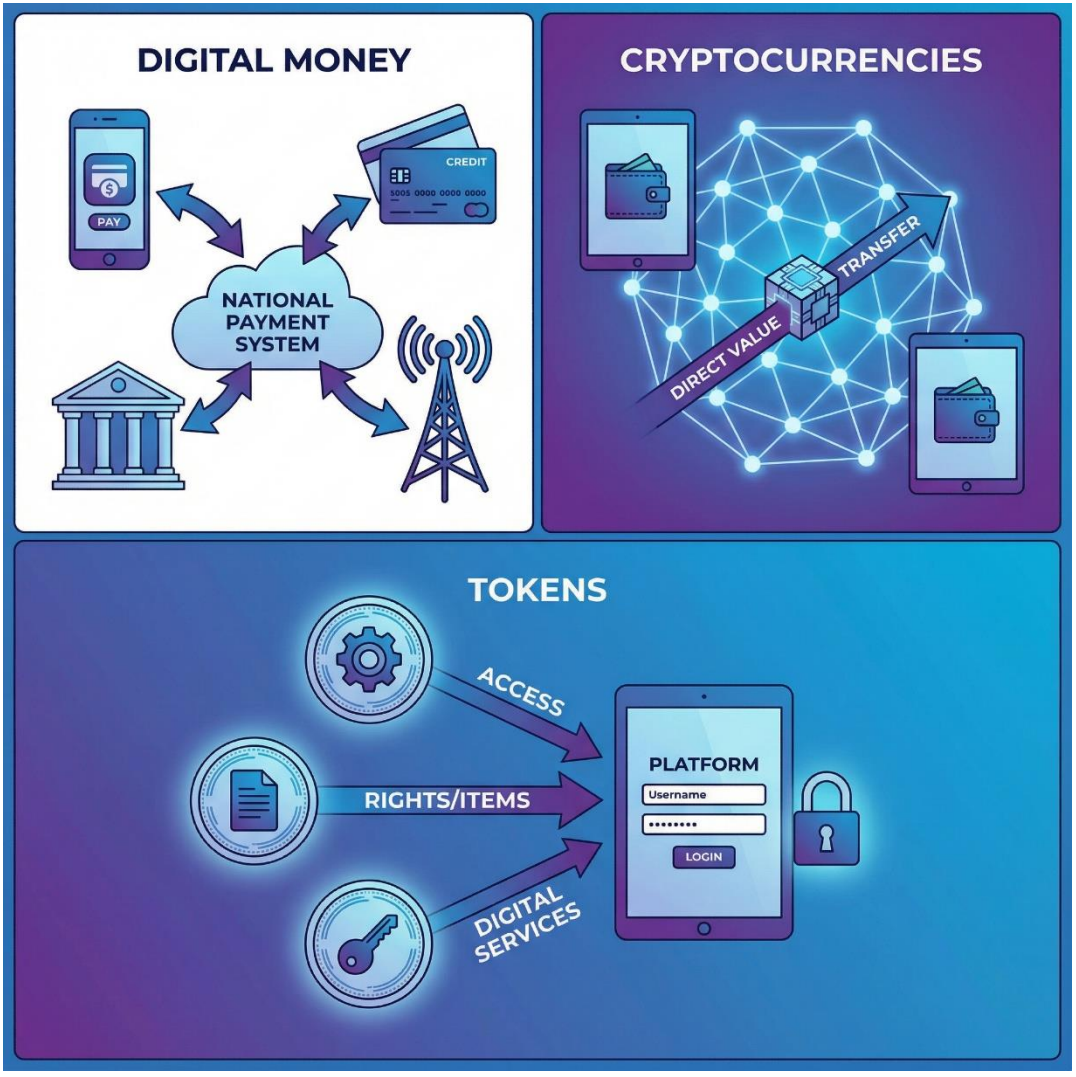
Digital Money, Cryptocurrencies, and Tokens

Digital money is a broad term for money used in electronic form. Examples include mobile money and digital bank transfers. Banks or telecom companies usually manage these under national payment systems.

Cryptocurrencies are a specific type of virtual asset. They are virtual assets that move through distributed digital networks rather than through banks or telecom systems. They allow users to send value directly to one another using digital wallets.

Tokens are created for specific purposes. Some tokens are used to access digital services, platforms, or applications. Others may represent rights, benefits, or digital items.

Understanding these differences helps users know what they are dealing with and the risks involved.

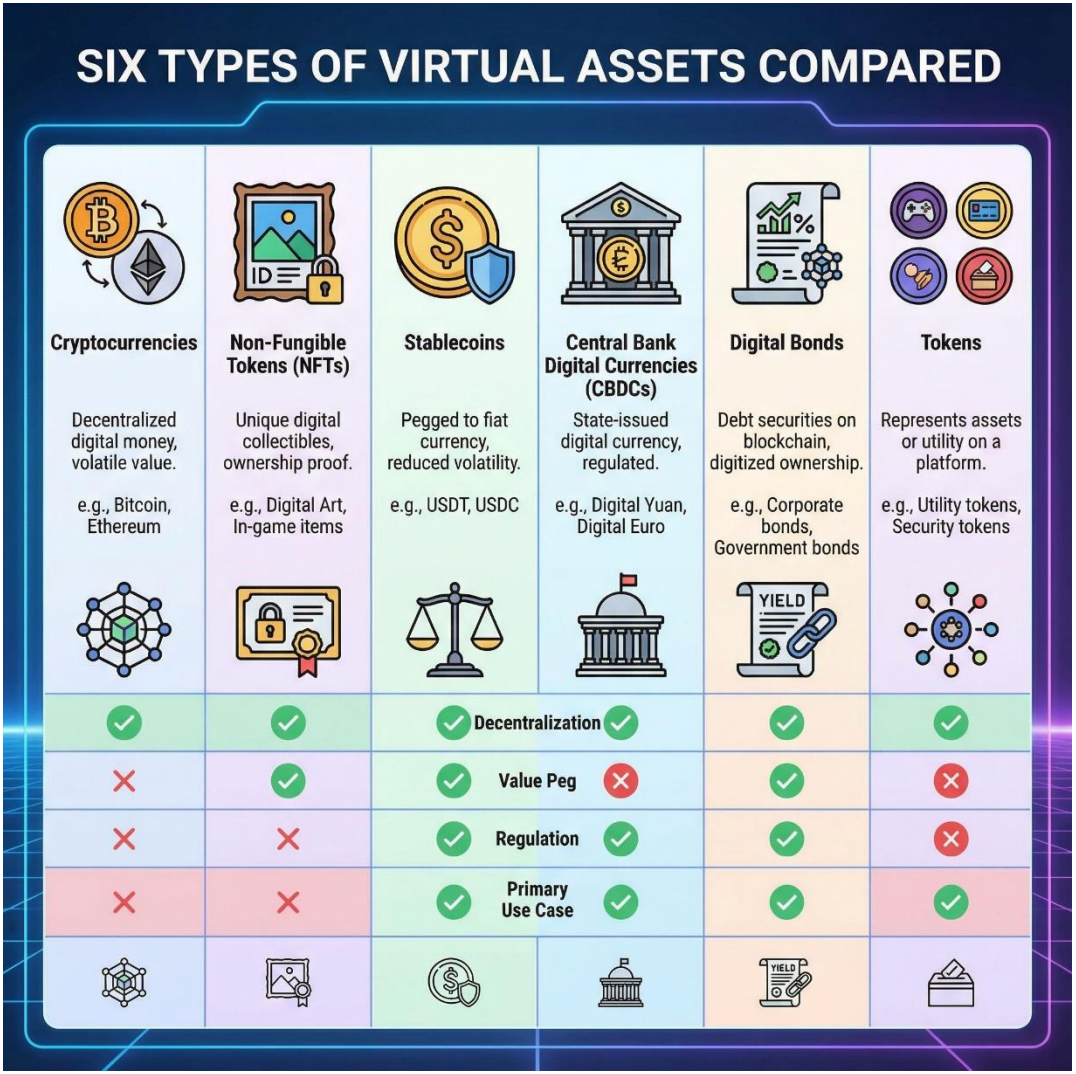

DIGITAL MONEY
PAY
CREDIT
NATIONAL PAYMENT SYSTEM
CRYPTOCURRENCIES
TRANSFER
DIRECT VALUE
TOKENS
ACCESS
RIGHTS/ITEMS
DIGITAL SERVICES
PLATFORM
Username
LOGIN

Categories of Virtual Assets

Virtual assets can be grouped into common categories:

- ✓ *Coins (Cryptocurrencies)* are virtual assets mainly used to send, receive, or store value.
- ✓ *Tokens* are digital assets created for specific uses, such as accessing a service or platform.
- ✓ *Non-Fungible Tokens (NFTs)* are unique tokens used to show ownership, access, or records. They are not used as money.
- ✓ *Stablecoins* are designed to maintain a steady value, often linked to known currencies, to reduce price volatility.
- ✓ *Central Bank Digital Currencies (CBDCs)* are digital versions of national currencies issued by central banks. Ghana's example is the eCedi.
- ✓ *A digital bond* is a loan that is created and managed using digital systems.

Each type serves a different purpose, and knowing the difference helps users make informed decisions.


SIX TYPES OF VIRTUAL ASSETS COMPARED
Cryptocurrencies
Decentralized digital money, volatile value.
e.g., Bitcoin, Ethereum
Non-Fungible Tokens (NFTs)
Unique digital collectibles, ownership proof.
e.g., Digital Art, In-game items
Stablecoins
Pegged to fiat currency, reduced volatility.
e.g., USDT, USDC
Central Bank Digital Currencies (CBDCs)
State-issued digital currency, regulated.
e.g., Digital Yuan, Digital Euro
Digital Bonds
Debt securities on blockchain, digitized ownership.
e.g., Corporate bonds, Government bonds
YIELD
Tokens
Represents assets or utility on a platform.
e.g., Utility tokens, Security tokens
Decentralization
Value Peg
Regulation
Primary Use Case

Difference Between Digital Assets, Virtual Assets and Crypto Assets

Aspect	Digital Assets (DA)	Virtual Assets (VA)	Crypto Assets
Scope	Broad category; includes blockchain and non-blockchain assets	Narrower subset; always blockchain/DLT-based	Assets built and managed on blockchain. A subset of virtual assets.
Transferability	May or may not be transferable	Specifically designed to be transferable, tradable, or exchangeable	May or may not be transferable
Verification	Can be verified by central authorities (e.g., banks, governments) or private systems	Verified through decentralised consensus mechanisms (blockchain/DLT)	Verified only on blockchain
Examples	CBDCs (eCedi), digital records, tokenised contracts	Cryptocurrencies, privately issued blockchain tokens, and tokenised commodities	Bitcoin
Regulatory Treatment	May fall under traditional financial regulation	Often treated under FATF's "virtual asset" framework, with specific	Often treated under FATF's "virtual asset" framework,

		AML/CFT implications.	with specific AML/CFT implications.

Virtual Asset Service Providers (VASPs)

Virtual Asset Service Providers, often called **VASPs**, are platforms or companies that help people access and use virtual assets. They may provide wallet services, exchanges, storage, or transfer facilities.

VASPs play an essential role because many users rely on them to manage accounts, secure assets, and provide support. Some VASPs hold users' assets, while others offer tools that users control themselves. Because VASPs interact directly with users' assets, their reliability and regulatory status are critical to safety.

How a Digital Transaction Works

A digital transaction follows a straightforward process:

1. The sender opens a digital wallet.
2. The sender selects the recipient and enters the amount.
3. The transaction is confirmed and sent into the digital network.
4. The network records the transaction and verifies it.
5. The recipient receives the value in their wallet.

This process usually happens quickly, but mistakes at any step can lead to loss. Understanding the transaction flow helps users check details carefully and avoid errors before confirming a transfer.

SECTION 2: Distributed Ledger Technology (DLT) Fundamentals

Distributed Ledger Technology (DLT) is a way to store and share data across many computers simultaneously, so everyone sees the same information. It removes the need for a central authority and helps ensure transparency, security, and trust. Think of it like a shared notebook that everyone can write in and check, but no one can secretly change. Blockchain is one popular type of DLT.

Ledgers as Shared Digital Records

A ledger is a record book that shows transactions. In digital systems, a ledger is an electronic record that stores information about who sent value, who received it, and when it happened. In DLT, this ledger is shared among many participants rather than kept by a single office or person. Everyone involved sees the same record, which reduces disputes and hidden changes. Blockchain is one well-known example of a system built using DLT. There are simple terms used in DLT. These are explained below.

Nodes as the Computers That Support the Ledger

Nodes are the computers or servers that keep copies of the shared ledger. Each node holds the same information and helps check that new transactions are correct. Because many nodes have the record simultaneously, no single person can secretly change the information. If one node fails, others still keep the record safe.

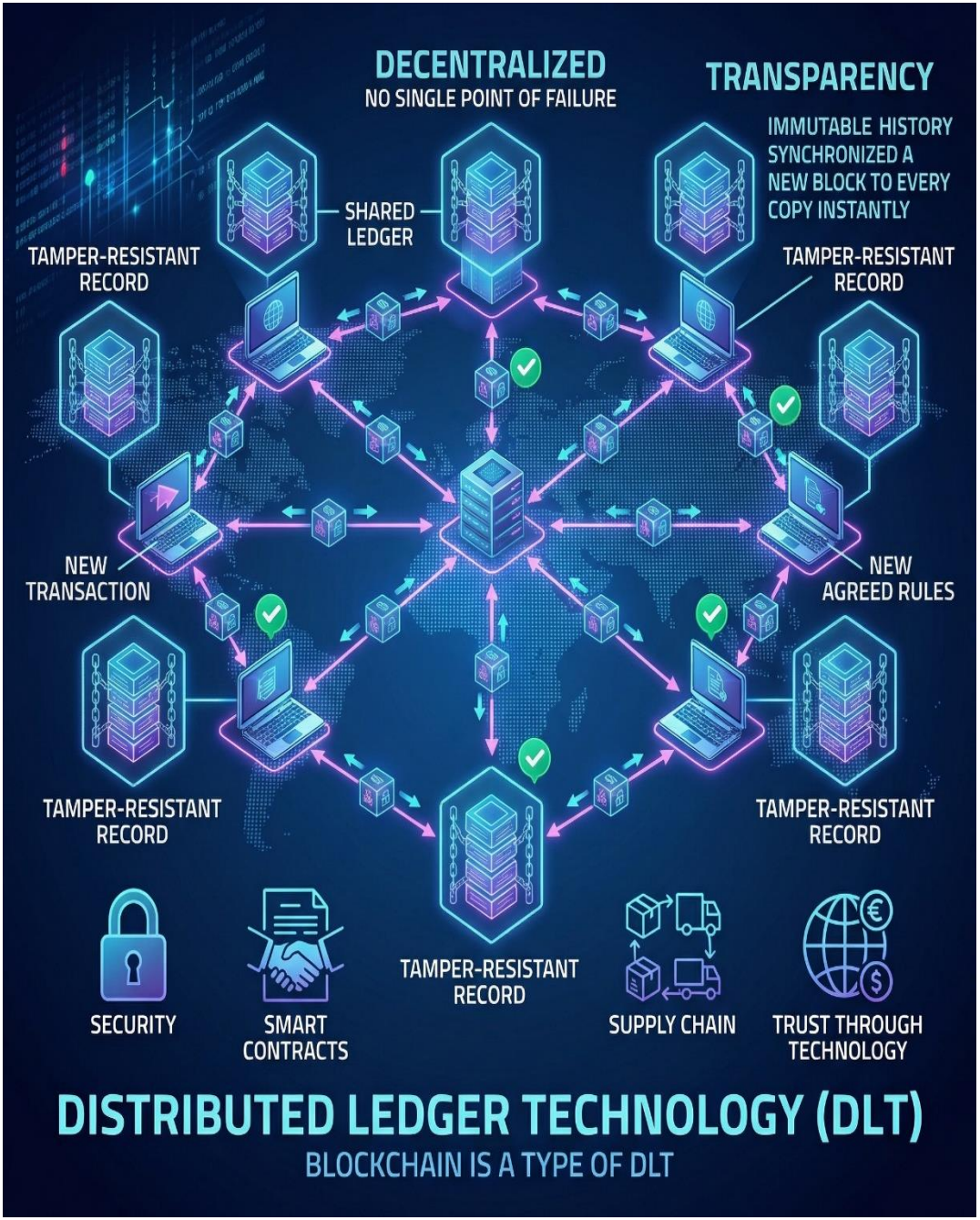
Blocks Linked Together

Transactions are grouped into blocks. Each block contains a list of recent transactions. Once a block is completed, it is linked to the previous block, forming a chain of records. This linking makes it hard to remove or change past information without being noticed. New blocks are added over time, creating a clear history of activity.

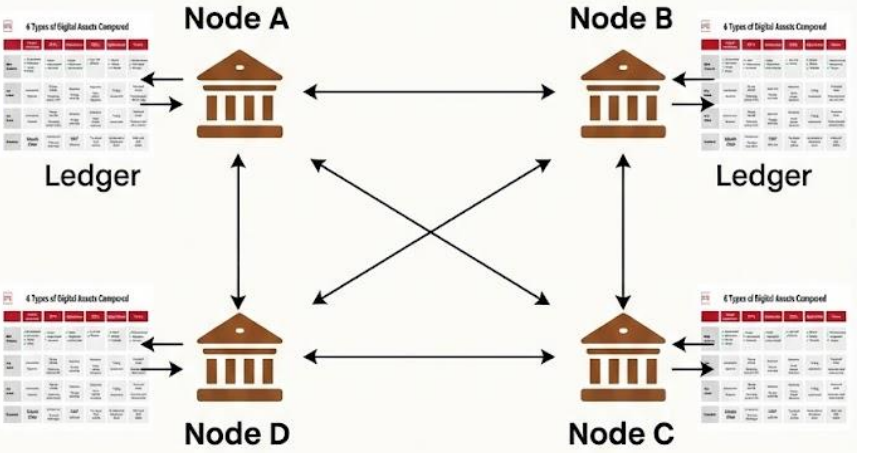
Why Transparency, Traceability, and Shared Records Matter

Transparency means transactions can be viewed and checked by authorised users. Traceability means a transaction can be traced from start to finish. Shared records mean everyone relies on the same version of information. Together, these features help reduce fraud, improve trust, and make it easier to confirm what has happened in a digital system.

This foundation explains why DLT is used to support virtual assets and other digital systems that require accuracy, trust, and shared agreement.


DECENTRALIZED
NO SINGLE POINT OF FAILURE
TRANSPARENCY
IMMUTABLE HISTORY SYNCHRONIZED A NEW BLOCK TO EVERY COPY INSTANTLY
SHARED LEDGER
TAMPER-RESISTANT RECORD
TAMPER-RESISTANT RECORD
NEW TRANSACTION
NEW AGREED RULES
TAMPER-RESISTANT RECORD
TAMPER-RESISTANT RECORD
TAMPER-RESISTANT RECORD
SECURITY
SMART CONTRACTS
SUPPLY CHAIN
TRUST THROUGH TECHNOLOGY
DISTRIBUTED LEDGER TECHNOLOGY (DLT)
BLOCKCHAIN IS A TYPE OF DLT

Distributed Ledger Technology: The Foundation of Digital Assets



DLT involves storing and sharing data across multiple computers so everyoen has the same information.

It removes the need for a central **authority** and supports **transparency, security,** and **trust.**

How does DLT work?

Many computers keep the same record of transactions simultaneously. When someone sends digital value, the information is shared with all these computers. They check the details and agree that the transaction is correct. Once they agree, the transaction is added to the shared record. The record is not erased or changed. It is only added to. Because everyone sees the same record, it becomes hard for anyone to cheat or hide information.

SECTION 3: Blockchain Deployment Models and Technical Concepts (Basic Idea)

This refers to the simple ways blockchain systems are set up and how they work. Some blockchains are open to everyone, some are used only by certain groups, and others are shared by trusted organisations. These systems follow set rules to automatically and safely record transactions without altering records. Blockchain is the underlying system. Wallets, platforms, and apps are tools built on top of it. This prevents confusion between infrastructure and user-facing services.

Types of Blockchain Networks

Blockchain systems can be deployed in different ways depending on who controls access and how decisions are made:

- Public Blockchains: These are open to everyone. Anyone can join, read, write, or validate transactions. Examples include Bitcoin and Ethereum. They promote transparency and decentralisation, but may be slower due to high participation. Public blockchains are for open payment systems and public networks.

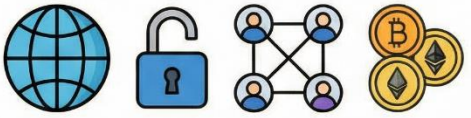
- Private Blockchains Access is restricted to specific participants. A single organisation or group controls who can read or write data. These are faster and more secure for internal use, but less decentralised. Private blockchains are for internal organisational records.

- Consortium Blockchains: A group of organisations jointly manages the network. It strikes a balance between decentralisation and control, making it ideal for industries such as banking, supply chains, or healthcare, where collaboration is crucial. Consortium blockchains are for shared industry systems

- A hybrid blockchain is a blockchain system that combines features of both public and private blockchains.

Four Types of Blockchain Compared

PUBLIC BLOCKCHAINS



- Open to everyone: Join, read, write, validate.
- Promotes transparency & decentralization.
- May be slower due to high participation.
- For open payment systems & public networks.

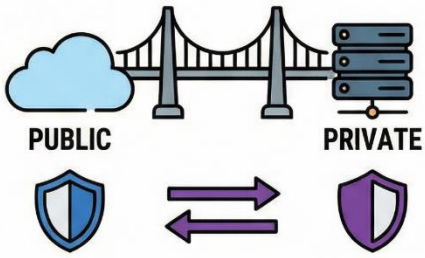
PRIVATE BLOCKCHAINS

- Restricted access to specific participants.
- Single organization controls data.
- Faster & more secure for internal use.
- Less decentralized.
- For internal organizational records.

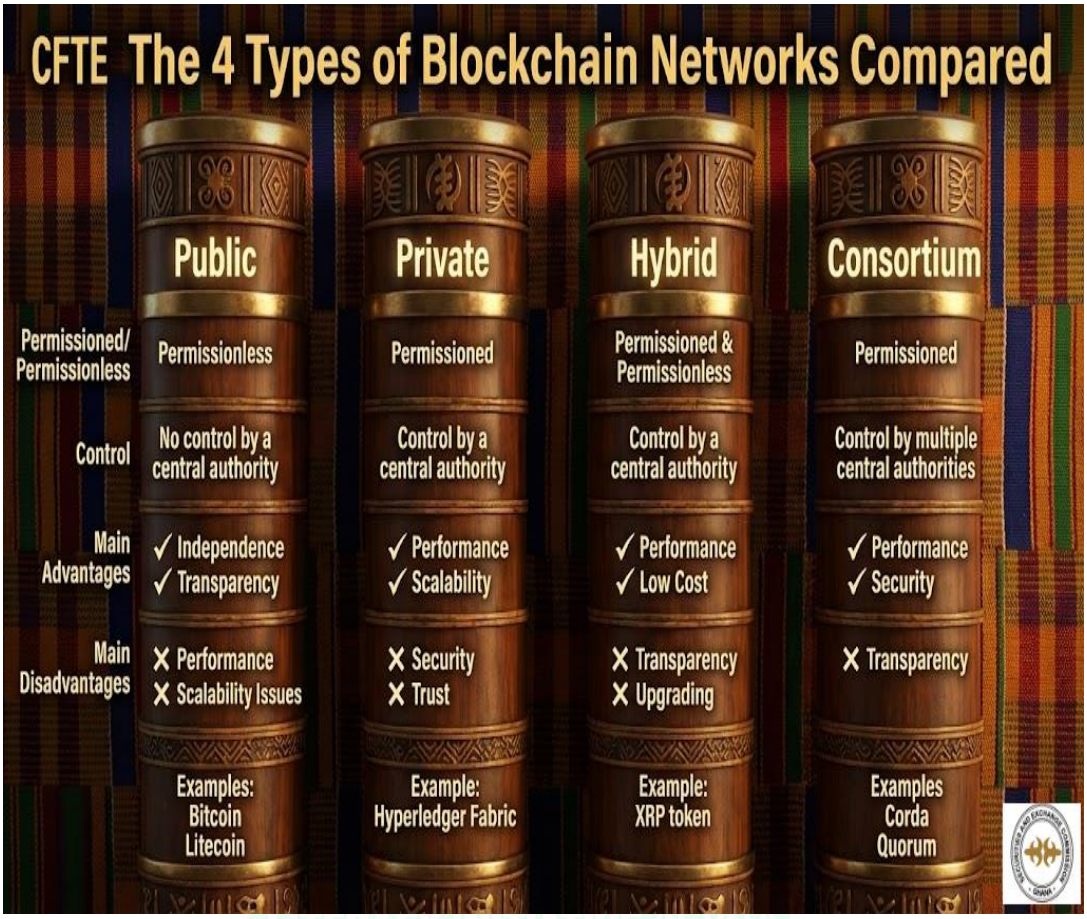
CONSORTIUM BLOCKCHAINS

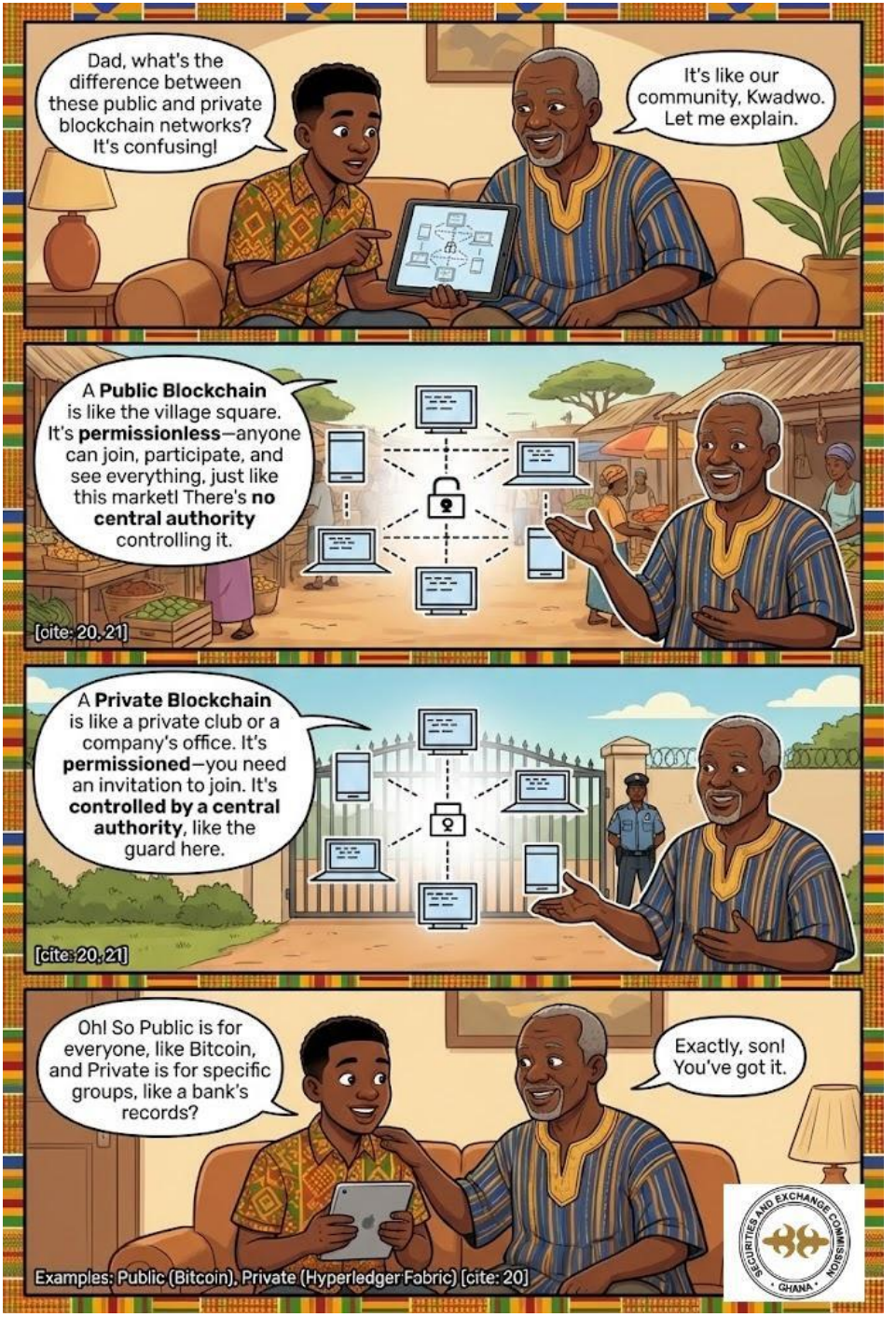
- Jointly managed by a group of organizations.
- Balances decentralization & control.
- Ideal for collaboration (banking, supply chain, healthcare).
- For shared industry systems.

HYBRID BLOCKCHAIN



Combines features of both public and private blockchains.




Dad, what's the difference between these public and private blockchain networks? It's confusing!
It's like our community, Kwadwo. Let me explain.
A **Public Blockchain** is like the village square. It's **permissionless**—anyone can join, participate, and see everything, just like this market! There's **no central authority** controlling it.
[cite: 20, 21]
A **Private Blockchain** is like a private club or a company's office. It's **permissioned**—you need an invitation to join. It's **controlled by a central authority**, like the guard here.
[cite: 20, 21]
Oh! So Public is for everyone, like Bitcoin, and Private is for specific groups, like a bank's records?
Exactly, son! You've got it.
Examples: Public (Bitcoin), Private (Hyperledger Fabric) [cite: 20]

Smart Contracts: Automated Digital Agreements

Smart contracts are self-executing programmes stored on the blockchain. They automatically execute instructions when predefined conditions are met, without the need for intermediaries. Example: A smart contract for a farming subsidy might release funds to a farmer once satellite data confirms rainfall and crop growth.

Benefits include:

- Reduced human error
- Faster execution
- Transparent and tamper-proof logic

Transaction Basics and Fees

Every blockchain transaction involves:

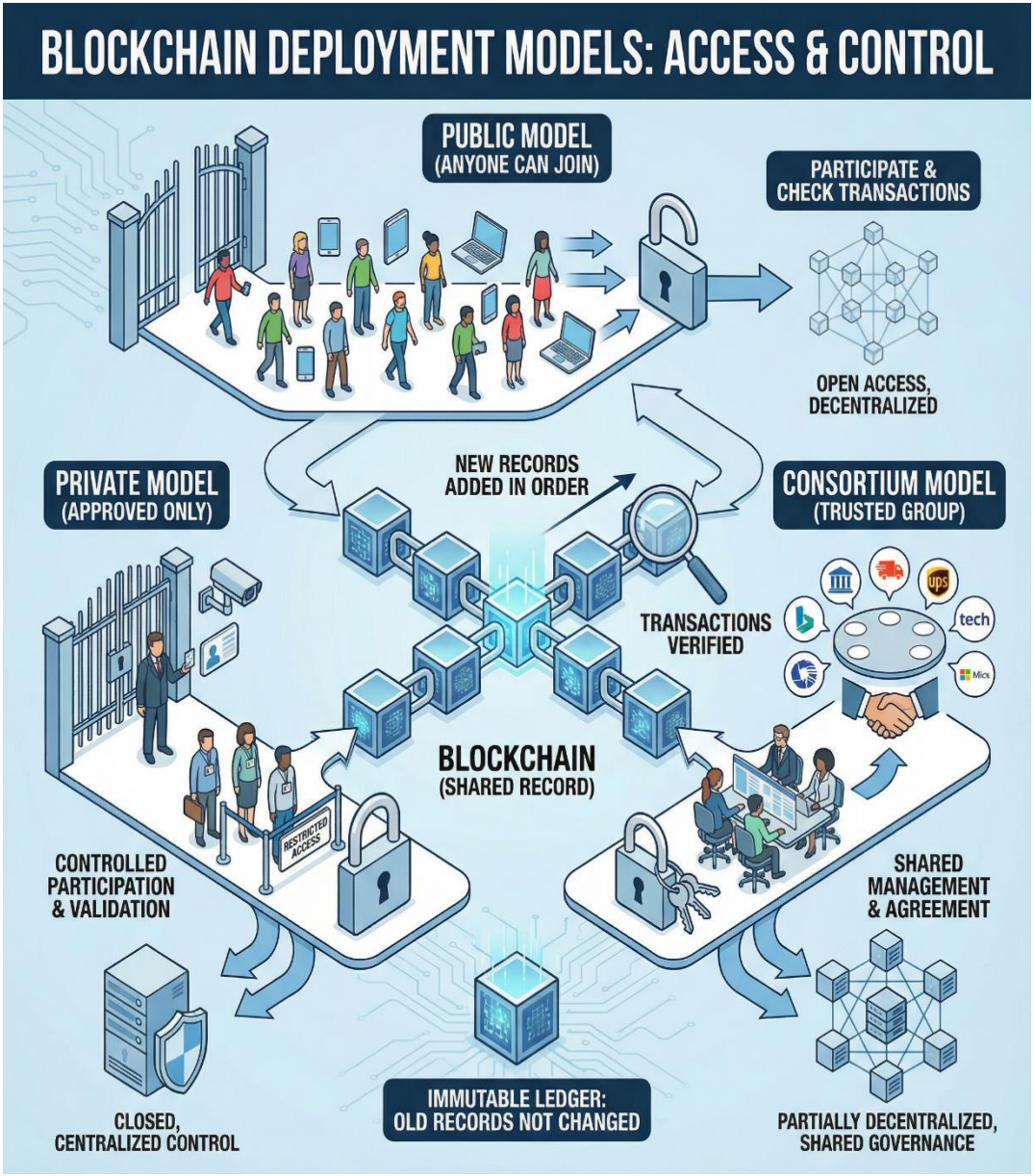
- ✓ Data validation, ensuring the transaction is legitimate.
- ✓ Recording: Adding it to the blockchain ledger.
- ✓ Network participation: Miners or validators using computing power to process transactions.

Why fees appear:

- ✓ Fees compensate validators for their work.
- ✓ They prevent spam and ensure network efficiency.
- ✓ In public blockchains, fees can vary depending on demand and complexity.

Simple Description of How Blockchain Deployment Models Work

Blockchain deployment models describe who is allowed to use a blockchain system and how access is controlled. In some models, anyone can join and use the system to send or receive digital value. In other models, only approved people or organisations are allowed to use the system. There are also models in which a group of trusted organisations shares a single system and agrees on how it is managed. In all cases, the blockchain keeps a shared record of transactions. New records are added in order, and old records are not changed. The main difference between the models is who can participate, who can check transactions, and who controls access. This setup helps organisations choose the type of blockchain that fits their needs for openness, privacy, and control.


BLOCKCHAIN DEPLOYMENT MODELS: ACCESS & CONTROL
PUBLIC MODEL
(ANYONE CAN JOIN)
PARTICIPATE &
CHECK TRANSACTIONS
OPEN ACCESS,
DECENTRALIZED
NEW RECORDS
ADDED IN ORDER
PRIVATE MODEL
(APPROVED ONLY)
CONSORTIUM MODEL
(TRUSTED GROUP)
TRANSACTIONS
VERIFIED
BLOCKCHAIN
(SHARED RECORD)
RESTRICTED ACCESS
CONTROLLED
PARTICIPATION
& VALIDATION
SHARED
MANAGEMENT
& AGREEMENT
CLOSED,
CENTRALIZED CONTROL
IMMUTABLE LEDGER:
OLD RECORDS NOT CHANGED
PARTIALLY DECENTRALIZED,
SHARED GOVERNANCE

SECTION 4: Real-World Applications and Use Cases

Virtual assets and blockchain systems are used in many practical ways that support daily activities, institutions, and services. These applications focus on improving speed, accuracy, and trust.

Faster Cross-Border Transfers

Virtual assets can be used to send money across borders more quickly than traditional methods. Instead of waiting several days for international transfers, value can move within minutes or hours. This is useful for supporting family members in other countries, paying suppliers, or receiving funds from abroad. Faster transfers also reduce delays and uncertainty for users.

Support for Banking Services

Banks and financial institutions use blockchain systems to improve internal processes. These systems help with record-keeping, transaction settlement, and reconciliation between institutions. By using shared digital records, banks reduce errors, speed up processing, and improve transparency. Virtual asset systems can also support new digital financial products.

Digital Identity for Public and Private Services

Blockchain systems can support digital identity solutions. These allow people to prove their identity when accessing services such as healthcare, education, or financial accounts. Digital identity records reduce the need for repeated paperwork and help prevent identity fraud. Both public institutions and private companies can use these systems to securely verify users.

Supply Chain Tracking and Record Keeping

Virtual assets and blockchain systems are used in many practical ways that support daily activities, institutions, and services. These

applications focus on improving speed, accuracy, transparency, and trust.

Faster Cross-Border Transfers
Virtual assets can be used to send money across borders more quickly than traditional methods. Instead of waiting several days, value can move within minutes or hours. This supports families receiving funds from abroad, businesses paying suppliers, and individuals receiving remittances.

Support for Banking and Financial Services
Banks and financial institutions use blockchain systems to improve record keeping, transaction settlement, and reconciliation. Shared digital records reduce errors, speed up processing, and improve transparency between institutions. These systems also support new forms of digital financial products and services.

Digital Identity for Public and Private Services
Blockchain systems can support digital identity solutions that enable people to prove their identity when accessing services. This is useful for healthcare, education, voting systems, and financial services. Digital identity helps reduce fraud, repeated paperwork, and identity theft.

Supply Chain Tracking, Certificate Verification, and Record-Keeping
Blockchain technology records each step as goods move from producers to consumers. This helps track food products, medicines, and manufactured goods. It also supports verification of certificates such as school records, licenses, inspection reports, and permits. Shared records improve accountability and trust.

Government Services and Public Administration
Public institutions can use blockchain systems for land and tax records, as well as for social support programmes . Digital records reduce

disputes, improve accuracy, and make it easier to confirm ownership or eligibility. This supports better service delivery and transparency.

Healthcare Data Management
Healthcare providers can use blockchain systems to securely manage patient records. Shared access allows authorised providers to see accurate information while protecting privacy. This improves care coordination and reduces errors.

Agriculture and Farmer Support
Blockchain systems are used to track farm produce, confirm sources, and manage subsidy or support payments. Farmers benefit from clearer records and faster access to funds. Buyers gain confidence in product origin and quality.

Insurance and Claims Processing
Insurance companies use blockchain systems to speed up claims processing. Intelligent systems can release payments automatically once conditions are met. This reduces delays, paperwork, and disputes.

Digital Voting and Community Records
Some systems use blockchain for secure voting or community decision records. Shared records help ensure transparency and prevent tampering, especially in local or organisational settings.

APPLICATIONS OF BLOCKCHAIN TECHNOLOGY IN GHANA

1) eCedi Central Bank Digital Currency Pilot (2021–2022)

*Ghana's central bank, the **Bank of Ghana (BoG)**, began developing a state-backed digital currency called the **eCedi** in **2021** as part of its "Digital Ghana Agenda." On **August 28, 2021**, the Governor of the Bank of Ghana announced the launch of the **eCedi pilot phase**, making Ghana one of the first African countries to test a general-purpose Central Bank Digital Currency (CBDC). The pilot aimed to test how a digital form of the Ghana cedi could be used for everyday transactions, promote financial inclusion, and support digital payment systems. The pilot continued through **2022**, during which eCedi was tested for online and offline transactions with users and merchants in selected locations.*

2) eCedi Hackathon for CBDC Use Cases (October 2023 – Early 2024)

*In **October 2023**, the Bank of Ghana launched a **12-week eCedi Hackathon** to explore practical applications of the eCedi and related blockchain solutions. This initiative brought together developers, fintech professionals, designers, and engineers to identify innovative use cases for the CBDC in areas such as merchant payments, government services, and digital identity. The hackathon was part of Ghana's efforts to build a local ecosystem around digital currency and blockchain innovation before broader rollout.*

SECTION 5: Common Misconceptions and Risk Awareness

Many problems around virtual assets come from misunderstanding rather than from the technology itself. Clearing up common misconceptions helps people make careful decisions and avoid unnecessary losses.

Virtual Assets Are Not Illegal by Default

Virtual assets are not automatically illegal. Many people hear rumours that all virtual assets are forbidden, which is not true. Some uses are lawful, while others may be restricted or regulated. What matters is how and where virtual assets are used. Using approved platforms and following national guidance helps users stay within the law.

Blockchain Is Not the Same as Cryptocurrency

Blockchain is a technology, while cryptocurrency is just one type of virtual asset that uses that technology. Blockchain is like the road or system that records information. Cryptocurrencies are one kind of vehicle that moves on that road. The same blockchain technology is also used for records, certificates, tracking goods, and identity systems, not only for money.

Digital Systems Still Need Rules and Supervision

Even though blockchain systems use technology to record transactions, they do not remove the need for rules. Digital systems can still be misused without oversight. Regulation and supervision help protect users, reduce fraud, and ensure platforms operate responsibly. Technology alone cannot guarantee safety without proper governance.

No Digital Asset Gives Automatic or Guaranteed Returns

There is no virtual asset that guarantees profit. Messages that promise fast, easy, or automatic returns are often false. Digital assets can go up or down in value, and some may lose value completely. Anyone

claiming “risk-free” or “guaranteed” profit is usually trying to deceive others.

Basic Risk Signals to Watch For

There are warning signs that show often amongst scams. These include promises of quick wealth, pressure to act immediately, people pretending to be helpers or officials, and apps or websites that copy real platforms. Fake platforms often disappear after collecting money. Recognising these signals early helps users stop, pause, and seek advice before loss occurs.

Understanding these misconceptions and risk signals supports safer behaviour. Awareness helps people avoid rushing into decisions, question suspicious offers, and use virtual assets with greater caution.

SECTION 6: Ghana’s Regulatory Context

Understanding Ghana’s regulatory environment helps users know what is allowed, what is monitored, and how they are protected when using virtual assets and digital money services.

Bank of Ghana Guidance at a High Level

The Bank of Ghana provides guidance on digital money and payment systems to protect the public and maintain confidence in the financial system. It oversees payment services, issues rules for safe operation, and works to reduce fraud and misuse. While not all virtual assets are treated the same, the Bank of Ghana encourages the careful use of approved services and warns the public against scams and false promises.

Licensing and Reporting in Simple Terms

Licensing means a service provider has received approval from the appropriate authority to operate. Licensed providers are expected to follow rules regarding security, customer support, and record-keeping.

Reporting means that when problems occur, such as fraud or suspicious activity, users and providers should inform the relevant authority. This helps regulators track risks, take action against wrongdoing, and, over time, improve protections.

How Regulation Protects Users and Supports Financial Stability

Regulation helps protect users by setting minimum standards for how services operate and how customer issues are handled. It reduces the chances of unsafe platforms harming the public. Regulation also supports financial stability by monitoring risks, limiting harmful practices, and ensuring that digital systems do not threaten the broader economy. Together, these measures help create a safer environment where people can use digital services with greater caution and awareness.

This section helps learners understand that rules are in place to protect them and the wider financial system, and that using approved channels and reporting problems early are key parts of staying safe.

Assessment Strategy: Scenario-Based Task

Scenario-Based Task 1: Choosing the Right Type of Virtual Asset

A small business officer is asked to advise a colleague who wants to receive payments from customers abroad. The colleague is unsure whether to use mobile money, cryptocurrency, a stablecoin, or a token offered by an online platform that promises quick conversion and low fees.

Task for Learners

- Identify the different types of virtual assets mentioned in the scenario.
- Explain the key differences between digital money, cryptocurrencies, stablecoins, and tokens.
- Recommend which type of virtual asset is most suitable for cross-border payments and explain why.
- Highlight one risk the colleague should be aware of before proceeding.

Learning Focus

Understanding virtual asset categories, use cases, and risk awareness.

Scenario-Based Task 2: Understanding a Digital Transaction and DLT

A staff member sends virtual assets to a supplier using a wallet. After sending, the supplier claims the funds have not arrived. The sender is unsure how to confirm whether the transaction was successful and worries that the money may be lost.

Task for Learners

- Describe the steps of how a digital transaction works from sender to receiver.

- Explain how Distributed Ledger Technology helps verify transactions.
- Identify what tools or information can be used to check transaction status.
- Explain why shared records improve transparency and reduce disputes.

Learning Focus
Transaction flow, DLT fundamentals, transparency, and traceability.

Scenario-Based Task 3: Platform Choice, Fees, and Regulatory Awareness
An employee discovers a new virtual asset platform advertised on social media. The platform offers lower fees and faster transactions than well-known services. It claims to be "fully decentralised" and does not clearly state whether it is licensed in Ghana.

Task for Learners
- Identify the platform and intermediary risks present in this scenario.
- Explain the difference between public, private, and consortium blockchain systems in relation to platform control.
- Discuss why fees, spreads, and transaction delays may differ across platforms.
- Outline the steps the employee should take to verify authorisation and protect themselves before using the platform.

Learning Focus
Platform selection, deployment models, costs and fees, and Ghana's regulatory context.

Module 2

Module Title: Key Tools and Components

Module Purpose: Introduce the principal tools, interface and operational building blocks used in accessing and managing virtual assets, emphasising foundational safeguards that reduce avoidable errors and losses

Module Learning Outcomes

i. Distinguish the primary forms of access and custody arrangements at a high level.
ii. Explain the general role of platforms/intermediaries and the implications for user responsibilities
iii. Recognise typical sources of cost and friction and how they influence user experience
iv. Outline baseline operational safeguards appropriate for varied user contexts

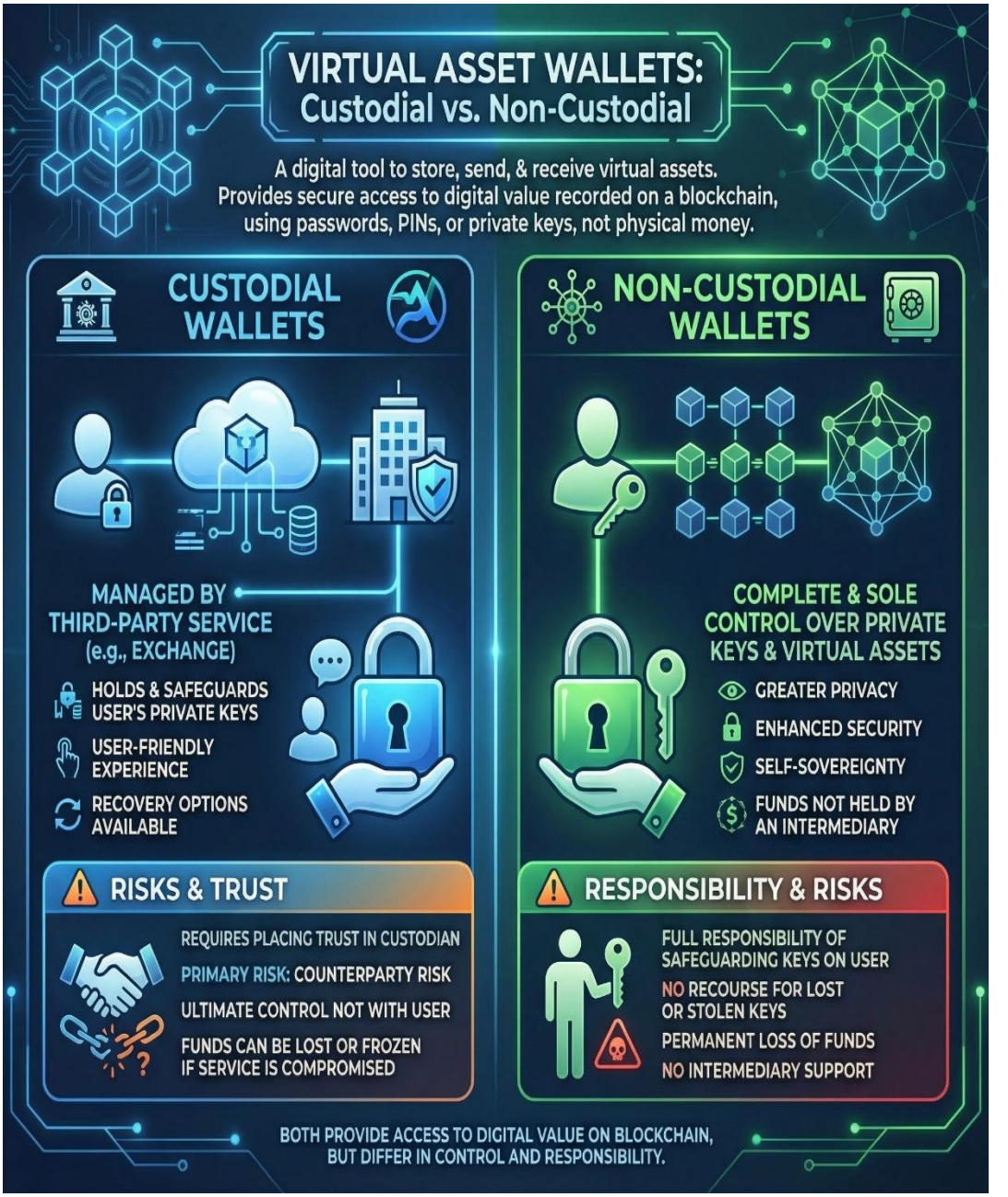
Section 1: Access and Custody Concepts

Custodial Wallets

A custodial wallet is a wallet in which a service provider maintains and manages the security on behalf of the user. The user accesses the wallet through an app or platform, and the service helps protect the assets and may assist with recovery if issues arise. This is similar to how mobile money or bank apps work.

Non-Custodial Wallets

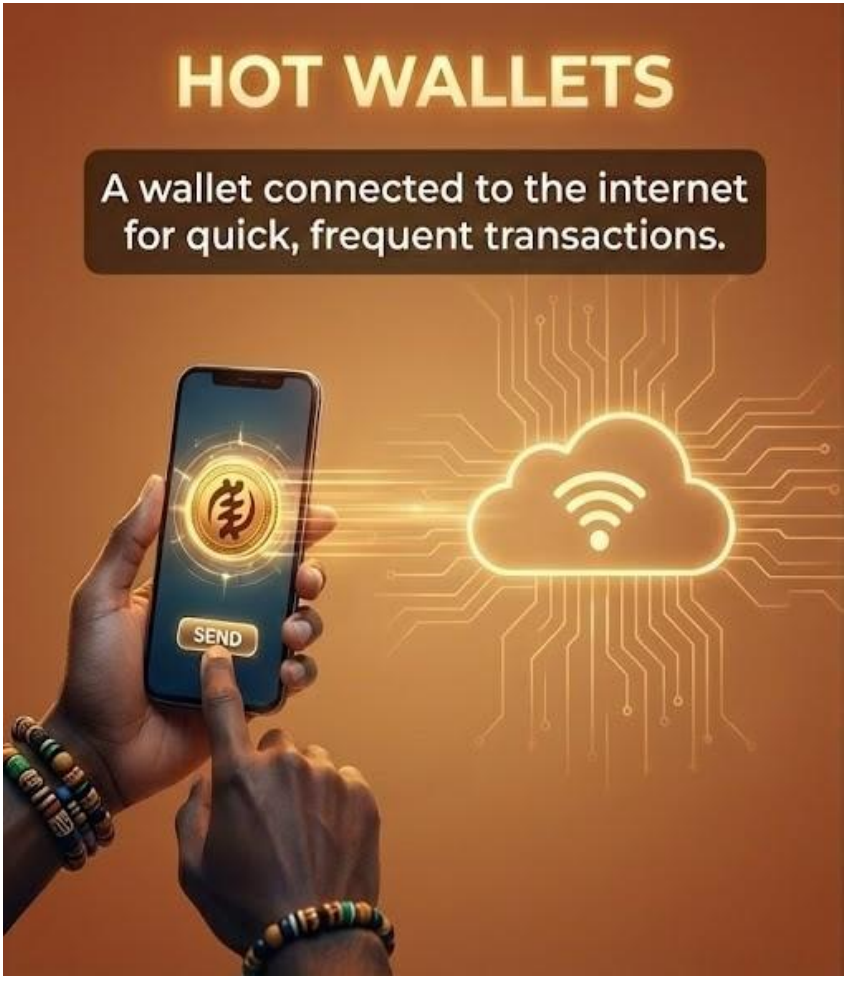
A non-custodial wallet is one in which the user has complete control over the wallet and its security details. The service provider does not hold the keys or passwords. This gives the user more power, but also more responsibility for keeping the wallet safe.


VIRTUAL ASSET WALLETS:
Custodial vs. Non-Custodial
A digital tool to store, send, & receive virtual assets.
Provides secure access to digital value recorded on a blockchain,
using passwords, PINs, or private keys, not physical money.
CUSTODIAL WALLETS
MANAGED BY THIRD-PARTY SERVICE (e.g., EXCHANGE)
HOLDS & SAFEGUARDS USER'S PRIVATE KEYS
USER-FRIENDLY EXPERIENCE
RECOVERY OPTIONS AVAILABLE
NON-CUSTODIAL WALLETS
COMPLETE & SOLE CONTROL OVER PRIVATE KEYS & VIRTUAL ASSETS
GREATER PRIVACY
ENHANCED SECURITY
SELF-SOVEREIGNTY
FUNDS NOT HELD BY AN INTERMEDIARY
RISKS & TRUST
REQUIRES PLACING TRUST IN CUSTODIAN
PRIMARY RISK: COUNTERPARTY RISK
ULTIMATE CONTROL NOT WITH USER
FUNDS CAN BE LOST OR FROZEN IF SERVICE IS COMPROMISED
RESPONSIBILITY & RISKS
FULL RESPONSIBILITY OF SAFEGUARDING KEYS ON USER
NO RECOURSE FOR LOST OR STOLEN KEYS
PERMANENT LOSS OF FUNDS
NO INTERMEDIARY SUPPORT
BOTH PROVIDE ACCESS TO DIGITAL VALUE ON BLOCKCHAIN,
BUT DIFFER IN CONTROL AND RESPONSIBILITY.


THE WALLET DECISION & CUSTODIAL WALLETS
Dad, what are these wallet types?
A wallet is a digital tool. **Custodial Wallets** are like banks. A company holds your **private keys**. You just use a password.
EXCHANGE / COMPANY
Key Concept: Company controls the keys for easy access.
CUSTODIAL: PROS & CONS
The good and bad?
PROS
CONS
Easy to use, password recovery, customer support.
You trust the company. Risk of hacks or freezing. "Not your keys, not your coins."
NON-CUSTODIAL WALLETS & TRUE OWNERSHIP
And Non-Custodial?
You hold your **own private keys**. Total control. No company can freeze your assets. It's true ownership and privacy.
Key Concept: You have full control and responsibility.
NON-CUSTODIAL CONS & CHOOSING
The catch?
CONS
CHOICE
Convenience
Control
Choose wisely, son.
Full responsibility. Lose your keys/seed phrase, it's gone forever. No recovery.
Trade-off: Convenience vs. Control. Many use both for different needs.

Hot Wallets

A hot wallet is a wallet connected to the internet. It is easy to use for the regular sending and receiving of digital assets. Because it is always online, it is convenient but needs strong security to reduce risk.



Cold Wallets

A cold wallet is a wallet kept offline, not connected to the internet. It is often used for storing digital assets for a long time. Because it is offline, it offers stronger protection from online attacks, but it is less convenient for daily use.

VIRTUAL ASSET WALLETS: HOT VS. COLD

HOT WALLET

Connects to the internet for frequent transactions.

Key features

- Always online
- Fast access for sending and receiving assets
- Common examples: mobile wallets, web wallets, exchange wallets

Advantages

- Convenient for daily use
- Easy to access from phones or computers

Risks

- Higher exposure to hacking, phishing, and malware
- Less suitable for storing large amounts for long periods

COLD WALLET

Stays offline for long-term storage.

Key features

- No internet connection
- Private keys stored offline
- Common examples: hardware wallets, paper wallets

Advantages

- Stronger protection against online attacks
- Better for holding large balances

Limitations

- Slower access when transactions are needed
- Requires careful handling to avoid loss or damage

SIMPLE COMPARISON

Feature	Hot Wallet	Cold Wallet
Internet connection	Online ✓	Offline ✗
Security level	↓ Lower	Higher ↑
Ease of access	High ↑	↓ Lower
Best use	Daily transactions	Long term storage

In practice, many users combine both types. A hot wallet handles regular transactions, while a cold wallet protects savings held over longer periods.

Private Keys

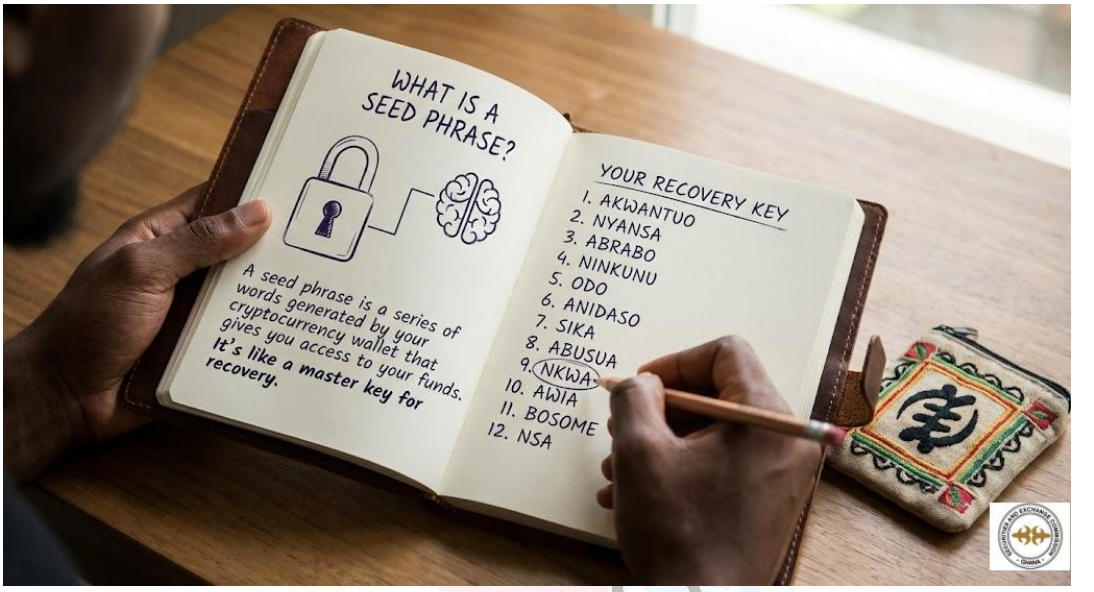
A private key is a secret code that grants access to a wallet and its assets. Whoever controls the private key controls the assets. It must be kept private and never shared.

Public Keys

A public key, in the context of virtual assets, is a cryptographic address used to receive digital assets and to verify transactions on a blockchain network. The public key is openly shared and, together with a corresponding private key, confirms ownership and authenticates transactions without revealing the private key.

Seed Phrases

A seed phrase is a set of words that can be used to recover a wallet if a device is lost or damaged. Anyone who has the seed phrase can access the wallet, so it must be stored securely and kept secret.



Password Recovery

Password recovery is the process of regaining access to a wallet or account when a password is forgotten. In custodial wallets, the service provider may help. In non-custodial wallets, recovery depends on having the correct seed phrase.

Trade-Offs: Convenience and Security

Convenience means how easy a wallet is to use for daily transactions. Security means how well the wallet protects assets from loss or theft. Custodial and hot wallets are usually more convenient but rely on third-party systems. Non-custodial and cold wallets offer stronger security but require careful user handling. Choosing a wallet involves balancing ease of use with the level of protection needed.

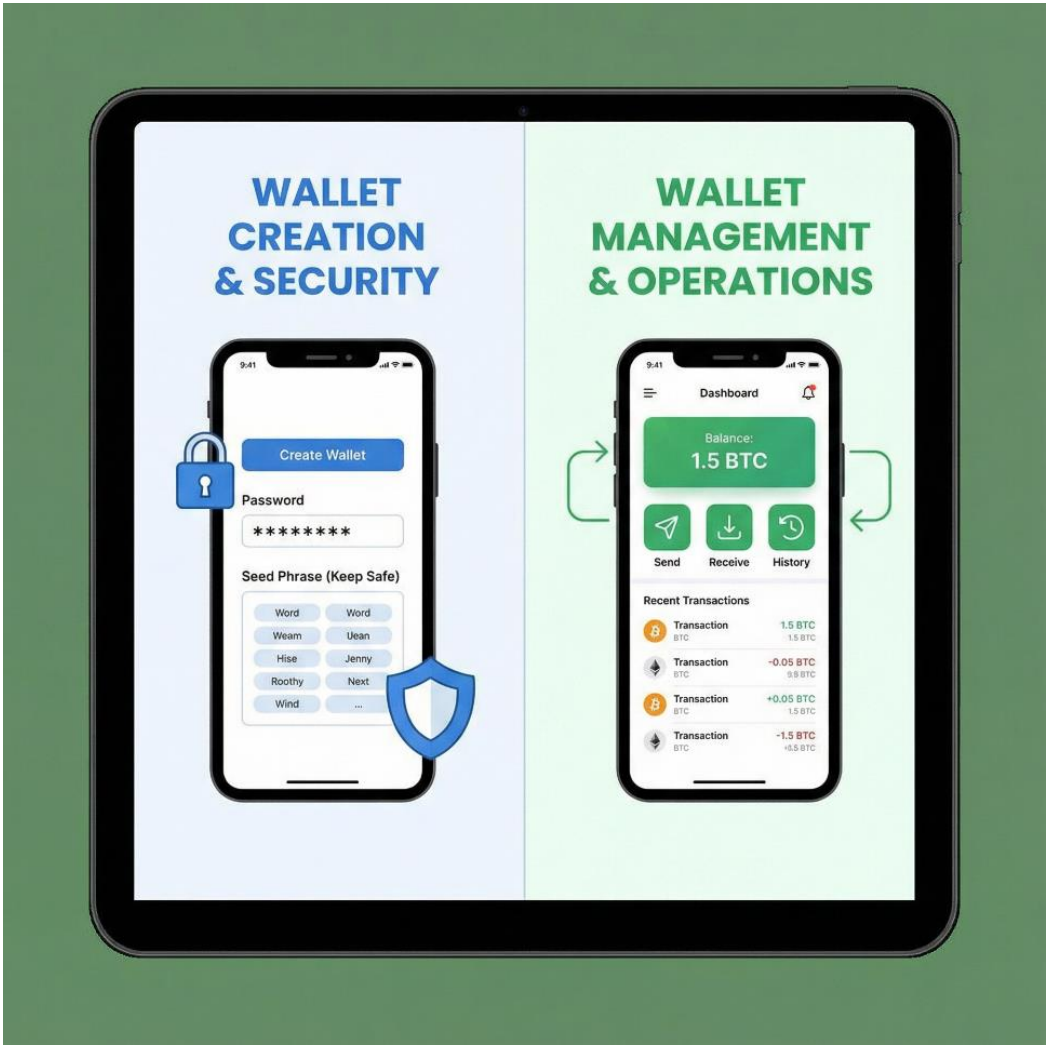
SECTION 2: Wallet Interfaces and Operations

This section explains how wallets are created and used, how transactions are checked, and how devices should be protected when handling virtual assets. The focus is on practical understanding and safe operation.

Wallet Creation and Management

Creating a wallet usually involves downloading an approved wallet application or using a service provided by a licensed platform. During setup, the user is asked to create a password or PIN and, in some cases, write down recovery information such as seed phrases. This information is vital because it controls access to the wallet.

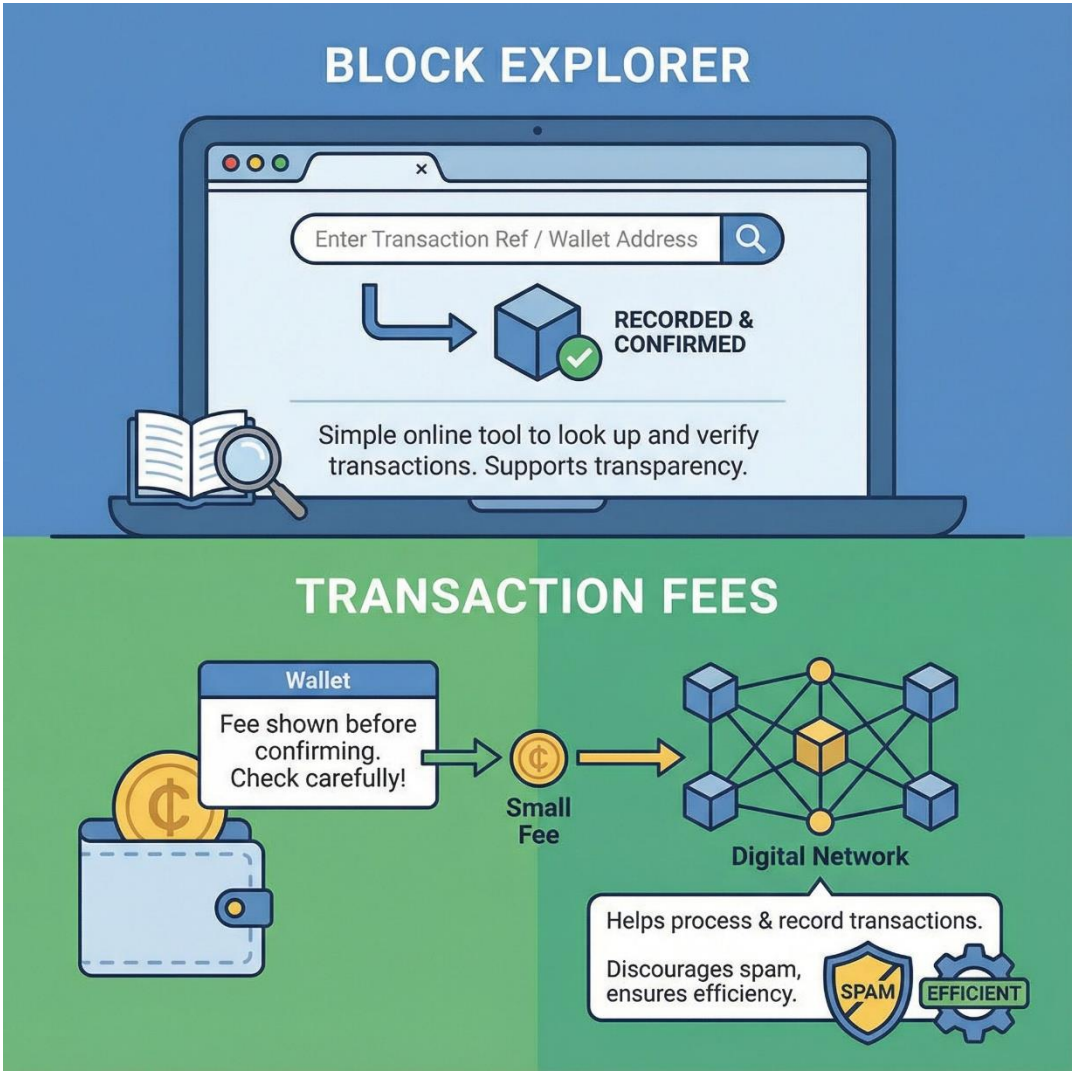
Managing a wallet includes checking balances, sending and receiving assets, and reviewing past transactions. Users should always log out properly after use and keep their wallet app up to date. Good wallet management also means keeping recovery information safe and never sharing access details with others.


WALLET CREATION & SECURITY
Create Wallet
Password
****
Seed Phrase (Keep Safe)
Word
Word
Weam
Uean
Hise
Jenny
Roothy
Next
Wind
...
WALLET MANAGEMENT & OPERATIONS
Dashboard
Balance:
1.5 BTC
Send
Receive
History
Recent Transactions
Transaction
BTC
1.5 BTC
Transaction
BTC
-0.05 BTC
Transaction
BTC
+0.05 BTC
Transaction
BTC
-1.5 BTC

Simple Explanation of Transaction Fees and Verification Tools

A block explorer is a simple online tool that allows users to look up and confirm transactions after they are sent. By entering a transaction reference or wallet address, a user can see whether the transaction has been recorded and confirmed. This helps verify that money was sent or received successfully and supports transparency.

When a transaction is made, a small transaction fee (Gas fee) is often charged. This fee helps the digital network process and record the transaction. Fees also discourage spam and ensure that transactions are handled efficiently. The wallet usually shows the cost before the user confirms the transaction, so users should check this carefully.



Secure Device Practices and Avoiding Threats

Because wallets run on phones or computers, device security is crucial. Users should lock their devices with a password, PIN, or biometric option. They should install apps only from trusted sources and avoid clicking links from unknown messages.

Malware and phishing attacks are common risks. Malware is harmful software that can steal information, while phishing involves fake messages or websites designed to trick users into revealing passwords or keys. To reduce these risks, users should keep their devices updated, avoid suspicious links, and ask for help when something seems unclear.

SECTION 3: Platforms and Intermediaries

Virtual assets are usually accessed through platforms and intermediaries. These are services that help users buy, sell, store, or transfer digital value. Understanding the different types of platforms helps users choose safe options and know their responsibilities.

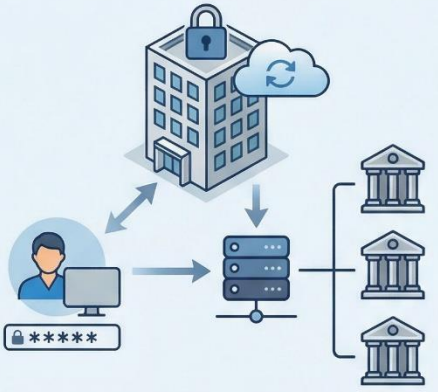
Centralised Exchanges (CEX) and Decentralised Exchanges (DEX)

A centralised exchange (CEX) is a platform operated by a company. The company manages the system, keeps records, and often holds users' assets on their behalf. Users create accounts, log in with passwords, and rely on the platform for customer support. This setup feels similar to using a bank or mobile money service.

A decentralised exchange (DEX) operates without a single company controlling it. Transactions happen directly between users through digital systems. Users connect their own wallets and keep control of their assets. While this gives more independence, it also means users are responsible for their own security and cannot rely on customer support if something goes wrong.

VIRTUAL ASSET PLATFORMS & INTERMEDIARIES

CENTRALIZED EXCHANGES (CEX)



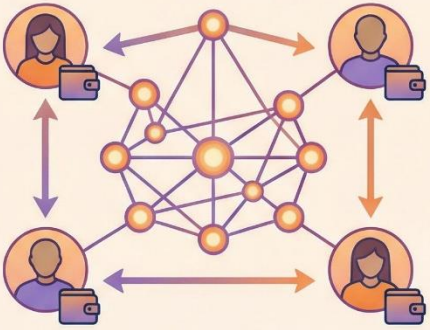
COMPANY MANAGED

USER ACCOUNTS & SUPPORT

ASSETS HELD ON BEHALF

RELIANCE ON PLATFORM SECURITY

DECENTRALIZED EXCHANGES (DEX)



USER-CONTROLLED

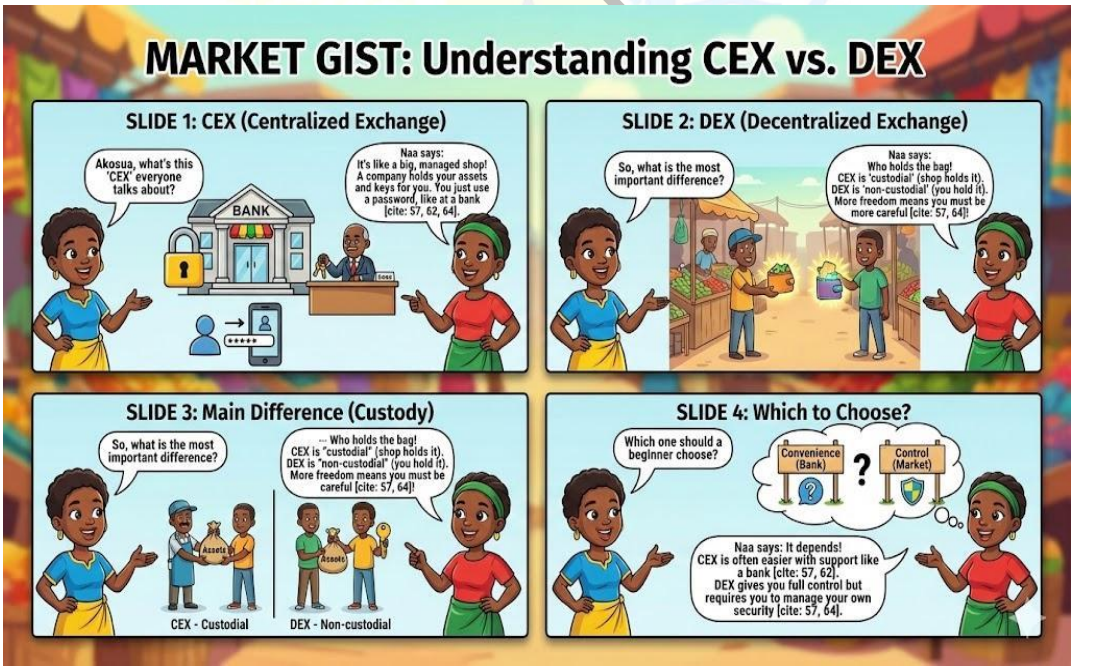
DIRECT TRANSACTIONS

SELF-CUSTODY WALLETS

USER RESPONSIBLE FOR SECURITY

Understanding different platforms helps users choose safe options and know their responsibilities.


CENTRALIZED EXCHANGE
(CEX)
EXCHANGE TYPES COMPARED
DECENTRALIZED EXCHANGE
(DEX)
COMPANY OPERATED PLATFORM
ASSETS HELD ON BEHALF
COMPANY MANAGES SYSTEM
USERS CREATE ACCOUNTS
CUSTOMER SUPPORT
Company holds assets, manages system. Bank-like feel. Customer support available. [cite: 57]
ADINKRAHENE (LEADERSHIP)
NKYINKYIM (VERSATILITY)
DIRECT USER-TO-USER TRANSACTIONS
USERS CONNECT OWN WALLETS & KEEP CONTROL
NO CUSTOMER SUPPORT. SELF-SECURITY RESPONSIBILITY.
Direct user-to-user, no central control. Users hold their own keys. Self-security required, no support. [cite: 57]

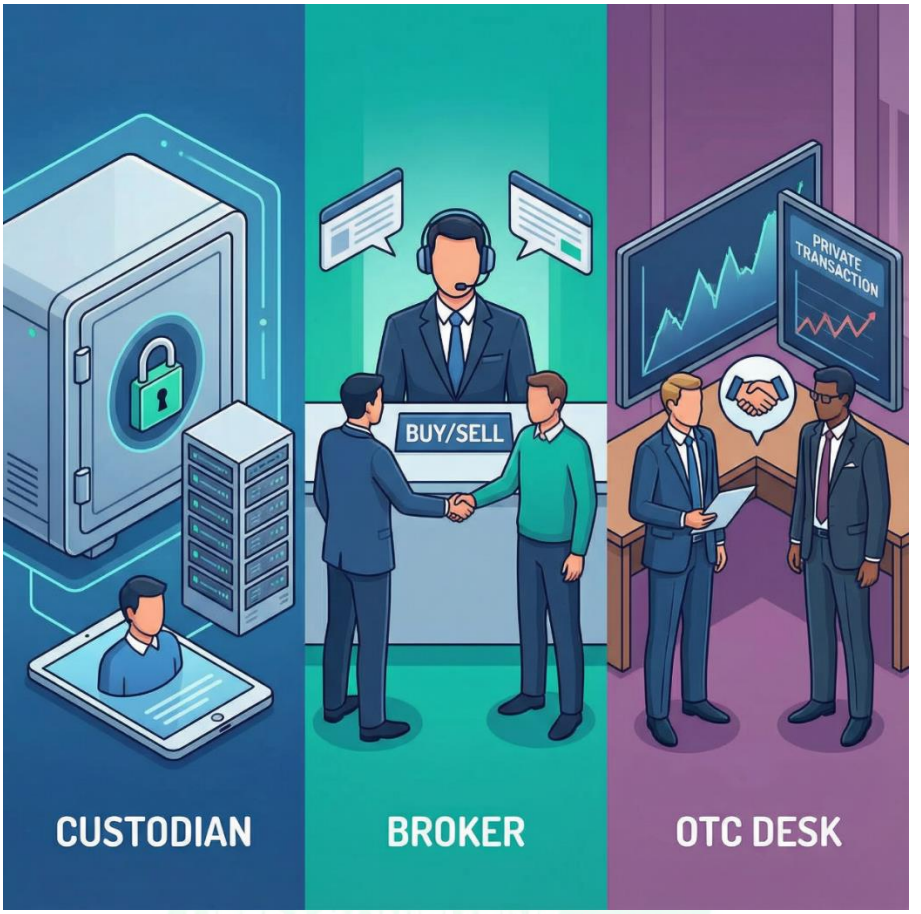

MARKET GIST: Understanding CEX vs. DEX
SLIDE 1: CEX (Centralized Exchange)
Akosua, what's this 'CEX' everyone talks about?
BANK
Naa says: It's like a big, managed shop! A company holds your assets and keys for you. You just use a password, like at a bank [cite: 57, 62, 64].
SLIDE 2: DEX (Decentralized Exchange)
So, what is the most important difference?
Naa says: Who holds the bag! CEX is 'custodial' (shop holds it). DEX is 'non-custodial' (you hold it). More freedom means you must be more careful [cite: 57, 64]!
SLIDE 3: Main Difference (Custody)
So, what is the most important difference?
Who holds the bag! CEX is "custodial" (shop holds it). DEX is "non-custodial" (you hold it). More freedom means you must be careful [cite: 57, 64]!
Assets
CEX - Custodial
DEX - Non-custodial
SLIDE 4: Which to Choose?
Which one should a beginner choose?
Convenience (Bank)
?
Control (Market)
Naa says: It depends! CEX is often easier with support like a bank [cite: 57, 62]. DEX gives you full control but requires you to manage your own security [cite: 57, 64].

Custodians, Brokers, and Over-the-Counter (OTC) Desks

A custodian is a service provider that holds and safeguards virtual assets on behalf of users. The custodian manages security and storage, while users access their holdings through that provider. This reduces the burden on users but requires trust in the provider. A custodian keeps users' digital assets safe, like a secure storage facility.

A broker acts as a middleman, helping users buy or sell virtual assets. The broker finds a buyer or seller and completes the transaction for a fee. Users do not usually trade directly with with one another..

An over-the-counter (OTC) desk handles large or special transactions outside regular exchanges. These desks are often used by institutions or individuals making high-value trades. OTC services aim to reduce price volatility and enhance privacy, but they require careful verification and strong due diligence..



On-Ramps and Off-Ramps (Fiat ↔ Virtual Asset)

On-ramps are services that allow users to convert fiat currency, such as cash deposits or bank funds, into virtual assets. This may involve bank transfers, mobile money, or card payments.

Off-ramps allow users to convert virtual assets back into fiat currency . These services are essential because they connect virtual assets with everyday financial systems. Using trusted on-ramps and off-ramps helps ensure smooth and lawful transactions.

On-Ramps, Off-Ramps, and Payment Connectivity in Ghana

User Responsibilities, Licensing, and Due Diligence

Users have responsibilities when using platforms and intermediaries. They should check whether a platform is licensed or approved by the relevant authority. Licensing shows that the provider meets basic standards and follows rules designed to protect users.

Due diligence means taking time to verify information before using a service. This includes checking the platform's name, contact details, reputation, and guidance from official sources. Users should also protect their own passwords and keys, understand fees, and avoid rushing into unfamiliar services.

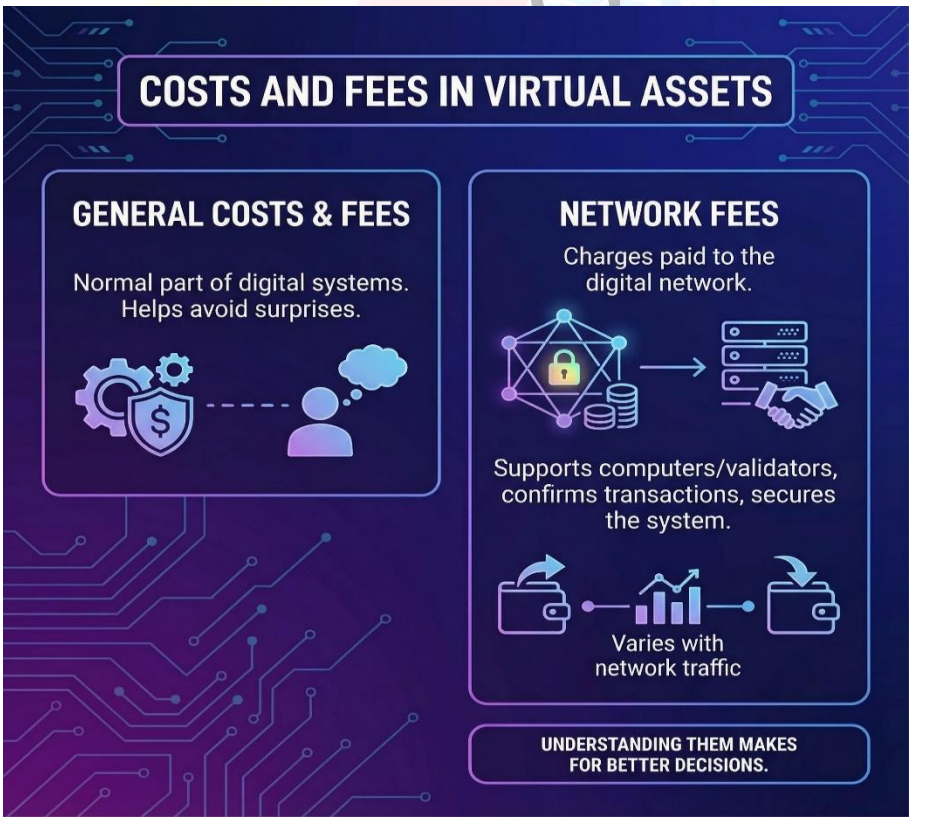
Choosing the right platform and understanding these roles helps reduce risk and supports safer participation in virtual asset activities.

SECTION 4: Costs and Fees

When using virtual assets, users often incur various fees. These costs are a regular part of how digital systems operate. Understanding them helps users avoid surprises and make better decisions.

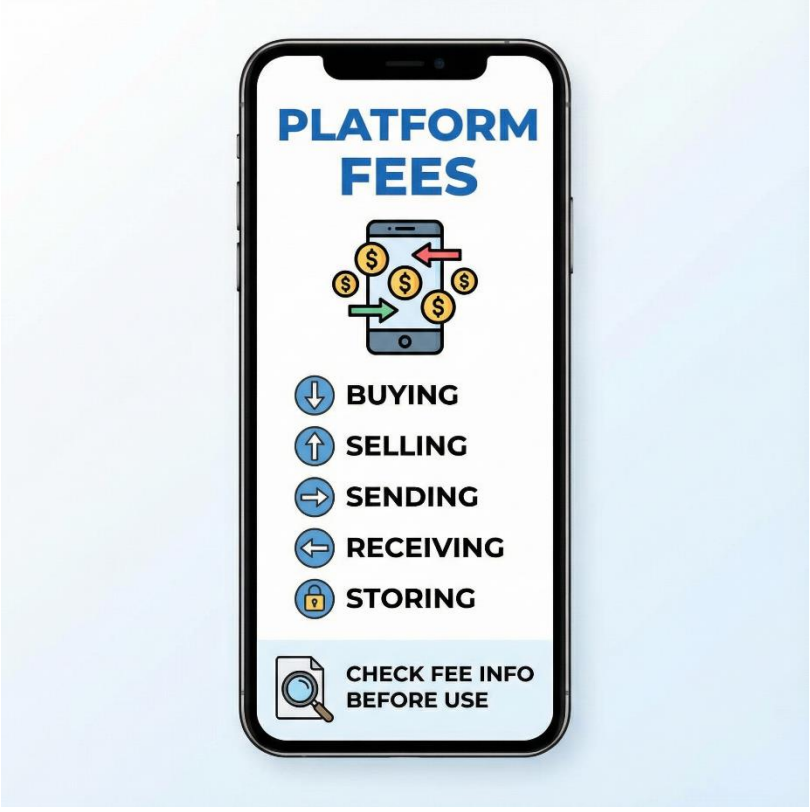
Network Fees

Network fees are charges paid to the digital network that processes and records transactions. These fees support network operations, including validators that confirm transactions and keep the system running securely. Network fees usually appear when sending virtual assets from one wallet to another. The amount can change depending on how busy the network is at that time.



Platform Fees

Platform fees are charges set by the service or app being used. These may include fees for buying, selling, sending, receiving, or storing virtual assets. Some platforms also charge fees for customer support or special services. Users should always check the platform's fee information before using the service



Spreads

A spread is the difference between the buy and sell prices of a virtual asset on a platform. Even when no separate fee is shown, the platform may earn money through this price difference. Spreads are typical on

exchanges and broker platforms and can affect how much value a user receives.

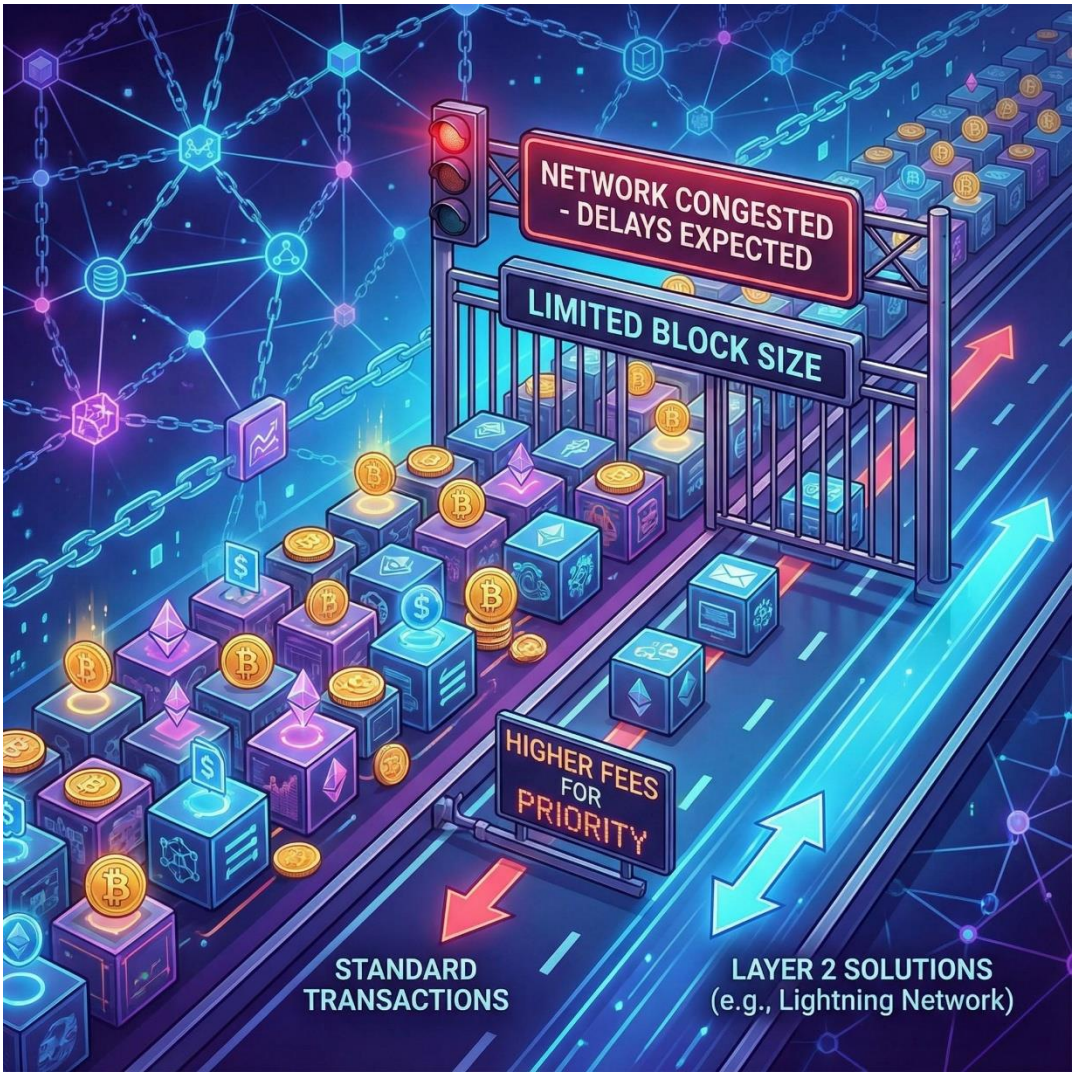
Blockchain Congestion and Transaction Delays

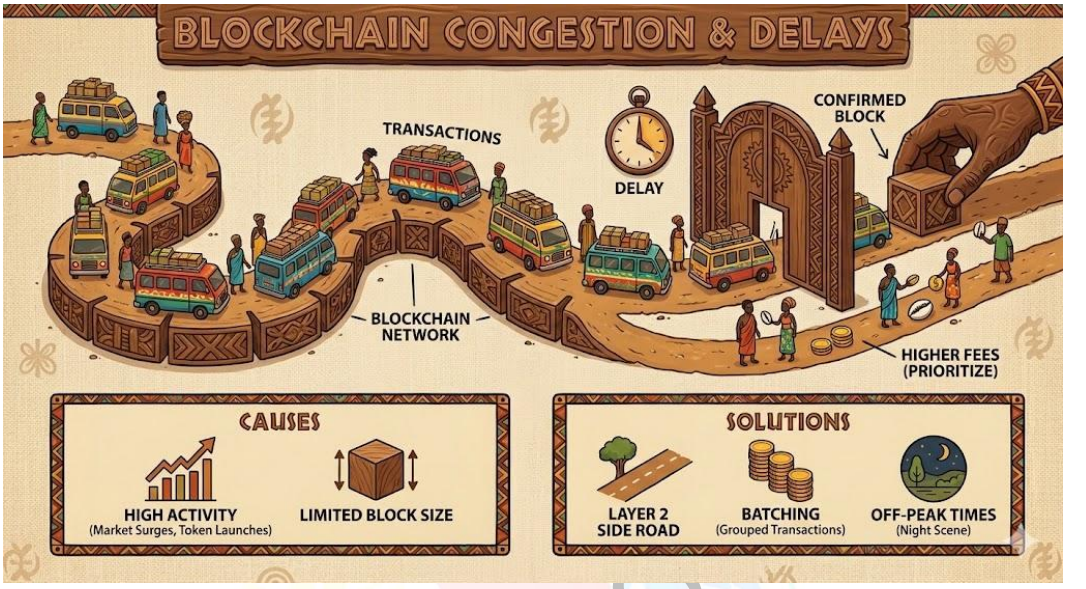
What is Blockchain Congestion?

Blockchain congestion occurs when too many users try to send transactions simultaneously through a blockchain network. Just as traffic on a busy road causes delays, this overload does too. When the network is congested, transactions take longer to be confirmed because only a limited number can fit into each block, which is added at fixed intervals.

As a result, users may experience slower processing times and may be required to pay higher fees to prioritise their transactions. These delays can affect the speed of sending or receiving funds, which is especially frustrating during urgent transfers. Congestion is most common on public blockchains such as Bitcoin and Ethereum, particularly during periods of high activity, including market surges, popular token launches, and NFT launches.

The technical reasons behind congestion include limited block size, fixed block time, and the consensus mechanisms used to validate transactions. To reduce congestion, developers are exploring solutions such as Layer 2 technologies (e.g., Lightning Network or rollups), increasing block capacity, batching transactions more efficiently, and encouraging users to transact during off-peak hours.


NETWORK CONGESTED
- DELAYS EXPECTED
LIMITED BLOCK SIZE
HIGHER FEES
FOR
PRIORITY
STANDARD
TRANSACTIONS
LAYER 2 SOLUTIONS
(e.g., Lightning Network)



SECTION 5: Operational Safeguard Principles

Operational safeguards are practical actions that help protect virtual assets from loss, theft, or misuse. These safeguards focus on how users manage access, confirm transactions, and stay alert to common threats.

Backup and Secure Storage of Keys and Seed Phrases
Keys and seed phrases are critical for accessing and recovering virtual asset wallets. Users should write down their seed phrases clearly and store them in a safe place that is not easily accessible to others. They should avoid storing seed phrases in plain texton phones, share them through messages, or give them to anyone. Keeping a secure backup ensures that assets can be recovered if a phone or device is lost or damaged.

Multi-Factor Authentication (MFA) and Secure Password Practices
Multi-factor authentication adds an extra layer of protection by requiring more than one form of verification, such as a password plus a code sent

to a phone. Where available, users should activate this feature. Passwords and PINs should be strong and not easy to guess. Avoid using personal information such as birthdays, names, or simple number patterns. Passwords should be kept private and changed if there is any suspicion of exposure.

Testing Small Transactions Before Large Transfers

Before sending a large amount of virtual assets, users should first send a small test transaction. This helps confirm that the recipient details are correct and that the transaction process works as expected. Once the small amount is received successfully, the larger transfer can be made with greater confidence. This practice reduces the risk of permanent loss due to errors.

Awareness of Phishing, Fake Websites, and Social Engineering

Phishing messages, fake websites, and social engineering attacks are common ways scammers trick users into giving up access details. These may appear as urgent messages, fake support requests, or official-looking links. Users should be cautious with unexpected messages, avoid clicking unknown links, and verify information through trusted channels.

Device Security and Safe Usage Habits

Users should keep their phones and computers locked at all times and avoid leaving devices unattended. Software updates should be installed when prompted, as updates help fix security weaknesses. Apps should only be downloaded from trusted sources. Avoid using public or shared devices for wallet access “where possible.

Regular Review of Wallet Activity

Users should regularly check their wallet activity and transaction history. Early detection of unfamiliar transactions allows quicker

response and reporting. Ignoring small, unusual activity can lead to larger losses later.

Knowing When and Where to Seek Help

If something looks wrong, users should stop immediately and avoid further actions. Assistance should be sought from trusted platforms, licensed service providers, or relevant authorities. Early reporting increases the chances of limiting damage and protecting others. Following these operational safeguard principles helps users maintain control over their assets, reduce exposure to risks. It also supports the use of virtual asset systems more safely and responsibly.


SECURE KEY STORAGE:
Backup & Keep Offline
MULTI-FACTOR AUTH (2FA):
Enable Extra Layer
SEEK TRUSTED HELP:
Report Suspicious Issues
OPERATIONAL SAFEGUARDS
TEST SMALL TRANSACTIONS:
Verify Before Large Sends
REGULAR REVIEW:
Check Activity Often
AVOID PHISHING:
Be Cautious of Scams
DEVICE SECURITY:
Update & Use Safe Habits

SECTION 6: Regulatory Tools

Know Your Customer (KYC) and Customer Due Diligence (CDD)
KYC and CDD are essential tools used by financial institutions and virtual asset service providers to verify user identities and assess potential risks.

- **KYC** involves collecting basic personal information, such as name, address, and ID number, to confirm who a person is before they can use financial services.
- **CDD** goes a step further by evaluating the customer's background, source of funds, and transaction behaviour to detect suspicious activity or prevent fraud.

These tools help protect the financial system from misuse, including money laundering and terrorist financing.


Regulatory Tools
Know Your Customer (KYC) and Customer Due Diligence (CDD)
KYC and CDD involve Identity verification and risk assessmennt
Digital Identity Verification with Ghana Card
Modern systems integratewith national databases like the Ghana Card.
Transaction Monitoring, Blockchain Analytics, and Risk Alerts
Simple explanation of transaction mointoring, blockchain analytics, and risk alert setup

Ghana Digital Identity Verification with Ghana Card

Modern systems now integrate digital identity verification with national databases, such as the **Ghana Card**. This means:

- Users can verify their identity online using biometric or ID number checks.
- Service providers can instantly confirm a person's identity without manual paperwork.
- It improves speed, accuracy, and trust in onboarding processes.

This integration supports secure access to virtual asset platforms while aligning with national regulations.

Transaction Monitoring, Blockchain Analytics, and Risk Alerts

To maintain safety and compliance, service providers use advanced tools to monitor blockchain activity:

- *Transaction Monitoring* tracks how funds move across the network, flagging unusual patterns.
- *Blockchain Analytics* helps trace the origin and destination of virtual assets, even across multiple wallets.
- *Risk Alert* automatically notifies providers when suspicious behaviour is detected, such as large transfers, rapid movements, or links to blocked addresses.

These tools help regulators and platforms respond quickly to threats, protect users, and maintain trust in the system.

SECTION 7: Security and Risk Management Tools

Cybersecurity Basics for Individuals

Cybersecurity for individuals means taking consistent but straightforward steps to protect devices, accounts, and virtual assets from theft or misuse. Because virtual assets are accessed through phones or computers, keeping these devices secure is essential.

Individuals should lock their devices with a PIN, password, or biometric option and avoid sharing access with others. Devices should be kept up to date to promptly fix security weaknesses. Users should avoid using public or shared devices to access wallets and be cautious when using public Wi-Fi networks. These basic habits reduce the risk of unauthorised access.

Smart Contract Auditing and Awareness of Common Vulnerabilities

Smart contract auditing is the process of reviewing these programmes for errors or weaknesses before they are widely used. For individuals, a basic level of awareness is often sufficient. Users should understand that not all smart contracts are safe and that poorly written ones can be exploited. Warning signs include projects launched without clear information, a lack of review by trusted parties, or promises of guaranteed returns linked to automated contracts.

Individuals should prefer platforms and services that clearly explain how their systems work and that have undergone proper review. Avoid interacting with unfamiliar or unverified smart contracts.

Recovery Planning for Virtual Assets

Recovery planning is about preparing for situations where access to a wallet or device is lost. This includes phone loss, device damage, or forgotten passwords.

Users should securely store recovery information, such as seed phrases or backup keys, in a separate, safe place away from their device. This

information should never be shared and should not be stored openly on phones or online platforms. For custodial wallets, users should understand the service provider's recovery process. For non-custodial wallets, recovery depends entirely on having the correct backup information.

Having a clear recovery plan helps users regain access to their assets and reduces panic or loss during unexpected events.

Assessment Strategy: Scenario-Based Task

Scenario-Based Task 1: Choosing the Right Wallet and Custody Option
Akosua wants to start using virtual assets for small online payments. She finds two options:

- A wallet offered by a well-known platform that keeps assets for users and helps with password recovery.
- Another wallet that gives her complete control but requires her to manage private keys and seed phrases herself.

She is unsure which one to choose and plans to use the wallet regularly.

Task for Learners

- Identify whether each wallet is custodial or non-custodial.
- Explain the difference between hot wallets and cold wallets in this context.
- Discuss the trade-off between convenience and security for Akosua.
- Recommend the most suitable option and justify the choice.

Learning Focus
Access and custody concepts, wallet types, and security responsibility.

Scenario-Based Task 2: Sending Funds, Fees, and Platform Choice
Scenario
Kojo wants to send virtual assets to a supplier using a platform he saw advertised online. The platform claims to charge "zero fees" and promises fast transactions. Kojo notices that the asset's purchase and sale prices differ, and the platform is not clearly listed as licensed in Ghana.

Task for Learners

- Identify the types of fees or costs involved, including network fees, platform fees, and spreads.
- Explain how blockchain congestion might affect transaction speed and cost.
- Identify platform and intermediary risks present in the scenario.
- Outline the steps Kojo should take before using the platform.

Learning Focus
Costs and fees, spreads, platform risks, and due diligence.

Scenario-Based Task 3: Security Incident and Recovery Planning
Scenario
Efua uses a wallet on her phone to store virtual assets. One day, she receives a message asking her to click a link to "secure her wallet." After clicking, she notices an unfamiliar transaction in her wallet history. She is unsure what to do next.

Task for Learners
- Identify the cybersecurity risks and red flags in the scenario.
- Explain the role of phishing and fake links in such incidents.
- List the immediate steps Efua should take to protect her assets.
- Describe how recovery planning and regulatory reporting can help resolve the issue.

Learning Focus
Cybersecurity basics, operational safeguards, incident response, and regulatory tools.

Assessment Guidance

Learners may complete these tasks through:

- Group discussion
- Short written analysis
- Facilitated presentations

Assessment should focus on reasoning, application of concepts, and safe decision-making, rather than memorisation of technical terms.

Module 3

Module Title: Markets and Consumer Risks

Module Purpose: Frame the principal risk domains and prevalent abuse patterns and set out a high-level pathway for prevention, response, and escalation consistent with good consumer-protection practice

Module Learning Outcomes

a. Classify key risk types relevant to users, firms, and the wider system
ii. Recognise hallmark indicators of fraud and misconduct without typologies
iii. Describe general pre-engagement behaviours that reduce exposure to harm
iv. Outline a high-level incident-response and escalation pathway, including evidence preservation

SECTION 1: Understanding Risk Areas

Risks linked to virtual assets appear at different levels. Some risks affect individual users, others affect service providers, and some involve the wider system. Understanding these risk areas helps people act carefully and reduce possible losses.

User-Level Risks

User-level risks arise from personal actions, mistakes, or a lack of awareness. These risks are common and often result in direct losses.

- ✓ Losing passwords or private keys. Passwords, PINs, and private keys control access to virtual assets. If they are lost or forgotten, the user may permanently lose access to their assets. If they are shared, others may take control of the wallet.

- ✓ Sending money to the wrong address. Virtual asset transactions are usually irreversible. Sending money to the wrong phone number or wallet address can result in permanent loss.
- ✓ Platforms shutting down without warning. Some platforms may stop operating suddenly due to technical problems, legal issues, or fraud. Users may lose access to funds if they rely on unsafe or unverified services.
- ✓ Criminals tricking people into sharing information. Scammers often use messages, calls, or fake websites to trick users into sharing passwords, PINs, or recovery details.
- ✓ Impersonation of support staff. Criminals may pretend to be customer support agents or officials. Once trusted, they request sensitive information and steal assets.

Firm-Level Risks

Firm-level risks relate to how service providers operate and manage their systems.

- ✓ Poor internal systems. Weak processes, poor recordkeeping, or a lack of clear procedures increase the risk of errors or losses.

- ✓ Weak safety controls. Firms that fail to invest in adequate security measures expose users to theft, hacking, and data leaks.
- ✓ Cyberattacks. Platforms may be targeted by hackers seeking to steal funds or user information. Poorly protected systems are more vulnerable.
- ✓ Failure to follow anti-money laundering and counter-terrorist financing requirements (AML/CFT). Firms that ignore compliance rules risk sanctions, shutdowns, or loss of trust. This can disrupt services and affect users.

System-Level Risks

System-level risks affect the broader virtual asset ecosystem and can affect many users simultaneously.

- ✓ Sharp price changes. Some virtual assets experience rapid price fluctuations, leading to unexpected losses.
- ✓ Low liquidity on some platforms. Platforms with low trading activity may make it difficult to buy or sell assets quickly without losing value.

- ✓ Dependence on a few custodial services. When many users rely on a small number of service providers, the failure of one provider can affect a large number of people.
- ✓ Weak supervision of cross-border activity. Virtual assets often cross borders, making oversight difficult. Weak coordination between authorities can increase risk.

Understanding these risk areas helps users recognise where problems can arise and why caution, verification, and safe practices are necessary when dealing with virtual assets.

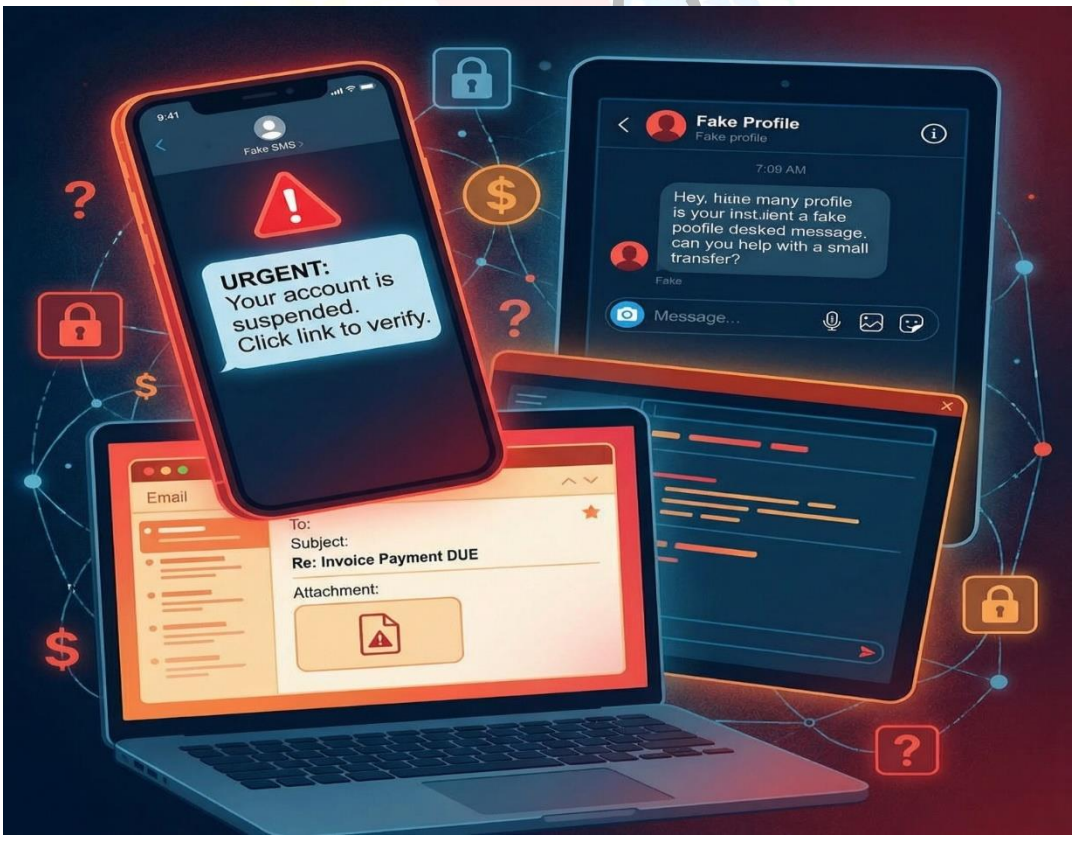

SYSTEM-LEVEL RISKS IN VIRTUAL ASSETS
SHARP PRICE CHANGES
Rapid, unpredictable value shifts leading to unexpected losses
LOW LIQUIDITY ON PLATFORMS
Difficulty buying/selling quickly without value loss due to low trading activity
WIDER ENVIRONMENT IMPACT
DEPENDENCE ON CUSTODIAL SERVICES
Failure of a few key providers affects many users relying on them
WEAK CROSS-BORDER SUPERVISION
Difficult oversight of assets moving across borders; weak authority coordination

SECTION 2: Common Abuse and Misconduct

Abuse and misconduct in virtual asset systems often exploit trust, urgency, and a lack of information. These activities are designed to deceive users and cause financial loss. Recognising common forms of misconduct helps users pause and avoid harmful decisions.

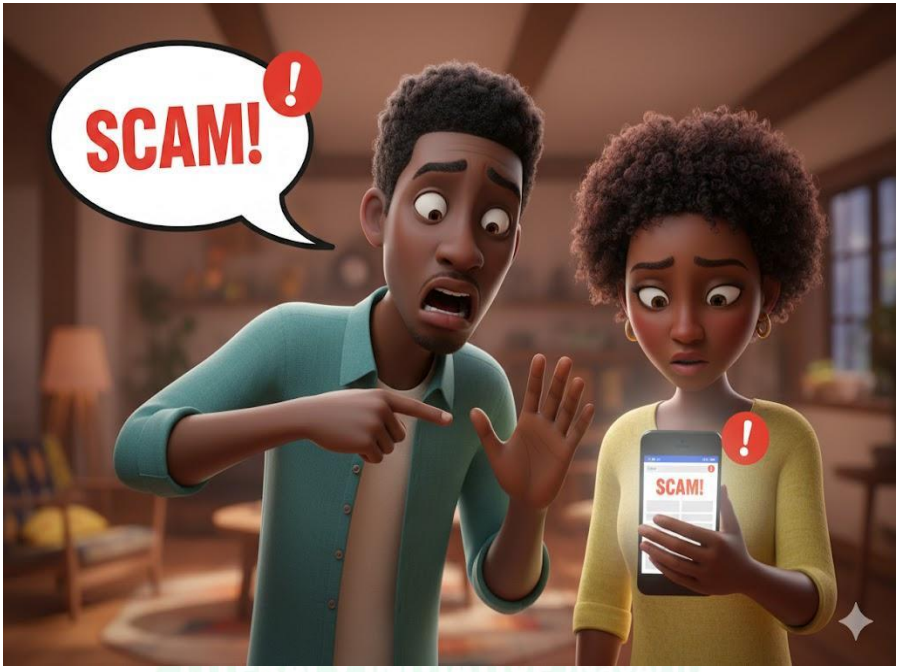
Fraud and Phishing Messages

Fraud and phishing messages are among the most common abuses. These messages may arrive through SMS, email, WhatsApp, or social media. They often ask users to click a link, send money, or share passwords and wallet details. Messages may appear urgent or official, but they aim to steal information or funds.



Platforms That Look Real but Are Copies

Fake platforms are designed to copy real websites or apps. They use similar names, colours, and layouts to confuse users. Once money is sent to these platforms, it is usually impossible to recover. These fake platforms may disappear suddenly after collecting funds.



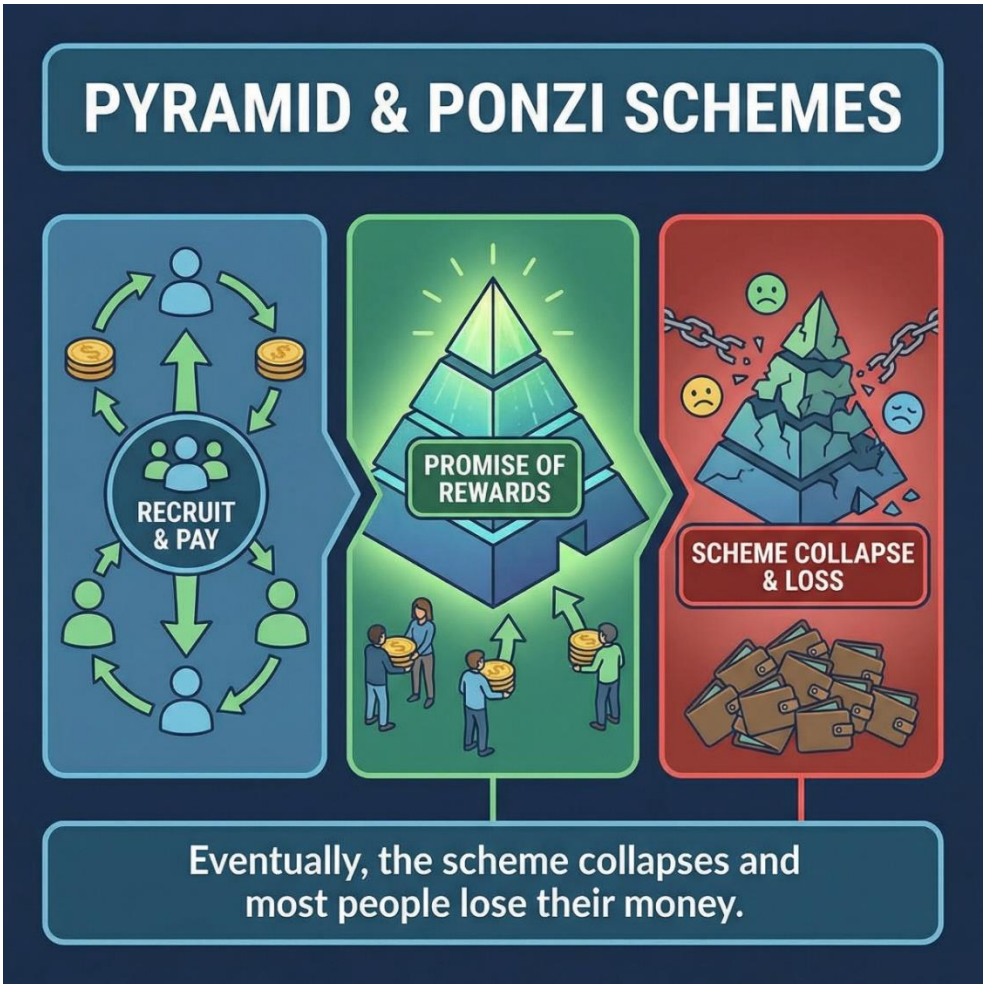
Impersonation of Banks, Security Agencies, or Trusted Figures

Some criminals pretend to represent banks, regulators, security agencies, or well-known individuals. They may use logos, names, or copied messages to appear legitimate. Once trust is gained, they request sensitive information or money. This form of impersonation is particularly dangerous because it exploits authority and familiarity.


IMPERSONATION
FRAUD

Ponzi and Pyramid Schemes

Ponzi and pyramid schemes promise high returns with little effort. Participants are asked to send money and recruit others. Early participants may receive small payouts from new members' funds, but the scheme eventually collapses. Most people lose their funds when recruitment slows or stops.



Groups Offering Quick Profits

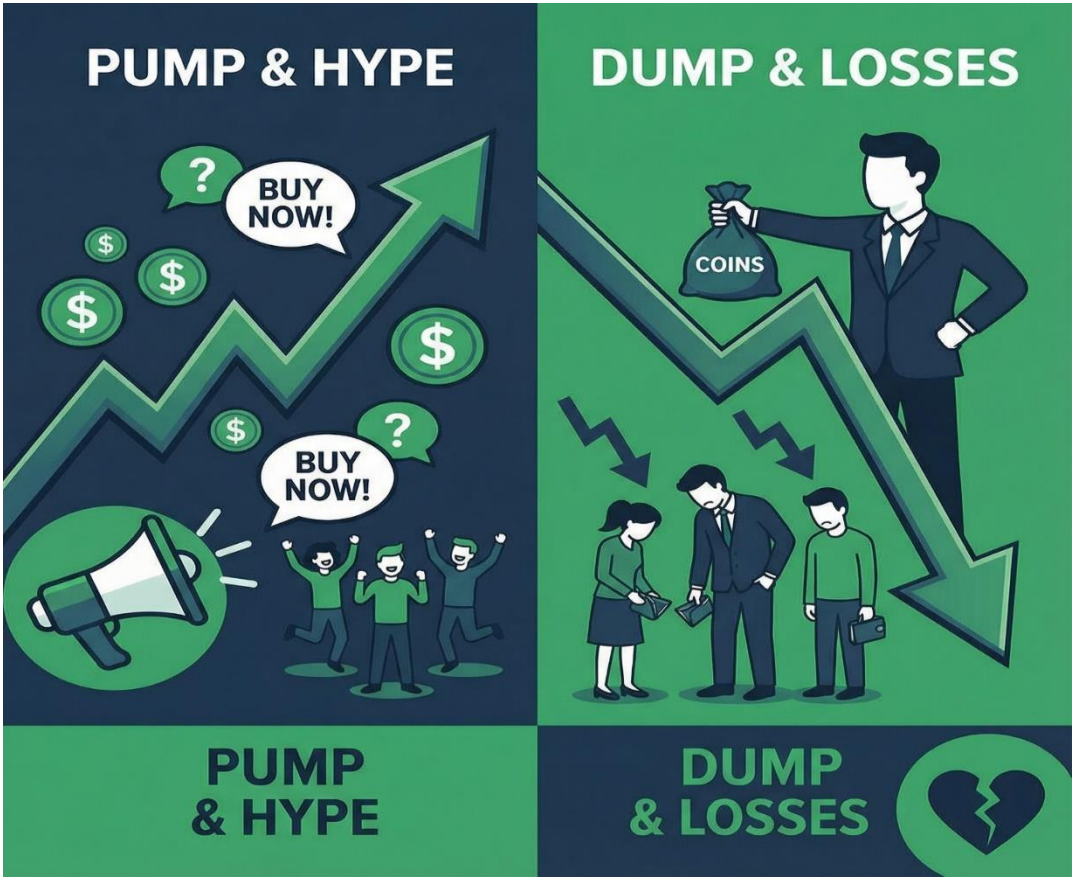
Some online groups promote fast-profit opportunities tied to virtual assets. These groups often pressure members to act quickly and discourage questions. Claims of guaranteed or risk-free returns are common signs of misconduct.

Sudden Removal of Funds on Fake Projects

In some cases, projects collect money from users and then suddenly withdraw all funds. This happens when the people behind the project abandon it after raising enough money. Users are left with worthless assets or no access to their funds.

Pump-and-Dump Activities

Pump-and-dump schemes involve artificially inflating the price of a virtual asset through hype and false information. Once many people buy in, the promoters sell their holdings quickly. The price then drops sharply, causing losses for others.



Understanding these forms of abuse and misconduct helps users identify warning signs, avoid rushing into decisions, and protect themselves from financial harm.

SECTION 3: Safe Behaviours Before Any Engagement

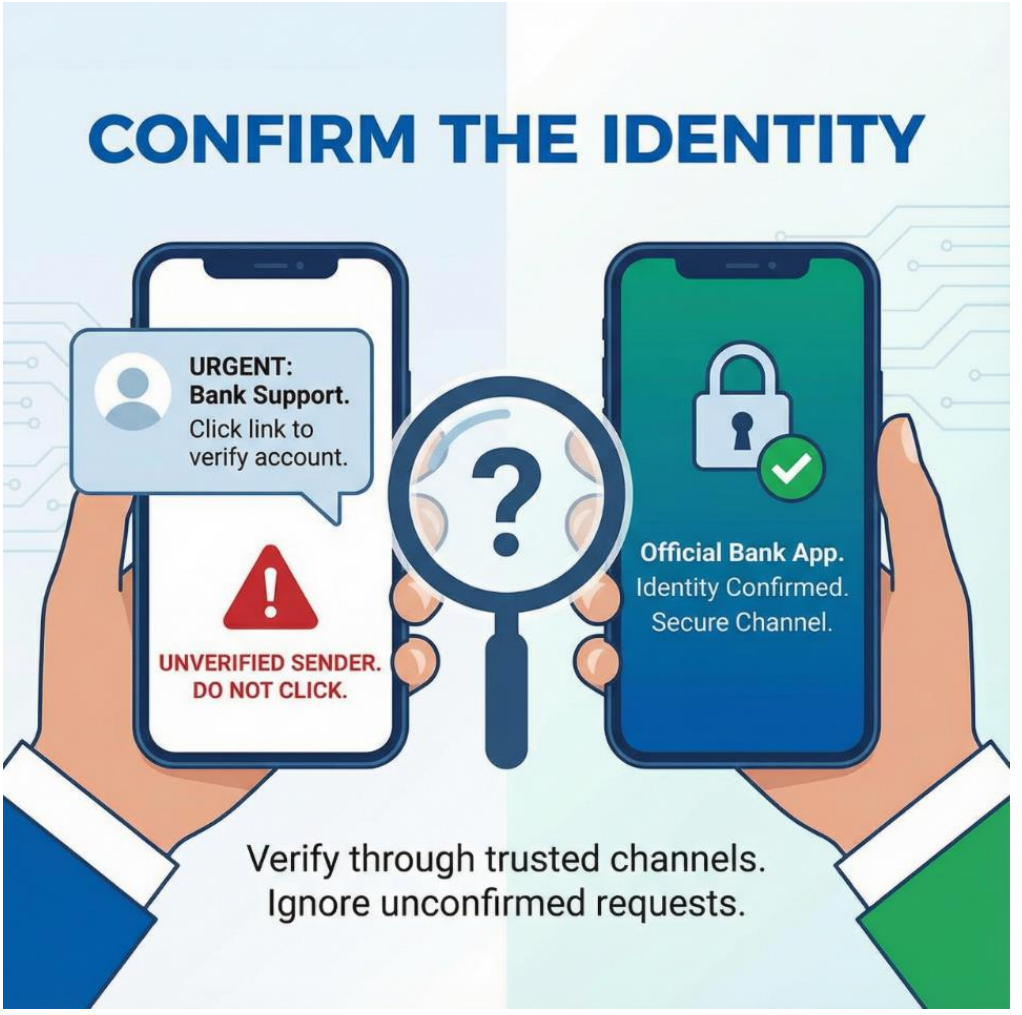
Before using any virtual asset service or responding to offers, it is essential to take simple but deliberate steps. These actions help prevent loss and reduce exposure to fraud or misuse.

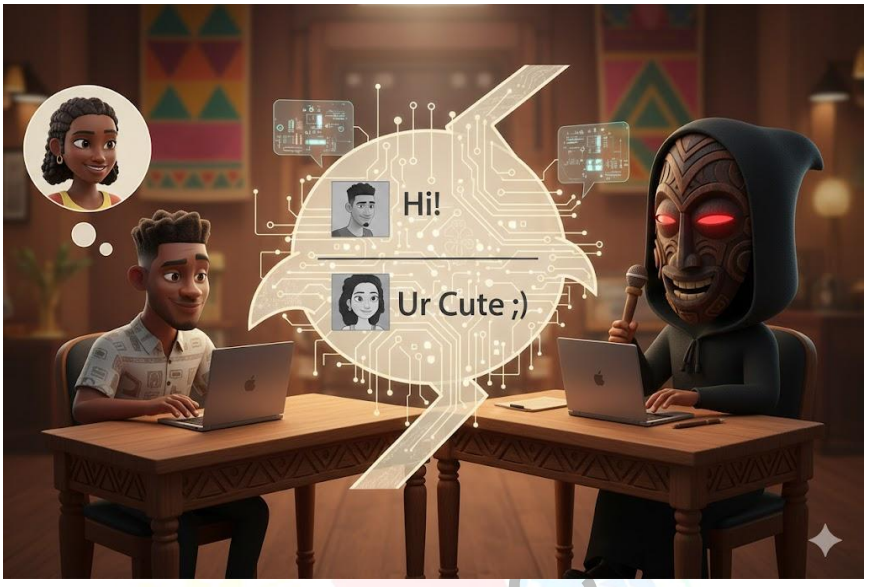
Check Whether a Platform Is Licensed in Ghana

Before using a platform or app, users should confirm that it is licensed or approved by the appropriate regulatory authority in Ghana. Licensed platforms are expected to meet basic security, record-keeping, and customer protection standards. Using unlicensed platforms increases the risk of loss if the service fails or disappears.

Confirm the Identity of the Person Contacting You

Users should always verify who they are dealing with. Messages claiming to come from banks, agents, support teams, or officials should be treated with caution. If the identity cannot be confirmed through trusted channels, the request should be ignored. Never rely solely on names, profile pictures, or voice messages.





Use Small Test Transfers Before Sending Larger Amounts

When sending virtual assets to a new address or person, users should start with a small test transfer. This confirms that the address is correct and that the transaction process works as expected. Larger transfers should only be made after the test is successful.

Turn On Two-Factor Authentication

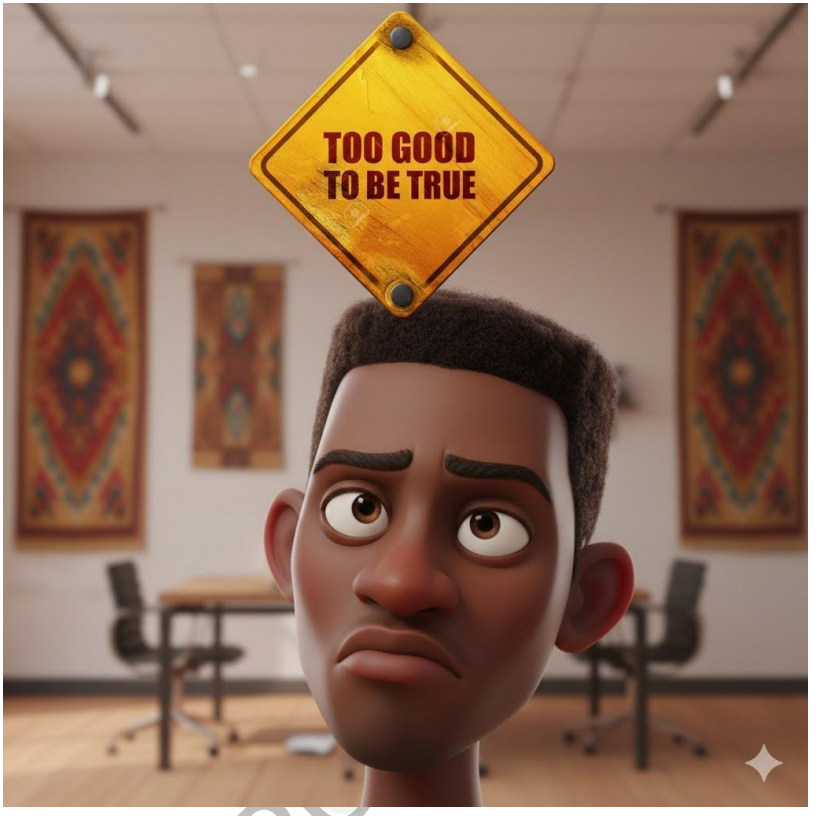
Where available, users should activate two-factor authentication. This adds an extra layer of security by requiring a second step, such as a code sent to a phone, in addition to a password or PIN. This makes it harder for unauthorised persons to access the wallet.

Use Strong Passwords and Keep Devices Safe

Passwords and PINs should be strong and not easy to guess. Personal information such as names, birthdays, or simple number patterns should be avoided. Devices should be locked at all times and kept secure. Apps should only be installed from trusted sources, and software updates should be applied promptly.

Take Time to Understand the Risk

Users should never rush into virtual asset transactions or offers. Taking time to read information, ask questions, and understand potential risks helps prevent mistakes. Any offer that pressures users to act quickly or promises guaranteed returns should be treated as a warning sign.



SECTION 4: Basic Cybersecurity Skills

Basic cybersecurity skills help protect virtual assets, personal information, and devices from theft or misuse. These skills focus on everyday habits that reduce risk and improve safety.

Use Strong Passwords and Change Them When Needed

Passwords should be strong and difficult to guess. Avoid using simple numbers, names, or dates of birth. If there is any suspicion that a password has been seen or exposed, it should be changed immediately. Strong passwords make it harder for unauthorised people to access accounts or wallets.

Avoid Sharing Passwords with Family or Colleagues
Passwords, PINs, private keys, and recovery phrases should never be shared, even with trusted family members or coworkers. Sharing access details removes personal control and increases the risk of loss, whether by mistake or misuse.

Turn On Two-Factor Authentication on Important Apps
Two-factor authentication adds an extra security step beyond a password. It may require a code sent to a phone or generated by an app. Turning this on helps block access even if a password is compromised. All wallets, exchanges, and critical digital services should use this feature when available.

Keep Phones and Computers Updated
Software updates fix security weaknesses and improve protection against new threats. Users should allow updates when prompted and avoid delaying them. Unupdated devices are easier targets for attackers.

Install Trusted Antivirus Tools
Antivirus tools help detect and remove harmful software. Only trusted and well-known security tools should be installed. These tools add another layer of protection, mainly when devices are used for digital payments or wallet access.

Learn the Signs of Phishing and Fake Links
Phishing attempts often appear as unexpected messages that ask users to click links, share information, or act urgently. Fake links may look official but lead to false websites. Users should avoid clicking on unknown links and verify messages through trusted sources before responding.

Understand the Difference Between Custodial and Non-Custodial Wallets

In custodial wallets, a service provider helps manage security and recovery. In non-custodial wallets, the user is fully responsible for security and recovery information. Understanding this difference helps users understand where responsibility lies and how carefully they must handle access details.

Store Private Keys Safely

Private keys and seed phrases control access to virtual assets. They should be written down and stored in a secure, private place. They should never be stored openly on phones, sent through messages, or shared with anyone. Losing or exposing these details can result in permanent loss of assets.

SECTION 5: Steps to Take After a Problem Occurs

When a problem occurs with virtual assets, quick, calm action is essential. Following clear steps can limit damage and improve the chances of resolving the issue.

Stop Activity Immediately

As soon as something unusual is noticed, stop all transactions. Do not send more funds or click on any links. Pausing immediately helps prevent further loss.

Log Out and Disconnect Affected Devices

Log out of wallet apps, platforms, or accounts involved. If possible, disconnect the device from the internet to stop any ongoing unauthorised activity. Avoid using the device until security steps are taken.

Change Passwords

Change passwords and PINs for affected wallets, email accounts, and related services. Use strong and unique passwords. If two-factor authentication is available, ensure it is activated.

Save Evidence

Take screenshots of messages, transaction details, wallet activity, and any suspicious links. Record dates, times, amounts, and wallet addresses involved. This information is essential for investigation and reporting.

Report to the Platform

Contact the customer support of the wallet or platform used. Provide precise details and evidence. Reporting early increases the chance of assistance and helps the platform take action.

Report to Relevant Authorities

Severe cases should be reported to the appropriate authorities. These include the Police Cybercrime Unit, the Bank of Ghana, and the

Securities and Exchange Commission. Reporting helps protect others and supports enforcement action.

Follow Up Until the Case Is Closed

Do not assume the issue has been resolved after reporting. Follow up with the platform and authorities to track progress. Keep all communication records until the case is fully addressed.

SECTION 6: Understanding the Regulatory Space in Ghana

Ghana's regulatory framework helps guide how virtual asset activities are carried out and how users are protected. Understanding this space allows users to understand their rights, the responsibilities of service providers, and where to seek help.

Consumer-Protection Systems

Consumer-protection systems set expectations for how service providers should treat users. These systems require platforms to operate fairly, explain fees clearly, protect customer information, and respond to complaints. They are designed to reduce abuse and ensure users are not mistreated.

Licensing and Supervision of Service Providers

Virtual asset service providers are expected to hold the appropriate licences and operate under supervision. Licensing demonstrates that a provider has met specific requirements for security, operations, and governance. Supervision allows regulators to monitor activities and address risks as they arise. Using licensed providers reduces exposure to unsafe practices.

Role of Law Enforcement Agencies

Law enforcement agencies are responsible for investigating fraud, scams, theft, and other illegal activities linked to virtual assets. They work with regulators and service providers to trace wrongdoing and take action against offenders. Reporting suspicious activity helps these agencies protect the public.

The VASP Bill

The Virtual Asset Service Providers (VASP) Bill establishes a clear framework for the operation of virtual asset activities in Ghana. It outlines rules for licensing, supervision, and compliance. The bill

supports transparency, accountability, and coordination among regulators, service providers, and enforcement bodies.

Understanding this regulatory space helps users make informed choices, recognise approved services, and know where to turn when problems occur.

SECTION 7: Market-level and National Risks

Some risks associated with virtual assets affect not only individual users and single platforms but also the broader market and the national system. These risks can cause widespread loss, instability, or loss of public trust if not appropriately managed.

Market Manipulation
Market manipulation occurs when individuals or groups try to control prices unfairly. Wash trading happens when fake trades are created to make an asset look more popular than it really is. These practices mislead users and often lead to losses for ordinary participants.

Platform Failure and Contagion
When a central platform fails, its problems can spread to other platforms or users. If many people depend on a single service, its collapse can disrupt payment flows, access to funds, and confidence in the system. This is known as contagion risk and can disturb the broader market.

CyberAttacks and Hacks
Hackers may target service providers. Successful attacks can shut down platforms, delay transactions, or result in the theft of assets and user data. Large-scale hacks can affect many users simultaneously and erode trust in digital systems.

Insider Theft
Insider theft happens when people within a platform misuse their access to steal funds or data. This risk exists when internal controls are weak or oversight is poor. Strong governance and monitoring are needed to reduce this threat.

Illicit Finance and National Security Risks

Virtual assets may be misused for money laundering, terrorism financing, or attempts to avoid sanctions. These activities threaten national security and financial stability. Regulators and law enforcement agencies monitor such risks and work to prevent abuse through supervision, reporting, and enforcement.

Understanding market-level and national risks helps users see why regulation, oversight, and caution are necessary. These risks highlight the importance of responsible participation and strong institutional controls in the virtual asset space.

Assessment Strategy: Scenario-Based

Scenario-Based Task 1: Risk Identification and Classification
Scenario
A staff member uses a wallet app to send funds to a supplier. The staff member types the address quickly, sends the funds, and later realises the address was wrong. At the same time, the platform's support line is not responding, and rumours spread that the platform may shut down.

Task for Learners

- Identify and classify the risks in this scenario as user-level, firm-level, and system-level risks.
- Explain why the transaction error may lead to permanent loss.
- State two safe behaviours that should have been followed before sending.
- Recommend two immediate steps the staff member should take once the issue is noticed.

Learning Focus
Risk classification, user mistakes, platform failure risk, and response planning.

Scenario-Based Task 2: Scam Detection and Safe Behaviour Before Engagement
A worker receives a WhatsApp message claiming to be from a well-known institution. The message says: "Your wallet has been flagged. Click this link to verify now, or your account will be locked." A second message from a group chat promises "fast profit" if members send funds and invite others.

Task for Learners

- Identify the scam types involved and list the red flags in each message.
- Explain why impersonation and urgency are dangerous signals.

- Outline the safe behaviours the user should follow before taking any action.
- Recommend what to do if the user already clicked the link.

Learning Focus
Fraud recognition, phishing, impersonation, Ponzi patterns, and safe pre-engagement steps.

Scenario-Based Task 3: Cybersecurity, Incident Response, and Reporting Channels
A user notices unusual wallet activity after logging in on a shared office computer. The user also remembers entering a password while colleagues were nearby. The user suspects the account has been compromised and worries about losing funds.

Task for Learners
- Identify the cybersecurity weaknesses in the scenario.
- Explain how phishing, malware, or shared device use could contribute to the problem.
- List step-by-step actions the user should take immediately.
- Identify where the case should be reported and what evidence should be preserved.

Learning Focus
Cybersecurity basics, incident response steps, evidence preservation, and reporting paths.

Assessment Note
Learners can complete these tasks through short written responses, group presentations, or guided class discussion. Marking should focus on correct reasoning, safe decisions, and precise application of the module principles.

Module 4

Module Title: Law and Regulatory Perimeter (Policy-Neutral)

Module Purpose: Provide an overview of the VASP bill, high-level obligations and responsibilities of regulated entities and official expected recourse channels

Module Learning Outcomes

a. Identify, in broad terms, activities typically within the scope of virtual assets regulation
ii. Differentiate the authorisation of entities from the treatment of specific assets or offerings
iii. Summarise shared governance, conduct, and financial crime control expectations at a principal level
iv. Describe how to verify authorisation status and stay informed as policies and guidance evolve

SECTION 1: Why Regulation Exists

Regulation exists to guide how virtual asset activities should be carried out and to reduce harm to the public and the broader economy. Regulations ensure consumer protection, market integrity, financial stability, and the combating of illicit finance.

- ✓ Consumer protection means protecting users from fraud, scams, unfair fees, and poor service.
- ✓ Market integrity means keeping the market fair so people are not misled by fake information or manipulation.
- ✓ Financial stability means preventing virtual asset activity from creating serious problems for the financial system and the economy.
- ✓ Combating illicit finance means reducing the use of virtual assets for crimes such as money laundering or other illegal activity.

SECTION 2: Activities Typically in Scope

Some activities are regulated because they involve handling virtual assets for others or providing services to the public.

- ✓ Operation of Virtual Asset Service Providers (VASPs) includes running platforms or services that help people buy, sell, store, or transfer virtual assets.
- ✓ Exchange of Virtual Assets ↔ fiat and fiat ↔ Virtual Assets: Changing virtual assets into normal money, and changing one virtual asset into another.
- ✓ Transfer, custody, or administration of virtual assets: Transfer is sending virtual holdings from one person to another. Custody is holding virtual assets for someone else. Administration is managing accounts, wallets, or access on behalf of users.
- ✓ The VASPs also offer advocacy services to various stakeholders.

SECTION 3: Expectations for Licensed Entities

Regulation often focuses on the service provider rather than on approving every asset the provider offers.

- ✓ Licensing or registration applies to the entity. A provider must meet standards such as governance, security, customer support, and record keeping.
- ✓ Asset categorisation is separate. Different assets may be treated differently depending on their features and risk level.
- ✓ Key point for users. A licensed provider is expected to follow rules, but licensing does not mean every product is safe or risk-free.

SECTION 4: Consumer-Facing Protections and Recourse

Users should know what to do when problems occur and what information is needed to support a complaint.

- ✓ Complaint management through platforms. Users should report issues first to the platform's support service and provide full details.
- ✓ Official reporting channels. Serious issues or unresolved cases should be reported through official channels provided by regulators or law enforcement.
- ✓ Evidence needed for recourse. Transaction IDs, screenshots, messages, emails, phone logs, and any payment confirmations.
- ✓ How consumers access information and remedies. Through platform customer support, official registers, public notices, guidance statements, and reporting systems.

SECTION 5: How to Verify Authorisation and Stay Updated

Checking authorisation helps users avoid unsafe or fake platforms. These may include

- ✓ Public registers of regulators or central banks. Users can check official lists to confirm if a provider is authorised.
- ✓ Cross-checking entity details and URLs. Confirm the exact name of the provider and ensure the website or app link matches official information.
- ✓ Staying updated. Follow official announcements, public advisories, and guidance notes to stay informed about changes and warnings.

References

101 Blockchains (2023), *Hot wallet vs cold wallet* [Infographic]. 101 Blockchains. https://101blockchains.com/wp-content/uploads/2023/07/hot-wallet-vs-cold-wallet-1.png.

CFTE. (2023), *The 4 types of blockchain networks: Definitions, examples and comparison*. CFTE. https://blog.cfte.education/types-of-blockchain-networks/.

CFTE. (2023), *Types of digital assets explained with examples and use cases*. CFTE. https://blog.cfte.education/types-of-digital-assets-explained/.

Debut Infotech (2025), *What are utility tokens and how do they work?* Debut Infotech. https://www.debutinfotech.com/blog/what-are-utility-tokens.

Financial Action Task Force. (2021), *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers* [PDF]. FATF.

GeeksforGeeks. (2025), *Distributed ledger technology (DLT) in a distributed system*

Weston, G. (2023), *Hot wallet vs cold wallet - key differences*. 101 Blockchains. https://101blockchains.com/hot-wallet-vs-cold-wallet-key-differences/.

Appendices

The appendices relate to the following:

1. Key Laws and Regulations, and
2. National Contacts and Reporting Channels
3. Glossary and Key Terms

1. Key Laws and Regulations

This section lists the main legal instruments, guidelines, and policy documents that shape virtual asset activity in Ghana. Each entry includes a short description of its purpose and the agency responsible for enforcement. The appendix helps professionals locate the correct reference points when reviewing cases, advising institutions, or assessing compliance matters. The focus is on clarity, relevance, and ease of use.

Document / Instrument	Issuing Authority	Purpose & Key Provisions
Passed the Virtual Asset Service Provider (VASP) Act	Parliament of Ghana (Ministry of Finance)	Purpose: To provide a comprehensive legal framework for regulating Virtual Asset Service Providers (VASPs) in Ghana. Key Provisions: Defines VASPs, outlines licensing requirements, sets standards for consumer protection, AML/CFT compliance, governance, and reporting. Establishes

		supervisory powers for designated regulators.
Bank of Ghana (BoG) Notice on Crypto Assets (2022)	Bank of Ghana	Purpose: To warn the public and regulated financial institutions about the risks associated with cryptocurrencies and similar digital assets. Key Provisions: Clarifies that crypto assets are not legal tender in Ghana. Prohibits banks, SDIs, and payment service providers from facilitating crypto transactions. Warns the public of high risks.
Payment Systems and Services Act, 2019 (Act 987)	Bank of Ghana	Purpose: To regulate payment systems, services, and providers in Ghana. Key Provisions: Establishes BoG's oversight of payment systems (like GhIPSS). Provides a framework for licensing payment service providers, including those for electronic money (e-money).

Securities Industry Act, 2016 (Act 929)	Securities and Exchange Commission (SEC)	Purpose: To regulate the securities market in Ghana. Key Provisions: Defines securities, licenses market operators, and establishes rules for investor protection and market integrity.
Anti-Money Laundering Act, 2020 (Act 1044) & Ghana's AML/CFT Framework	Financial Intelligence Centre (FIC) / Bank of Ghana / SEC	Purpose: To prevent money laundering and terrorist financing. Key Provisions: Imposes Customer Due Diligence (CDD), record-keeping, and suspicious transaction reporting obligations on designated entities, which will include licensed VASPs.
Data Protection Act, 2012 (Act 843)	Data Protection Commission	Purpose: To protect the privacy of personal data. Key Provisions: Sets rules for the collection, use, and disclosure of personal information by data controllers.

2. National Contacts and Reporting Channels

This section provides official contact points for guidance, escalation, and reporting. It includes national hotlines, regulatory portals, agency email addresses, and institutional desks responsible for financial integrity, cybersecurity, consumer protection, and law enforcement. The appendix supports quick decision-making and timely reporting during investigations, supervisory work, or advisory assignments.

Institution / Agency	Relevant Department / Unit	Contact Purpose & Channels	Notes for Effective Engagement
Bank of Ghana (BoG)	FinTech & Innovation Office; Financial Stability Department; Consumer Protection Office.	Purpose: For inquiries and reporting related to licensed Payment System Providers, the eCedi, and general warnings on virtual assets. Channels: Website: www.bog.gov.gh Phone: +233 593974486	For virtual asset-specific issues, first check the website for public advisories. When emailing, be clear and concise, stating "Virtual Asset Query" in the subject line.
Securities and Exchange Commission (SEC) Ghana	Market Surveillance Department; Legal Department.	Purpose: For inquiries and reporting related to potential securities fraud and unlicensed investment schemes involving digital assets.	Report if you encounter an investment-like Virtual Asset product promising

		Website: www.sec.gov.gh Phone: +233 302 768 970 / 08001000	returns that is not licensed by the SEC.

General Advice for Reporting:

1. **Act Quickly**: The sooner you report, the better the chance of mitigating loss or preventing others from being victimised.

2. **Be Prepared**: Have all relevant details ready: dates, amounts, platform names, wallet addresses (cryptocurrency), transaction IDs, screenshots, and communication records.

3. **Follow Up**: Note your report reference number if given, and follow up if you have additional information.

GLOSSARY AND KEY TERMS

Module 1 Glossary: Virtual Assets – Concepts & Context

This module covers the fundamental concepts and the broader ecosystem of digital finance.

Term	Definition
Virtual Asset (VA)	A digital representation of value that can be digitally traded, transferred, or used for payment. It does not include digital representations of fiat currencies, securities, or other financial assets that are already regulated.
Cryptocurrency	A type of virtual asset that uses cryptography for security and operates on a decentralised network, typically a blockchain, independent of a central bank. (e.g., Bitcoin, Ethereum).
Blockchain	A distributed, immutable digital ledger that records transactions in a verifiable and permanent way. Data is stored in "blocks" that are linked together in a "chain."
Distributed Ledger Technology (DLT)	A broader term for technologies that distribute record-keeping across a network of participants. Blockchain is one type of DLT.
Bitcoin (BTC)	The first and most well-known cryptocurrency was created in 2009 by the pseudonymous Satoshi Nakamoto. It introduced the concept of a peer-to-peer electronic cash system.

Ethereum (ETH)	A decentralised, open-source blockchain with smart contract functionality. It is a platform for building decentralised applications (dApps) and is the native currency for that platform.
Stablecoin	A type of virtual asset designed to maintain a stable value relative to a specified asset, like the U.S. Dollar or gold (e.g., USDT, USDC).
Fiat Currency	Government-issued currency that is not backed by a physical commodity like gold, but rather by the trust in the government that issues it (e.g., USD, EUR, JPY).
Central Bank Digital Currency (CBDC)	A digital form of a country's fiat currency, issued and regulated by the central bank. It is a direct liability of the central bank, unlike decentralised cryptocurrencies.
Tokenisation	The process of converting rights to an asset into a digital token on a blockchain. This can represent anything from real estate and art to loyalty points.
DeFi (Decentralised Finance)	An ecosystem of financial applications built on blockchain networks that aim to recreate and improve upon traditional financial systems (like lending and borrowing) without central intermediaries.
CeFi (Centralised Finance)	Traditional financial services and institutions that are centralised, such as banks and centralised cryptocurrency exchanges (e.g., Coinbase, Binance).

Module 2 Glossary: Key Tools & Components

This module covers the essential technologies, platforms, and mechanisms for interacting with virtual assets.

Term	Definition
Wallet	A software programme or hardware device that stores the public and private keys used to interact with a blockchain, allowing users to send, receive, and monitor their virtual assets.
Private Key	A sophisticated form of cryptography that allows a user to access their virtual assets. It is a secret number that proves the right to spend the assets and must be kept secure.
Public Key	A cryptographic key that can be obtained and used by anyone to encrypt messages for the owner or verify digital signatures. Derived from the private key, it is often shared as a public address.
Public Address	An alphanumeric identifier that is derived from a public key, functioning like a bank account number for receiving virtual assets.
Seed Phrase (Recovery Phrase)	A series of words (usually 12, 18, or 24) generated by a wallet that can be used to recover all the private keys and addresses within that wallet. This is the most critical piece of information to back up securely.
Hot Wallet	A cryptocurrency wallet that is connected to the internet. While convenient for frequent transactions, it is more vulnerable to hacking than cold storage.

Cold Wallet / Cold Storage	A wallet that stores private keys completely offline, making it highly secure against online hacking attempts (e.g., hardware wallets like Ledger or Trezor, or paper wallets).
Cryptocurrency Exchange	A platform that allows customers to trade virtual assets for other assets, such as fiat money or other digital currencies. They can be centralised (CeFi) or decentralised (DeFi).
Smart Contract	Self-executing contracts with the terms of the agreement directly written into code. They automatically execute and enforce obligations when predefined conditions are met.
Consensus Mechanism	A fault-tolerant mechanism used in blockchain networks to achieve agreement on a single data value or the state of the network (e.g., Proof-of-Work, Proof-of-Stake).
Proof-of-Work (PoW)	A consensus mechanism (used by Bitcoin) that requires participants (miners) to solve complex mathematical puzzles to validate transactions and create new blocks. It is computationally intensive.
Proof-of-Stake (PoS)	A consensus mechanism (used by Ethereum) where validators are chosen to create new blocks based on the amount of cryptocurrency they "stake" or lock up as collateral. It is more energy-efficient than PoW.
Gas Fees	The transaction fees are required to successfully conduct a transaction or execute a smart contract on a blockchain network like Ethereum.

Module 3 Glossary: Market & Consumer Risks

This module covers the primary risks associated with investing in, holding, and transacting with virtual assets.

Term	Definition
Volatility	The statistical measure of the dispersion of returns for a given asset. Virtual assets are known for their extreme price volatility, with values that can swing dramatically in short periods.
Market Risk	The risk of investors incurring losses due to factors affecting overall market performance, primarily price volatility, is a concern in this context.
Liquidity Risk	The risk that an investor may not be able to buy or sell a virtual asset quickly enough to prevent a loss (or to make a profit) due to a lack of market participants.
Operational Risk	The risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events. This includes exchange hacks and wallet mismanagement.
Counterparty Risk	The risk that the other party in an agreement will not fulfil their obligation. In CeFi, this is the risk that an exchange or custodian becomes insolvent or engages in fraudulent activity.
Custodial Risk	The risk associated with entrusting a third party (e.g., an exchange) with holding one's private keys. "Not your keys, not your crypto" is a common adage highlighting this risk.

Scam / Fraud	Deceptive schemes are designed to deprive users of their virtual assets. Common types include Ponzi schemes, fake ICOs, and phishing attacks.
Phishing	A cybercrime where targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data, such as private keys or seed phrases.
Rug Pull	A type of scam in the DeFi space where developers abandon a project and run away with investors' funds, often after liquidity has been locked in a pool.
Smart Contract Risk	The risk is that a bug or vulnerability in a smart contract's code could be exploited, leading to the loss of locked funds.
Regulatory Risk	The risk that changes in laws or regulations could negatively impact the value or utility of a virtual asset. This includes the potential for bans or restrictive policies.
Systemic Risk	The risk of the collapse of an entire financial system or entire market, due to the interconnectedness of its participants. As the VA market grows, so does its potential for systemic risk.

Module 4 Glossary: Legal & Regulatory Definitions

This module covers the key legal terms, regulatory bodies, and compliance frameworks governing virtual assets.

Term	Definition
Anti-Money Laundering (AML)	A set of laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income.
Combating the Financing of Terrorism (CFT)	Policies and laws specifically designed to prevent, detect, and prosecute the financing of terrorist acts and organisations and often grouped with AML as AML/CFT.
Financial Action Task Force (FATF)	An intergovernmental organisation that sets international standards for AML/CFT. Its recommendations are highly influential in shaping national regulations for Virtual Asset Service Providers (VASPs).
Virtual Asset Service Provider (VASP)	A broad term defined by the FATF as any natural or legal person that conducts one or more of the following activities on behalf of another: exchange between VAs and fiat; exchange between VAs; transfer of VAs; safekeeping/administration of VAs; participation in financial services related to VA issuance/sale.
Travel Rule	An AML/CFT requirement, originally for banks, now applies to VASPs by the FATF. It mandates that VASPs transmitting funds over a certain threshold must share specific originator and beneficiary information with the next VASP in the chain.
Know Your Customer (KYC)	The process a business uses to verify its clients' identities. It is a critical component of AML frameworks and is commonly used by regulated exchanges.

Securities Law	Laws that govern the offer and sale of securities (e.g., stocks, bonds). A key legal question is whether a specific virtual asset qualifies as a "security" under laws like the U.S. "Howey Test".
Howey Test	A test created by the U.S. Supreme Court to determine whether a transaction qualifies as an "investment contract" and is therefore subject to U.S. securities laws.
MiCA (Markets in Crypto-Assets)	A comprehensive regulatory framework for crypto-assets in the European Union, aiming to provide legal clarity and consumer protection.
Financial Crimes Enforcement Network (FinCEN)	A bureau of the U.S. Department of the Treasury that collects and analyses information about financial transactions to combat domestic and international money laundering and other financial crimes.
Office of Foreign Assets Control (OFAC)	A U.S. agency that administers and enforces economic and trade sanctions. OFAC maintains a Specially Designated Nationals (SDN) list, with which U.S. persons are prohibited from transacting.
Licensing & Registration	Requirements imposed by national regulators (e.g., the NYDFS BitLicense in New York) for VASPs to legally operate within their jurisdictions often include rigorous AML/CFT and capital requirements.

BOOK SUMMARY

This book addresses virtual assets and digital value systems in public education and professional training. The subject matter focuses on explaining what virtual assets are and how they differ from traditional financial arrangements. The discussion places strong attention on understanding digital value, transaction processes, and the roles of users, platforms, and networks.

The book examines key concepts, including digital, virtual, and crypto assets. Core principles are explained and illustrated with practical examples that show how virtual asset systems operate in real-world situations.

Risk awareness forms a central theme. The content explains familiar sources of loss, including fraud, misleading investment claims, fake platforms, and technology failures. Consumer protection and safe behaviour are repeatedly emphasised, with guidance on verification, caution, and responsible decision-making.

Legal and policy considerations are also discussed. The book describes the regulatory scope in Ghana, emphasising the respective mandates of the Bank of Ghana and the Securities and Exchange Commission.

Practical application is emphasized throughout the text. Readers are guided through fundamental fact-checking methods. Scenario-based discussions and assessment activities enhance learning and reinforce safety messages.

In summary, the book presents a structured introduction to virtual assets as a socio-economic and technological phenomenon. The subject matter combines technical explanation, risk awareness, regulatory context, and practical guidance, with the overarching goal of strengthening literacy, reducing harm, and supporting informed engagement with digital financial tools in Ghana.

ISBN: 978-9988-41-655-3