EDUCATION MANUAL

National Virtual Assets Literacy Initiative (NaVALI)

Advanced Professional Literacy (APL)

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) and Frank Sekyere Tawiah, CFA

Manual Title
National Virtual Assets Education Manual

Programme Name
National Virtual Assets Literacy Initiative

Advanced Professional Literacy

By
Joseph Antwi Baafi (Ph.D), Eric Effah Sarkodie (Ph.D),
Pearl Seyram Kumah (Ph.D) and Frank Sekyere Tawiah, CFA

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).

Printed in Ghana.

Main Authors

Joseph Antwi Baafi (Ph.D)[1], Eric Effah Sarkodie (Ph.D)[1], Pearl Seyram Kumah (Ph.D)[2] and Frank Sekyere Tawiah, CFA[3]

[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
[3]Core Afrique Investment Ltd.

Contributors

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

Cover Design by: Evans Oppong

ISBN: 978-9988-41-654-6

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. Accurate knowledge has therefore become essential for safety, trust, and informed decision-making. The National Virtual Assets Literacy Initiative (NaVALI) 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 educational 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 leadership of the Bank of Ghana and the Securities and Exchange Commission 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 support 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, transferred, 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 clear, careful, and practical way, without pressure to adopt any digital system.

The primary audience for this manual relies primarily on spoken explanation, pictures, and practical demonstrations. Many participants have limited literacy, 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 the technology itself, but to build careful habits and awareness that reduce harm.

This manual reflects a strong 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 to the development of this manual. I encourage all participants to engage fully with the training and awareness sessions and to 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 grounded in the public interest. This training marks an important milestone in positioning Ghana as a trusted and progressive hub for digital finance in Africa.

James Kutse 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 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 ask questions whenever something is not understood.

iv. *Apply learning through practice*

Practical demonstrations and role-play activities should be carried out using simulated or minimal amounts. 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 contacts 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 precise national aim to strengthen understanding across all sectors. It equips professionals with the knowledge needed to interpret 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 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 group includes tech-savvy individuals with high institutional and professional literacy and strong analytical skills.

- Constituents include regulators, law-enforcement agencies, bank risk/compliance teams, auditors, policymakers, journalists, and legal professionals.
- They require a full spectrum understanding of virtual assets because their decisions influence supervision, enforcement, systemic stability, and public communication.
- Training includes topics such as regulatory perimeter, AML/Travel Rule, custody frameworks, chain analytics, etc., while avoiding any endorsement or investment content.

3. Learning Philosophy

This manual follows a learning approach that supports advanced professionals who must think clearly, evaluate evidence, and link concepts to real decisions. The goal is to move beyond surface explanations and provide space for structured analysis, practical reasoning, and informed judgment.

The programme encourages analytical learning where participants examine principles, break down processes, and weigh the implications of virtual asset activity for systems they help oversee. Sessions introduce concepts in a precise sequence, then guide participants to compare models, evaluate risks, and judge operational outcomes.

Case-based problem-solving is a core part of the approach. Real-world examples from Ghana and other jurisdictions illustrate how virtual assets shape finance, compliance, security, and public administration. Participants study each case, identify the turning points, and propose responses guided by their professional duties.

Policy interpretation is treated as a practical skill. The manual helps participants read rules, frameworks, and notices with attention to jurisdiction, scope, and intent. This strengthens their ability to offer advice, enforce standards, and design procedures aligned with national priorities.

The technical application is presented in simple steps throughout the modules. Participants work with tools, platforms, and data flows in a structured way, linking hands-on activity to broader governance and supervisory needs. The approach supports confident engagement with virtual assets while reinforcing safety, accountability, and professional responsibility.

Diagrams – the group can quickly grasp concepts and operational mechanisms through diagrams that mirror their potential real-world interactions. Diagrams depict “how things work" and "what the end user sees/does," and pose philosophical or strategic dilemmas to stimulate critical thinking among participants.

4. Programme Learning Outcomes

The aims are to achieve the following;

i. To increase awareness of the riskiness of 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 source feedback for incorporation into regulatory frameworks

MODULE STRUCTURE

Module 1

Model Title: Virtual Assets: Concepts and Context

Module Purpose

This module serves as the foundation of the NaVALI curriculum. It moves participants from zero knowledge to a functional understanding of what virtual assets are, how the underlying technology works, and the key components of the ecosystem, all within the context of Ghana's VASP legislation, which seeks to highlight the inherent riskiness of the emerging virtual asset ecosystem without stifling innovative and responsible usage and participation. Specifically, the module aims;

- To establish a clear, technically sound, and policy-neutral foundation on virtual assets and Distributed Ledger Technology (DLT), clarifying key terminology, scope, and practical relevance for Ghanaian professionals.
- To equip participants with the conceptual understanding needed to distinguish between virtual asset types, comprehend basic system mechanics, identify realistic applications, and correct common misconceptions, forming a risk-conscious basis for a safe and informed engagement.

Module Learning Outcomes

By the end of this module, participants will be able to:

1. Articulate core virtual assets concepts and terminology in a clear, policy-neutral manner.
2. Differentiate between major virtual asset categories (e.g., cryptocurrencies, stablecoins, eCedi, NFTs) at a conceptual level.

3. Describe, in principle, how distributed ledgers function and why their features (transparency, traceability) matter for users and markets.
4. Identify realistic application areas for virtual assets and DLT within Ghanaian sectors versus common misconceptions or overstated claims.

SECTION 1: Concept Overview

Evolution of Virtual Assets

i. The Journey of Money: A Series of Upgrades

- ✓ *Barter*: Direct trade (e.g., my cow for your grain). Problem: The "coincidence of wants" was rare and inefficient.
- ✓ *Commodity Money*: Using rare, desirable things like gold and silver. They were portable, durable, and had inherent value.
- ✓ *Representative Money*: Paper receipts (IOUs) that could be exchanged for a fixed amount of gold held in a vault. This was easier to carry.
- ✓ *Fiat Currency*: The paper receipts became the money itself, backed only by government decree and trust in the system (e.g., US Dollar, Naira).
- ✓ *Digital Fiat*: Today, most money is just digital entries in bank databases (e.g., Mobile Money, bank transfers). This is convenient but relies entirely on third parties.

ii. The Catalyst: The 2008 Global Financial Crisis

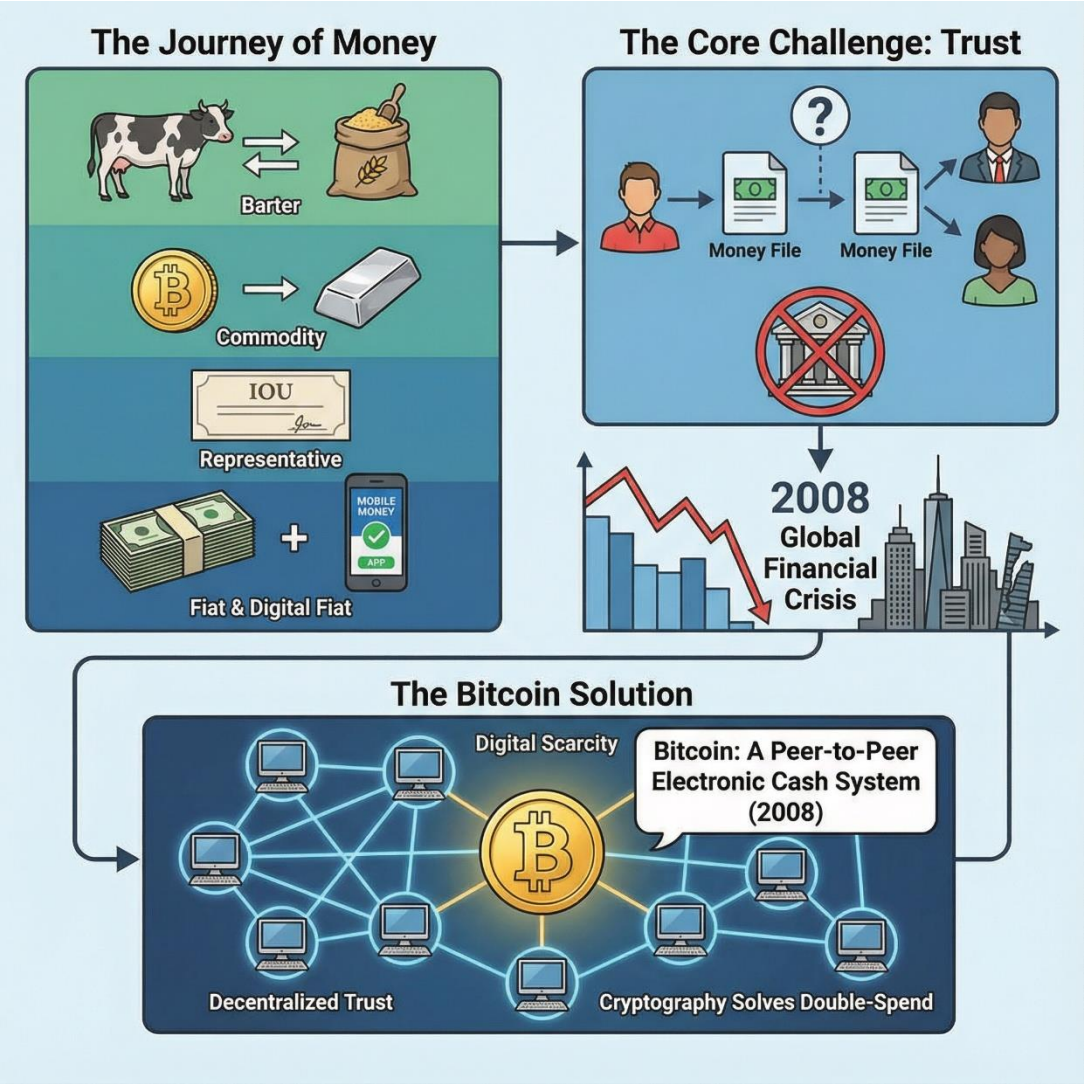
The global financial meltdown of 2008 shook public confidence in Wall Street and other central institutions. These entities had taken reckless risks that triggered a worldwide economic collapse, forcing governments in advanced economies to bail them out with taxpayer money. In the aftermath, a critical question arose: *Could we build a digital payment system that didn't depend on a fallible central intermediary?*

iii. The Bitcoin Solution: Digital Scarcity & Decentralised Trust

Later that same year, Satoshi Nakamoto introduced a groundbreaking idea in the whitepaper *"Bitcoin: A Peer-to-Peer Electronic Cash System."* The innovation was profound: Bitcoin created digital scarcity without a central authority, a kind of *digital gold*.

- ✓ New units are difficult and costly to produce, much like mining real gold.
- ✓ Bitcoins cannot be copied or duplicated.
- ✓ Ownership and transactions are validated not by a single company or government, but by a decentralised network of computers following a shared set of rules (a consensus mechanism).

This design solved the long-standing double-spend problem, the risk of spending the same digital money twice, not through trusted intermediaries like banks or payment processors, but through cryptography and a distributed consensus shared across thousands of machines worldwide.


The Journey of Money
Barter
Commodity
IOU
Representative
MOBILE MONEY
APP
Fiat & Digital Fiat
The Core Challenge: Trust
?
Money File
Money File
2008
Global
Financial
Crisis
The Bitcoin Solution
Digital Scarcity
Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
Decentralized Trust
Cryptography Solves Double-Spend

iv. The Core Challenge of Digital Money: Trust

- ✓ The Nature of Digital Files: When I email you a photo, I don't lose my copy; I still have the original. Digital information can be duplicated endlessly with copy-and-paste.
- ✓ The Double-Spend Problem: Now imagine trying to send digital money. How do we stop someone from sending the same "money file" to multiple people? This risk of duplication is known as the *Double-Spend Problem*.
- ✓ The Traditional Solution: For decades, we've relied on trusted intermediaries, banks, payment networks like Visa, or mobile money providers such as MTN. These institutions maintain a central ledger that records everyone's balances and verifies each transaction. Their oversight ensures that no one spends the same money twice.

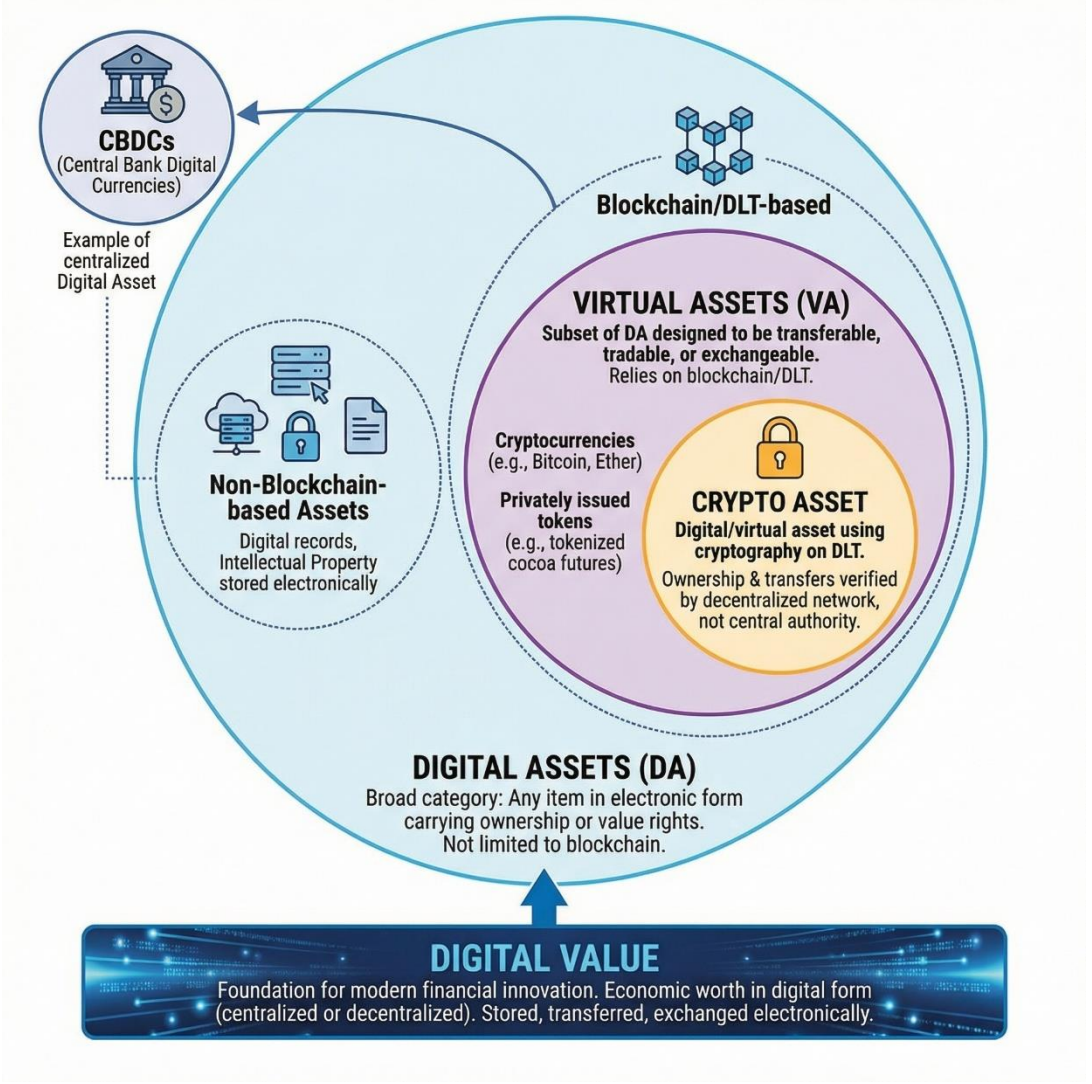
Core Concepts

Digital Assets (DA): A digital asset is any item that exists in electronic form and carries ownership or value rights. The broad category includes both blockchain-based and non-blockchain-based assets. Examples include Central Bank Digital Currencies (CBDCs), tokenised securities, digital records, and even electronically stored intellectual property. Digital assets are not limited to blockchain; they represent value or rights in digital form.

Virtual Assets (VA): A virtual asset is a subset of digital assets that is specifically designed to be transferable, tradable, or exchangeable in digital form. VAs rely on blockchain or Distributed Ledger Technology (DLT) to validate ownership and transactions. Examples include cryptocurrencies such as Bitcoin or Ether, privately issued tokens such as tokenised cocoa futures contracts traded on blockchain.

Digital Value refers to the economic value represented in digital form, whether centralised (such as CBDCs) or decentralised (such as cryptocurrencies). It can be stored, transferred, or exchanged electronically. Digital value underpins both digital assets and virtual assets, serving as the foundation for modern financial innovation.

A crypto asset is a digital or virtual asset that uses cryptography for security and exists on a distributed ledger technology (DLT), such as a blockchain. Ownership and transfers are recorded and verified on this decentralised network, not by a central authority.

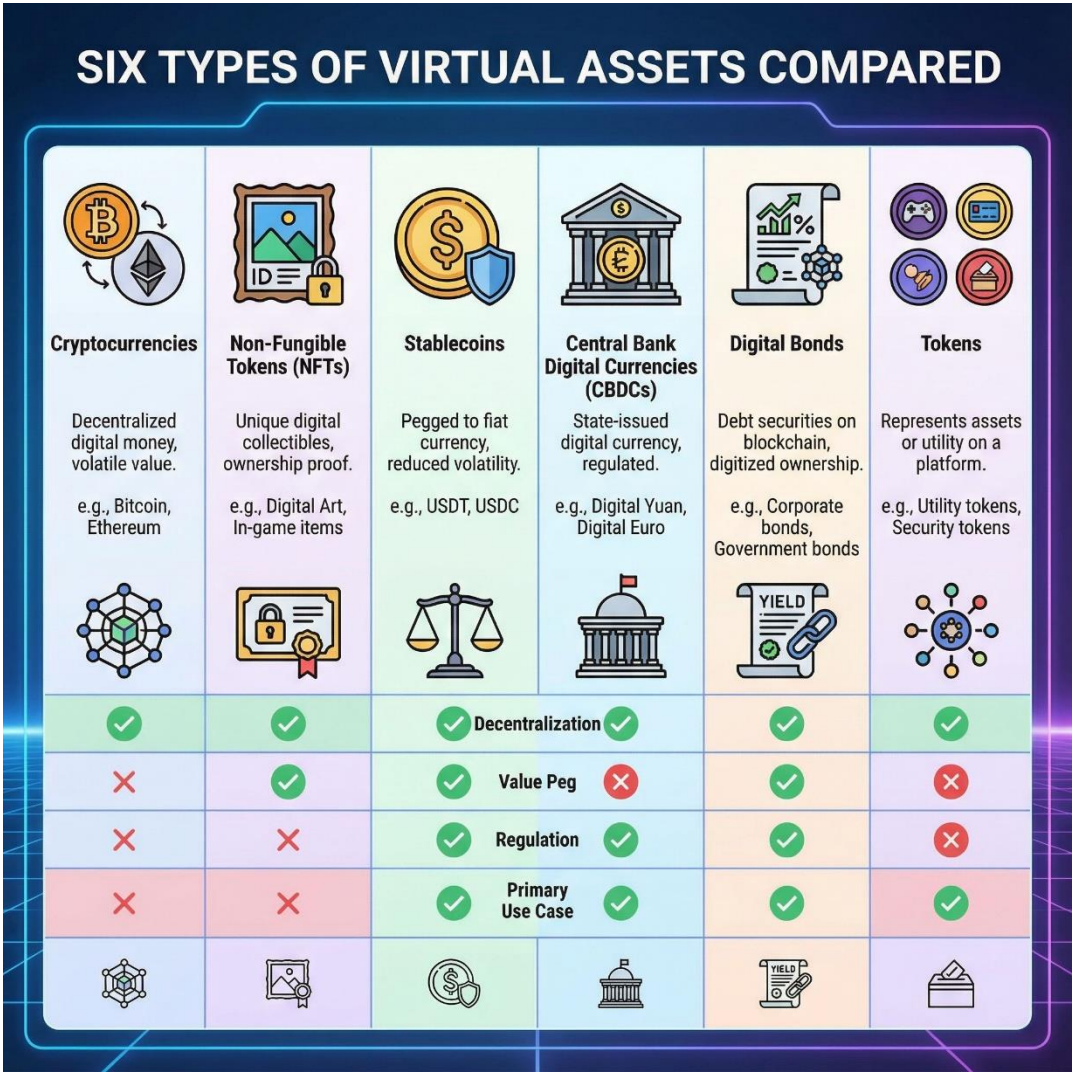

CBDCs
(Central Bank Digital Currencies)
Example of centralized Digital Asset
Blockchain/DLT-based
VIRTUAL ASSETS (VA)
Subset of DA designed to be transferable, tradable, or exchangeable.
Relies on blockchain/DLT.
Cryptocurrencies
(e.g., Bitcoin, Ether)
Privately issued tokens
(e.g., tokenized cocoa futures)
CRYPTO ASSET
Digital/virtual asset using cryptography on DLT.
Ownership & transfers verified by decentralized network, not central authority.
Non-Blockchain-based Assets
Digital records, Intellectual Property stored electronically
DIGITAL ASSETS (DA)
Broad category: Any item in electronic form carrying ownership or value rights.
Not limited to blockchain.
DIGITAL VALUE
Foundation for modern financial innovation. Economic worth in digital form (centralized or decentralized). Stored, transferred, exchanged electronically.

Difference Between Digital Assets, Virtual Assets and Crypto Assets

Aspect	Digital Assets (DA)	Virtual Assets (VA)	Crypto Asset
Scope	Broad category; includes blockchain and non-blockchain assets	Narrower subset; always blockchain/DLT-based	Assets that are 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)	Only 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, with specific

		AML/CFT implications.	AML/CFT implications.

Types of Virtual Assets



Distributed Ledger Technology (DLT)

Distributed Ledger Technology (DLT) is a digital system used to record transactions and data across multiple computers simultaneously. Instead of one central office or authority keeping the main record, every participating computer holds a copy of the same record. This shared setup ensures that all participants see the same information.

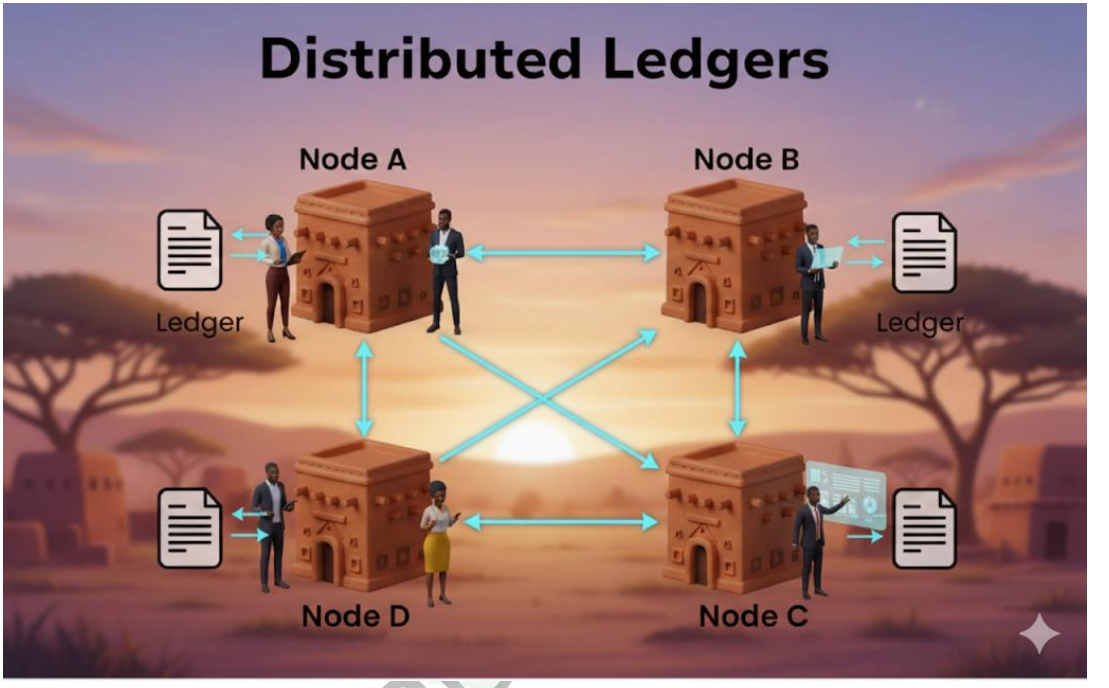
Because the record is shared, no single person or institution controls the data. When a transaction occurs, it is sent to the network of computers, often called a network of nodes. These nodes check the transaction using agreed-upon rules. Once verified, the transaction is added to the shared ledger and updated across all copies. This process makes the system decentralised.

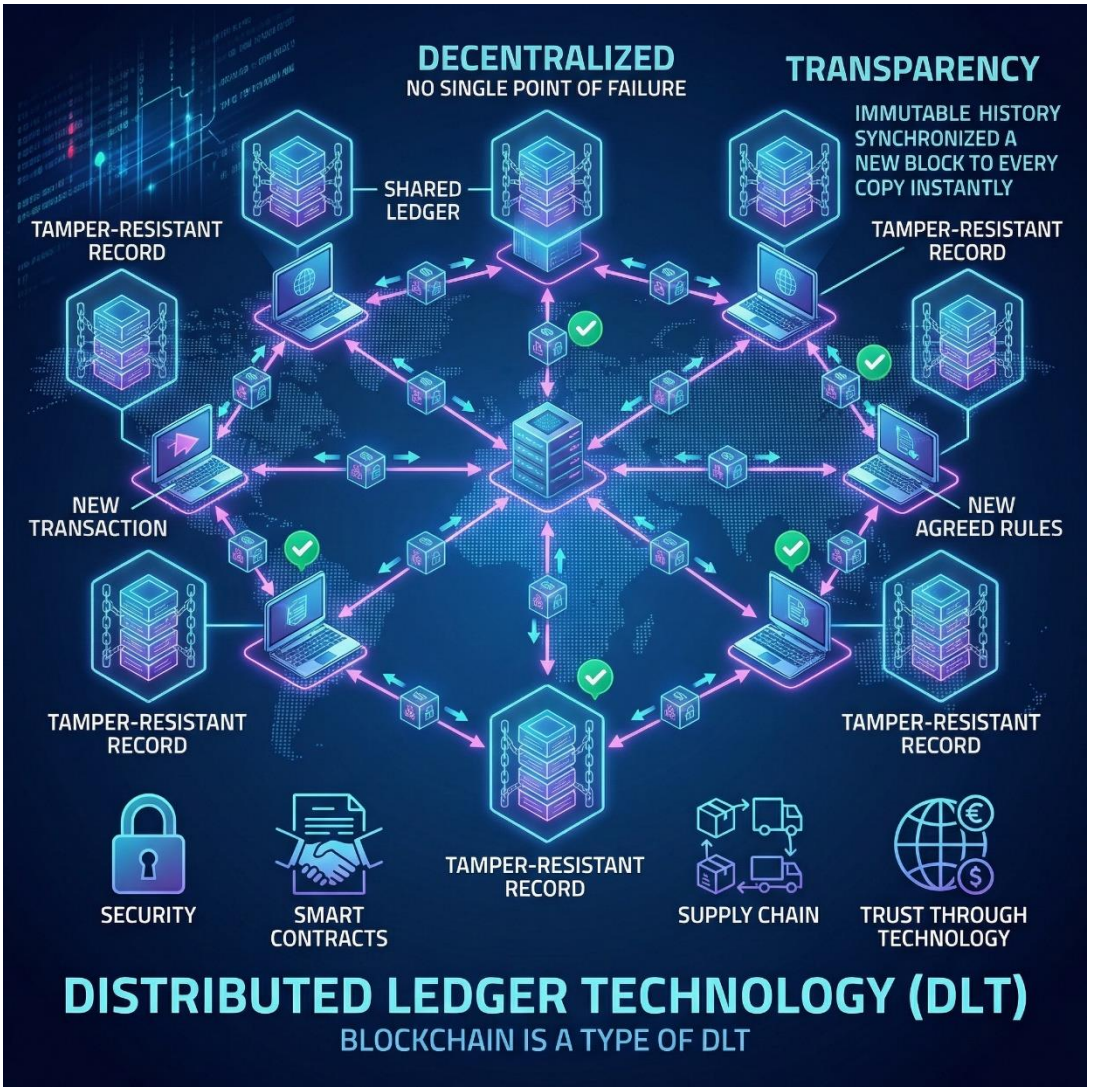
DLT improves transparency because transactions can be viewed and verified by permitted participants. Everyone relies on the same version of the truth, which reduces disputes and hidden changes. It also improves security because changing records would require altering many ledger copies at once, which is extremely difficult.

By eliminating the need for intermediaries such as banks or clearinghouses to confirm transactions, DLT reduces reliance on a single trusted middleman. Instead, trust is created through technology, shared rules, and agreement among participants. This makes the system more resilient to failure, manipulation, or single points of attack.

Once data is recorded on a distributed ledger, it is tamper-resistant. Records are not deleted or overwritten. New information is added in sequence, creating a clear history that can be checked later. This reliability makes DLT useful for virtual assets, payments, supply chains, records management, and other systems where accuracy and trust are essential.

Blockchain is one well-known example of a system built using Distributed Ledger Technology.




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

Understanding Blockchain

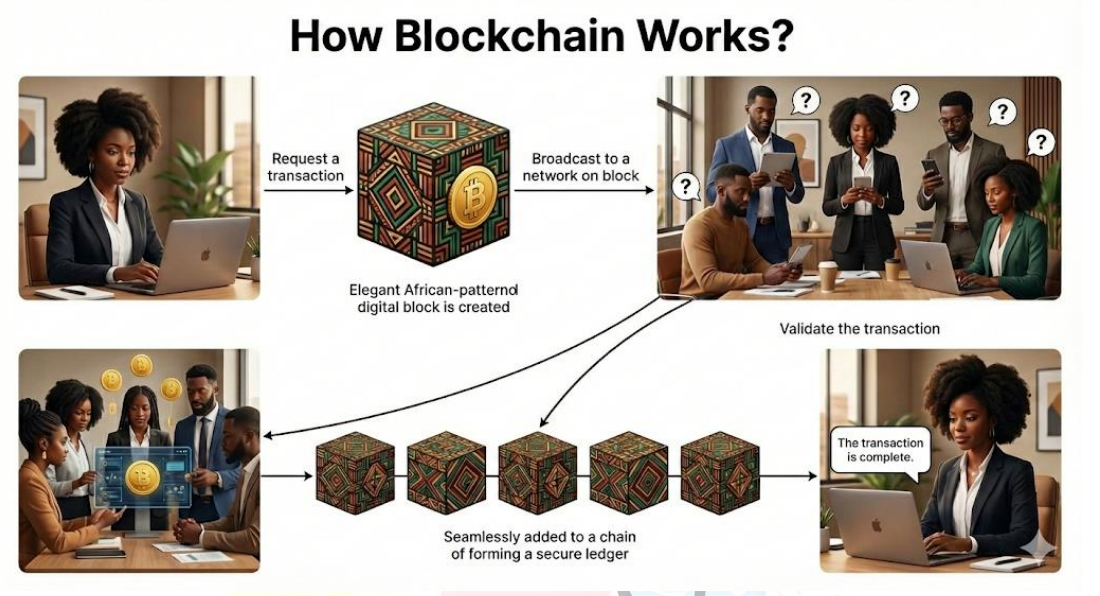
Blockchain is a type of Distributed Ledger Technology (DLT). This means it is one way of keeping shared digital records, but not the only way. Blockchain works like a shared record book that many people or systems can use simultaneously.

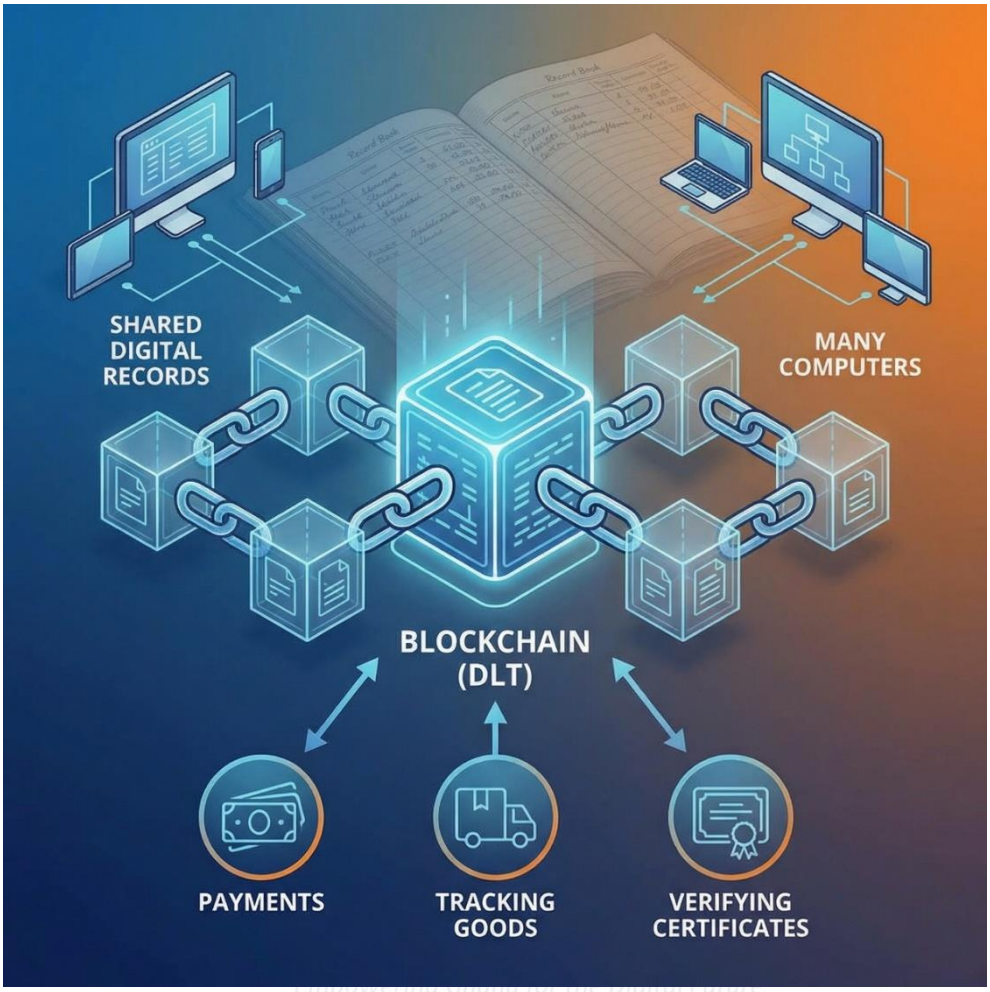
To understand blockchain, think of a classroom register, a clinic patient log, or a workshop job card system. In these systems, records are written down so everyone can see what has happened. Once an entry is made, it cannot be erased without notice. This helps prevent disputes and keeps information accurate.

Blockchain works similarly, but in digital form. Transactions or records are written into blocks. Each block is linked to the previous one, forming a chain of records. Once a block is added, it becomes challenging to change without others in the system noticing.

Blockchain is shared because many computers hold identical copies of the record. It is verifiable because participants can check that entries are correct. It is tamper-resistant because altering past records would require changing many copies simultaneously, which is extremely difficult.

Because of these features, blockchain is useful for recording payments, tracking goods, verifying certificates, and managing digital assets. It helps build trust among people who may not know or trust one another, without relying on a single central authority.





Private/Public key

In cryptography, public and private keys are fundamental to securing digital communication and transactions. A public key is a cryptographic code that can be shared openly with anyone. It is used to encrypt information or verify digital signatures, allowing others to send secure messages or validate authenticity without compromising security. Think of it like a padlock: anyone can use it to lock a box, but only the person with the corresponding private key can unlock it.

On the other hand, a private key is a secret code that must be kept confidential. It is used to decrypt messages or create digital signatures, proving ownership or authorisation. If someone gains access to your private key, they can impersonate you or access your encrypted data. Together, public and private keys form a secure pair that enables trustless, encrypted communication, which is essential for technologies such as blockchain, digital wallets, and secure messaging systems.

How a Virtual Asset Transaction Works

A virtual asset transaction follows a clear and structured process. Understanding each stage helps users see where mistakes can occur and why careful checking is essential.

Sender

The process begins with the sender. The sender opens a digital wallet, enters the recipient's wallet address or identifier, specifies the amount to be sent, and confirms the transaction. At this stage, the sender must carefully check all details. Any error, such as a wrong address or amount, cannot be corrected later.

Network Validation

After the sender confirms, the transaction is sent to the digital network. Multiple computers on the network, often called validators or nodes, verify transactions. They confirm that the sender has sufficient balance and that the transaction complies with the network's rules. This step replaces the role usually played by banks or clearing houses.

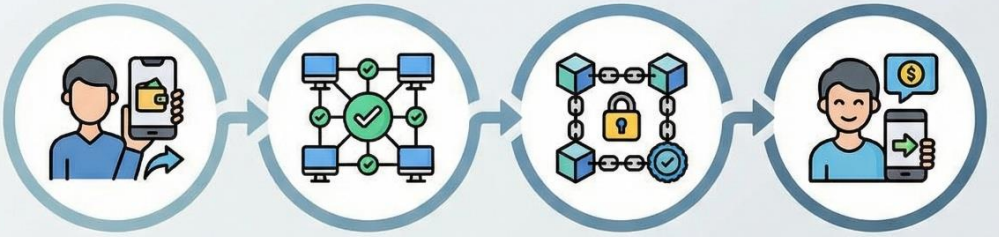
Confirmation

Once the network agrees that the transaction is valid, it is recorded on the shared digital ledger. This recording is permanent. The transaction becomes part of the blockchain, or distributed ledger, and is visible to authorised participants. At this point, the transaction is considered confirmed.

Receiver

Upon confirmation, the virtual asset is credited to the receiver's wallet. The receiver can then use, hold, or transfer the asset. The time it takes for the receiver to see the funds depends on the network and its current load, but once confirmed, the transfer is final.

How a Virtual Asset Transaction Works



1. Sender

Opens wallet, enters details, confirms transaction.

MUST CHECK CAREFULLY.

2. Network Validation

Validators/nodes check balance and rules.

Replaces banks.

3. Confirmation

Recorded on shared ledger.

PERMANENT & IRREVERSIBLE.

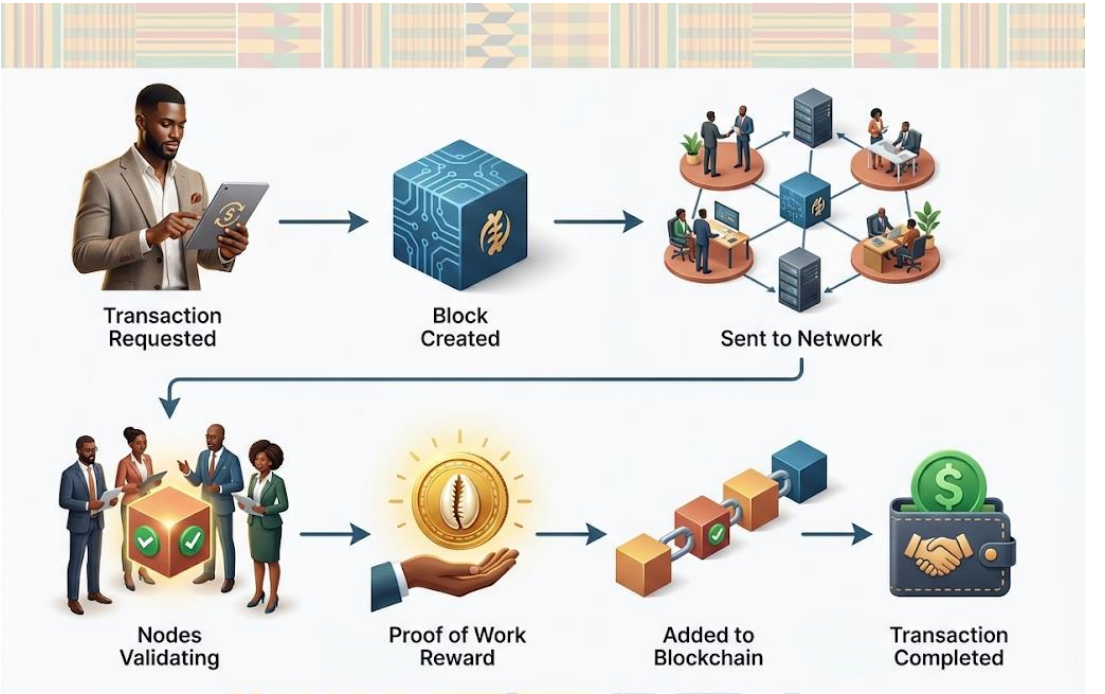
4. Receiver

Asset appears in wallet.

Transfer is final.

KEY POINT: TRANSACTIONS ARE IRREVERSIBLE. NO UNDO.

- Double-check details. Start small. Don't rush. Use trusted platforms.



Key Point: Virtual Asset Transactions Are Irreversible

Unlike bank or mobile money transactions, virtual asset transactions cannot be reversed or cancelled once confirmed. There is no central authority that can undo the transfer. If funds are sent to the wrong address, they are usually lost permanently.

This is why users must:

- Double-check recipient details before sending
- Start with small test transactions
- Avoid rushing
- Use trusted platforms and verified addresses

Understanding this transaction flow and its irreversible nature is critical for safe and responsible use of virtual assets.

Risks in Virtual Asset Use

Using virtual assets involves several risks that users must understand before participating. Many losses occur not because the technology fails, but because users are misled, rushed, or unaware of how the systems work.

Misleading Investment Promises

One significant risk comes from false investment claims. Some offers promise high, fast, or guaranteed returns with little effort. These claims are usually unrealistic. Virtual assets can rise or fall in value, and no legitimate investment guarantees profit. Offers that pressure users to act quickly or discourage questions are strong warning signs.

Fake Platforms

Fake platforms are apps or websites that appear to be real services. They often copy names, logos, colours, and layouts of known platforms. Once users send money to these platforms, the funds are usually lost. Fake platforms may disappear suddenly, leaving no way to recover assets.

Fraud and Impersonation Scams

Fraudsters often impersonate trusted figures, such as platform support staff, banks, government agencies, or well-known individuals. They may contact users through messages, calls, or social media. Their goal is to gain trust and request passwords, PINs, private keys, or direct transfers. Once this information is shared, assets can be stolen quickly.

Loss of Access Due to Poor Key Management

Virtual assets are controlled through private keys, passwords, and seed phrases. If these details are lost, forgotten, or shared, users may permanently lose access to their assets. Unlike traditional banking systems, there may be no recovery option if backup information is not stored securely.

Transaction Errors and Irreversibility

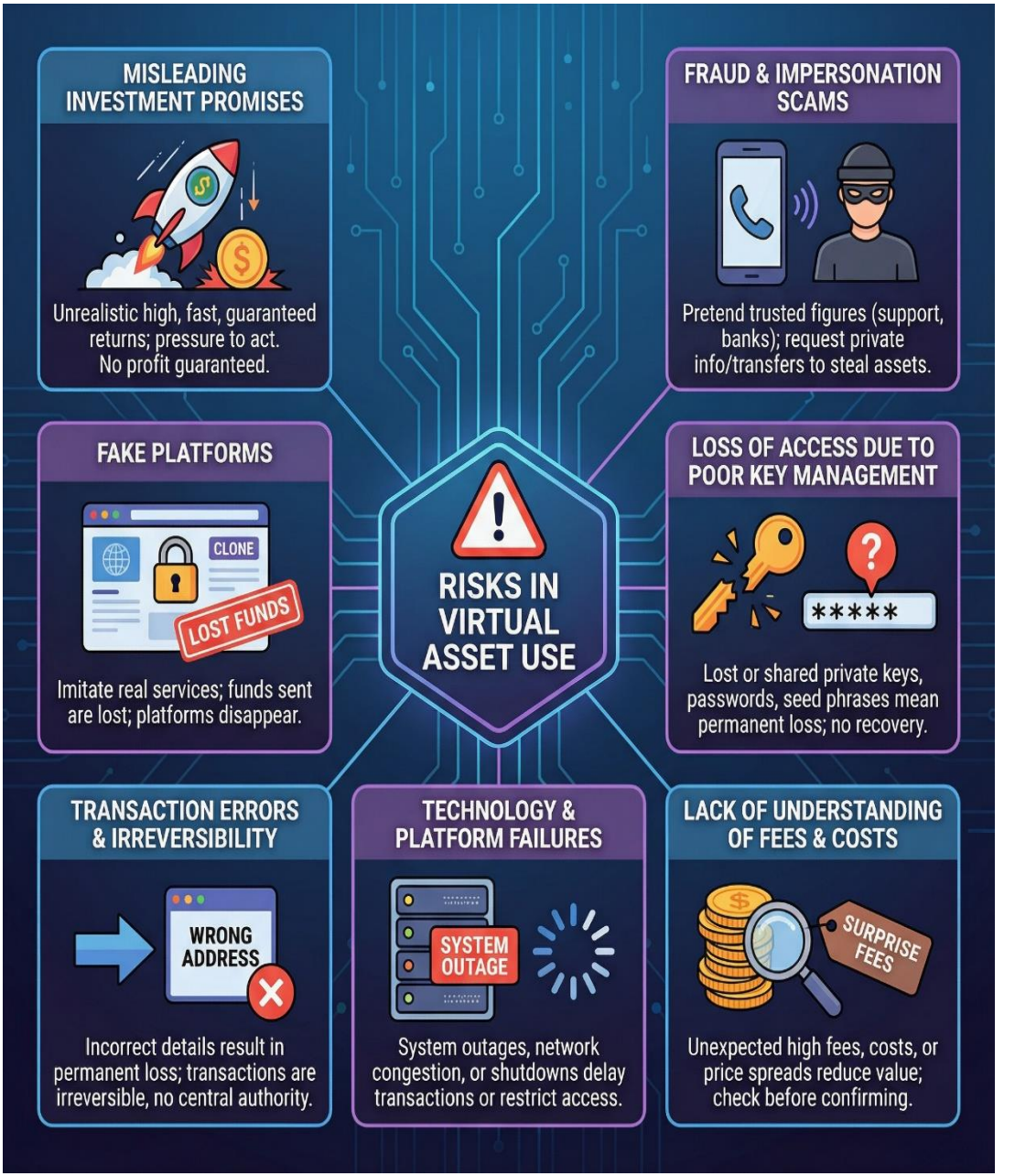
Sending virtual assets to the wrong address or entering incorrect details can result in permanent loss. Virtual asset transactions are generally irreversible once confirmed. There is no central authority to cancel or reverse a completed transfer.

Technology and Platform Failures

Technical problems such as system outages, network congestion, or platform shutdowns can delay transactions or restrict access to funds. Users relying on a single platform may be affected if that platform fails.

Lack of Understanding of Fees and Costs

Unexpected fees, high transaction costs during network congestion, or wide price spreads can reduce the value users receive. Not checking fees before confirming transactions can lead to surprise losses.

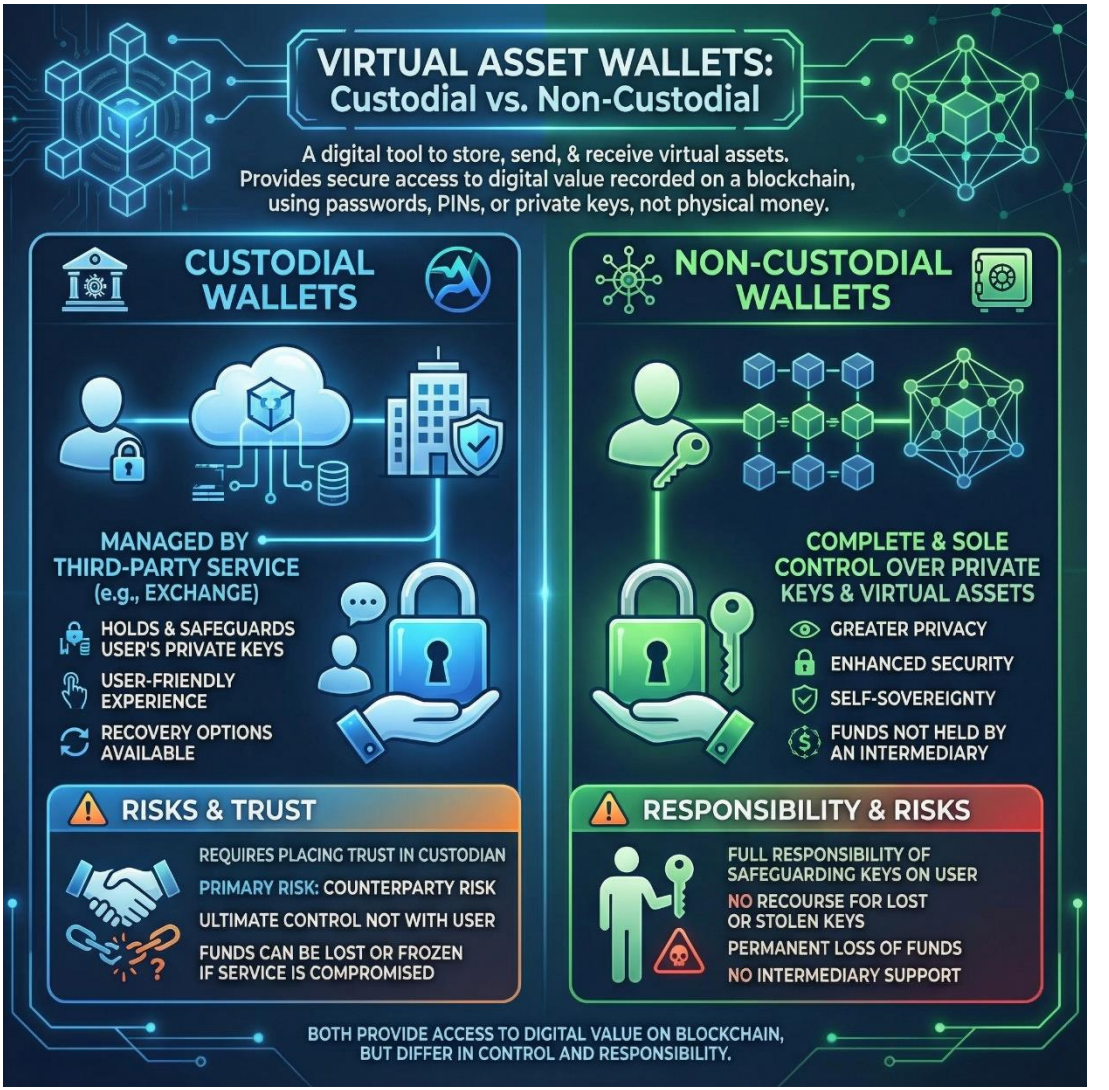

MISLEADING INVESTMENT PROMISES
Unrealistic high, fast, guaranteed returns; pressure to act. No profit guaranteed.
FRAUD & IMPERSONATION SCAMS
Pretend trusted figures (support, banks); request private info/transfers to steal assets.
FAKE PLATFORMS
CLONE
LOST FUNDS
Imitate real services; funds sent are lost; platforms disappear.
RISKS IN VIRTUAL ASSET USE
LOSS OF ACCESS DUE TO POOR KEY MANAGEMENT
*****
Lost or shared private keys, passwords, seed phrases mean permanent loss; no recovery.
TRANSACTION ERRORS & IRREVERSIBILITY
WRONG ADDRESS
Incorrect details result in permanent loss; transactions are irreversible, no central authority.
TECHNOLOGY & PLATFORM FAILURES
SYSTEM OUTAGE
System outages, network congestion, or shutdowns delay transactions or restrict access.
LACK OF UNDERSTANDING OF FEES & COSTS
SURPRISE FEES
Unexpected high fees, costs, or price spreads reduce value; check before confirming.

Technical Definitions:

A wallet for virtual assets is a digital tool used to store, send, and receive them. It allows users to access their holdings by using security details such as passwords, PINs, or private keys. The wallet does not hold physical money; instead, it provides secure access to digital value recorded on a blockchain or other distributed ledger system.

Custodial Wallets are managed by a third-party service, such as an exchange, which holds and safeguards a user's private keys. This offers a user-friendly experience with recovery options but requires trusting the custodian to secure the funds. The primary risk is counterparty risk, as users do not have ultimate control over their assets, which can be lost or frozen if the service is compromised.

Non-Custodial Wallets provide users with complete and sole control over their private keys and virtual assets. They offer greater privacy, security, and self-sovereignty, as an intermediary does not hold funds. However, this places full responsibility for safeguarding private keys on the user, leaving no recourse for lost or stolen keys and resulting in permanent loss of funds.



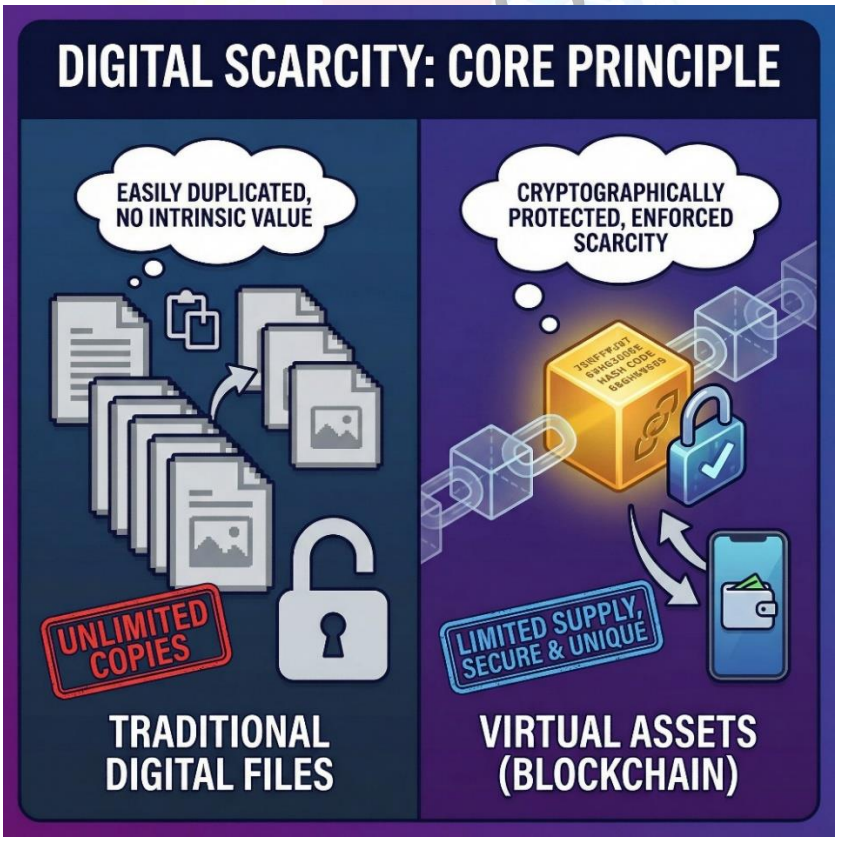
The *Virtual Asset Service Provider Act (VASP Act)* establishes a regulatory framework for virtual asset service providers operating in Ghana. It aims to combat illicit financing by mandating licensing, registration, and strict compliance with anti-money laundering (AML) and counter-terrorism financing (CFT) rules. This legislation seeks to protect consumers and ensure financial stability within Ghana's growing digital economy.

SECTION 2: KEY PRINCIPLES

Virtual assets and blockchain systems are built on a set of core principles. These principles explain why the system works, can be trusted, and behaves differently from traditional financial systems.

Digital Scarcity

Digital scarcity means that virtual assets are designed to exist in limited quantities and cannot be copied or duplicated at will. Unlike ordinary digital files such as photos or documents, virtual assets are protected by cryptographic rules that ensure each unit is unique and controlled. The system itself enforces this scarcity. New units can only be created through predefined rules, and the network verifies ownership. This prevents unauthorised duplication and preserves value.

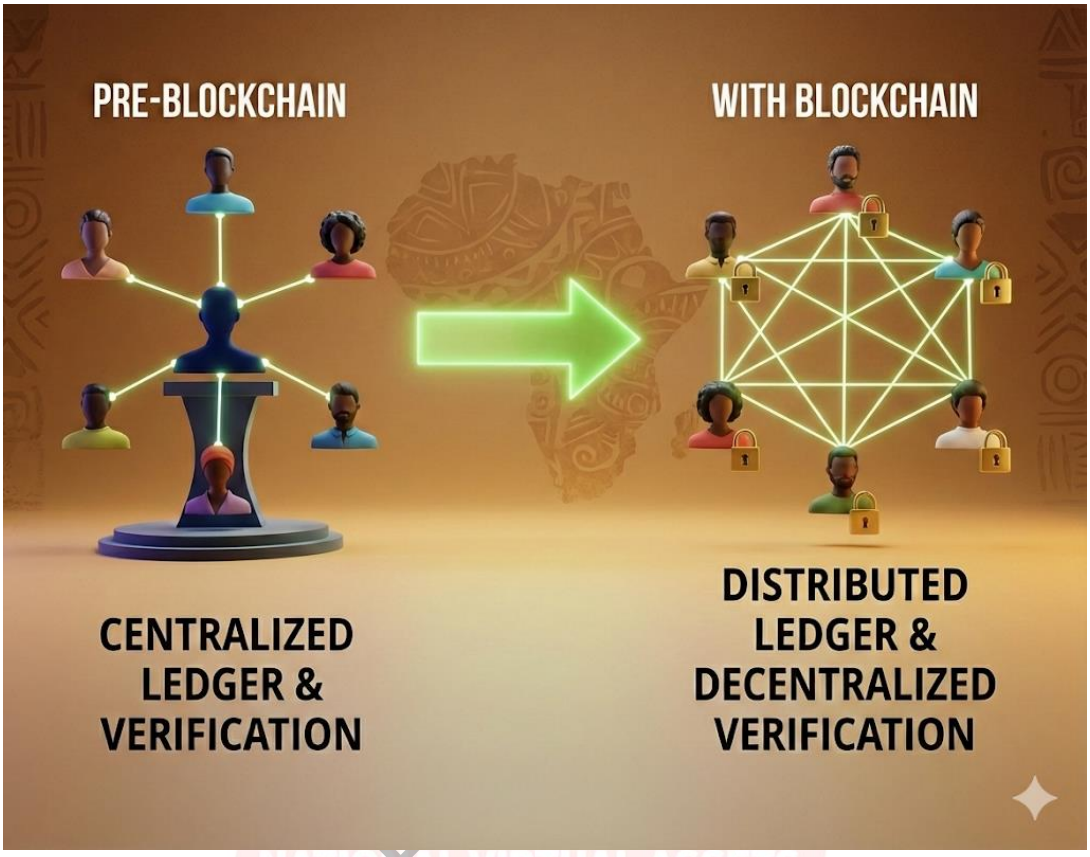


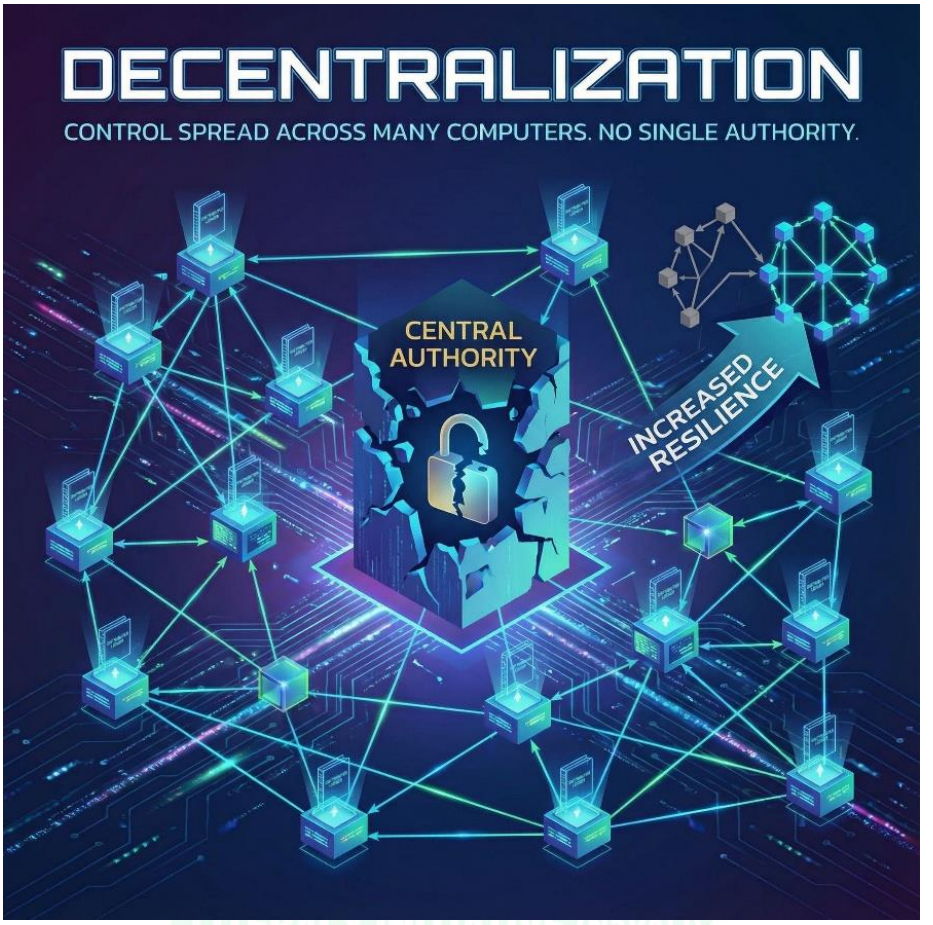
Cryptographic Security

Cryptographic security is the use of advanced mathematical techniques to protect ownership and transactions. It ensures that only the rightful owner of a virtual asset can authorise its transfer. Encryption protects private keys, verifies transactions, and prevents tampering. Without valid cryptographic proof, transactions are rejected by the network. This makes forgery and unauthorised access extremely difficult.

Decentralization

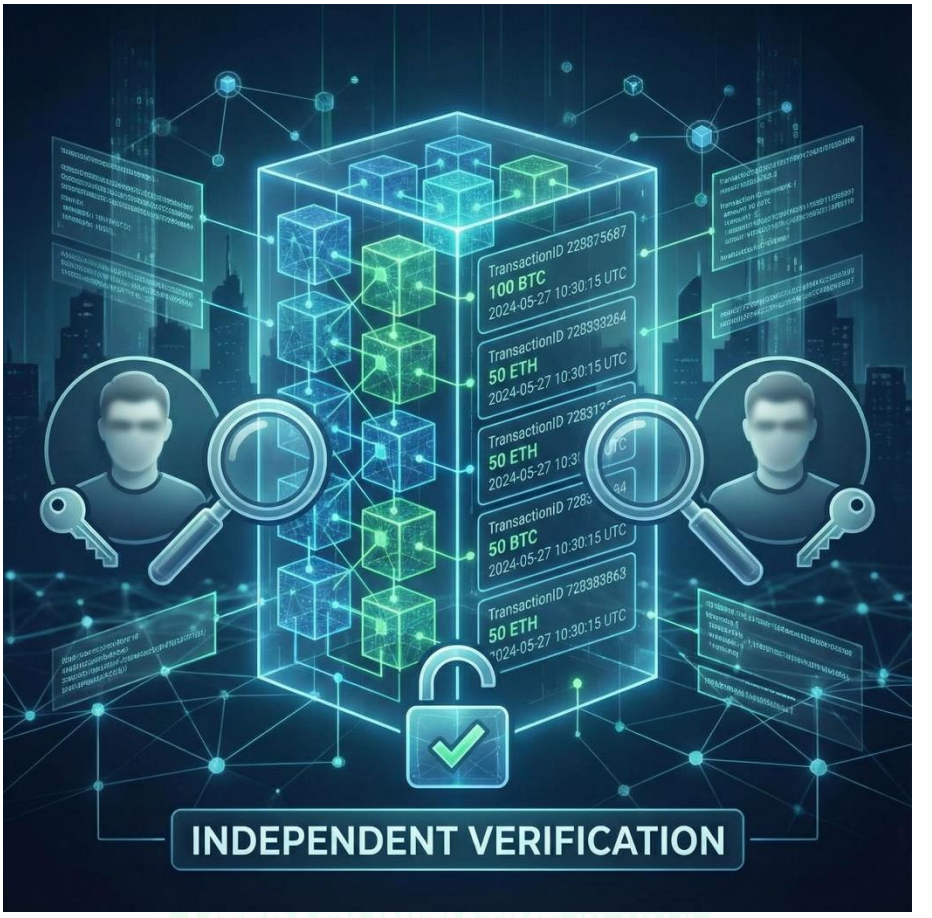
Decentralisation means that control is spread across many computers rather than held by a single institution. No single authority owns or controls the system. Each participant in the network holds a copy of the ledger and follows shared rules. This structure increases resilience because the system can continue to operate even if some participants fail or leave the network.

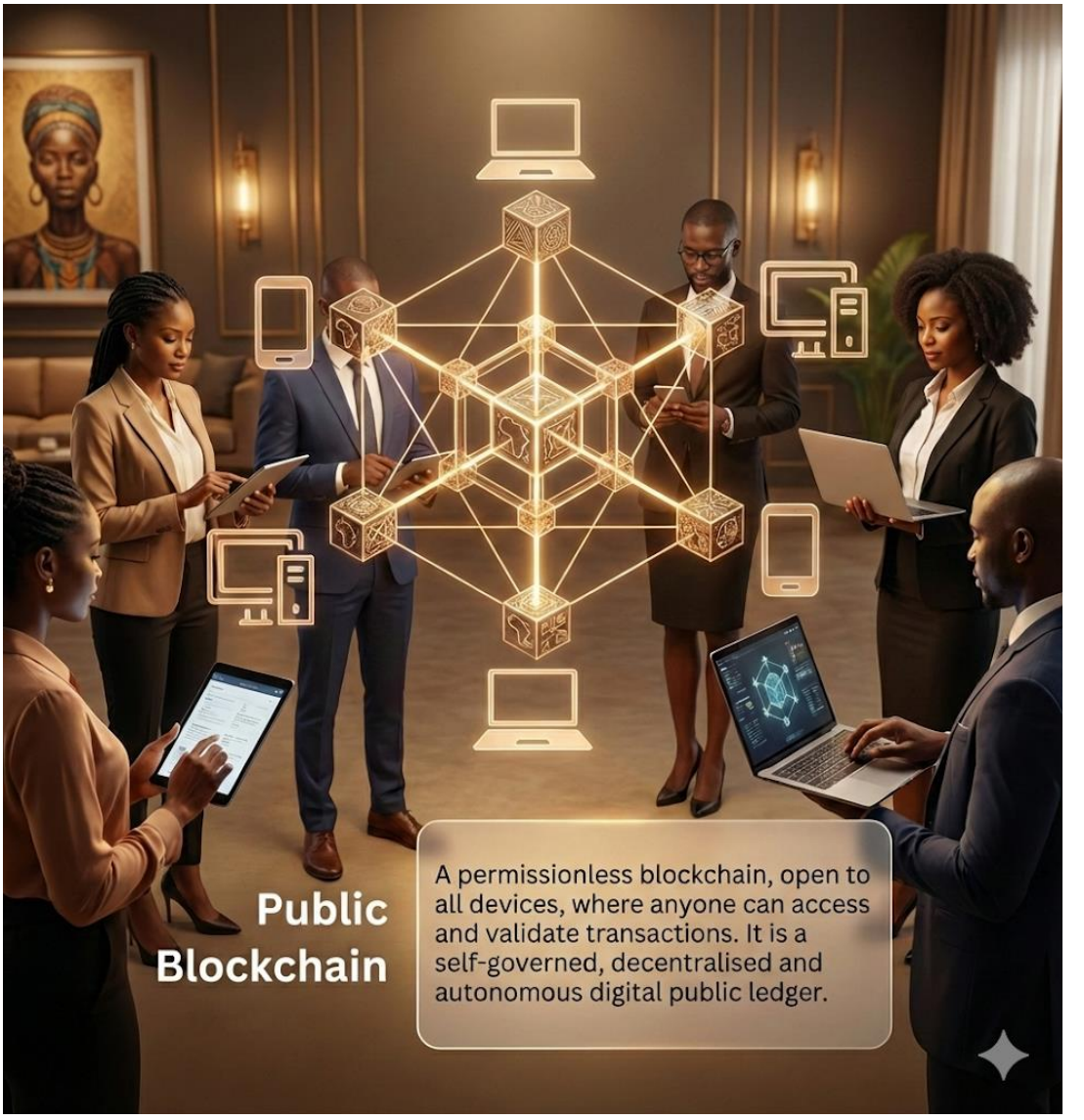




Transparency of Transactions

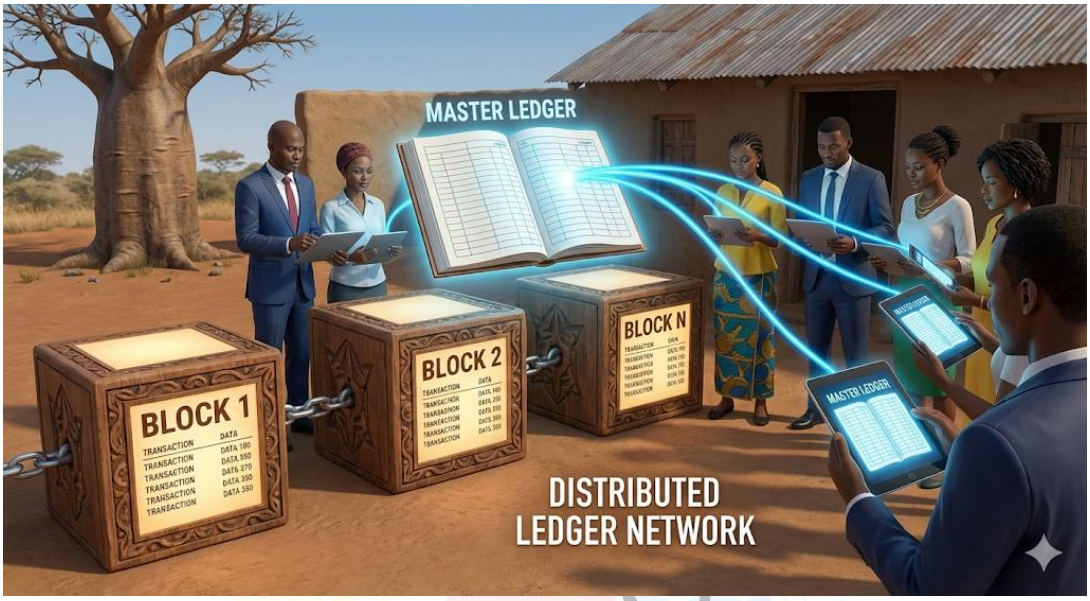
Transparency means that transactions are recorded on a shared ledger that participants can verify. While personal identities are protected, transaction data such as amounts and timestamps can be checked. This openness reduces disputes, supports accountability, and allows independent verification without relying on trust in a single organisation.




Public Blockchain
A permissionless blockchain, open to all devices, where anyone can access and validate transactions. It is a self-governed, decentralised and autonomous digital public ledger.

Immutability of Records

Immutability means that once a transaction is recorded, it cannot be changed or erased. New records can be added without disrupting existing ones. This creates a permanent and tamper-resistant history of activity. Attempts to alter records would be detected by the network, making fraud or manipulation very difficult.



Key Takeaway for Learners

Together, these principles explain why virtual assets and blockchain systems can operate without a central authority, remain secure, and maintain trust through technology rather than intermediaries.

SECTION 3: OPERATIONAL MECHANICS

Operational mechanics explain how virtual asset systems work in practice, from the moment a user initiates a transaction to the moment it is recorded and received. This section focuses on the flow of transactions, the roles of different actors, and how technology coordinates their interaction.

How the System Functions

A virtual asset transaction begins with a user and ends with a receiver, but several components work together in between.

- ✓ The user initiates a transaction using a digital wallet.
- ✓ The transaction details, such as the amount and recipient, are sent to the network.
- ✓ Network nodes or validators check whether the transaction follows the system's rules, including sufficient balance and valid authorisation.
- ✓ Once validated, the transaction is recorded on the blockchain or distributed ledger.
- ✓ The receiver's wallet reflects the transferred value after confirmation.

This process replaces traditional intermediaries with automated validation and shared records.

Interactions Among Key Actors

Several actors interact during a transaction:

- ✓ User: Initiates and authorises the transaction using a wallet.
- ✓ Virtual Asset Service Provider (VASP): May act as an exchange, custodian, or platform that provides wallet services, user interfaces, customer support, or compliance checks.
- ✓ Network Validators or Miners: Independent computers that verify transactions and agree on which transactions are added to the ledger.

Each actor has a distinct role, and the system works only when all roles function correctly.

Technical Workflow

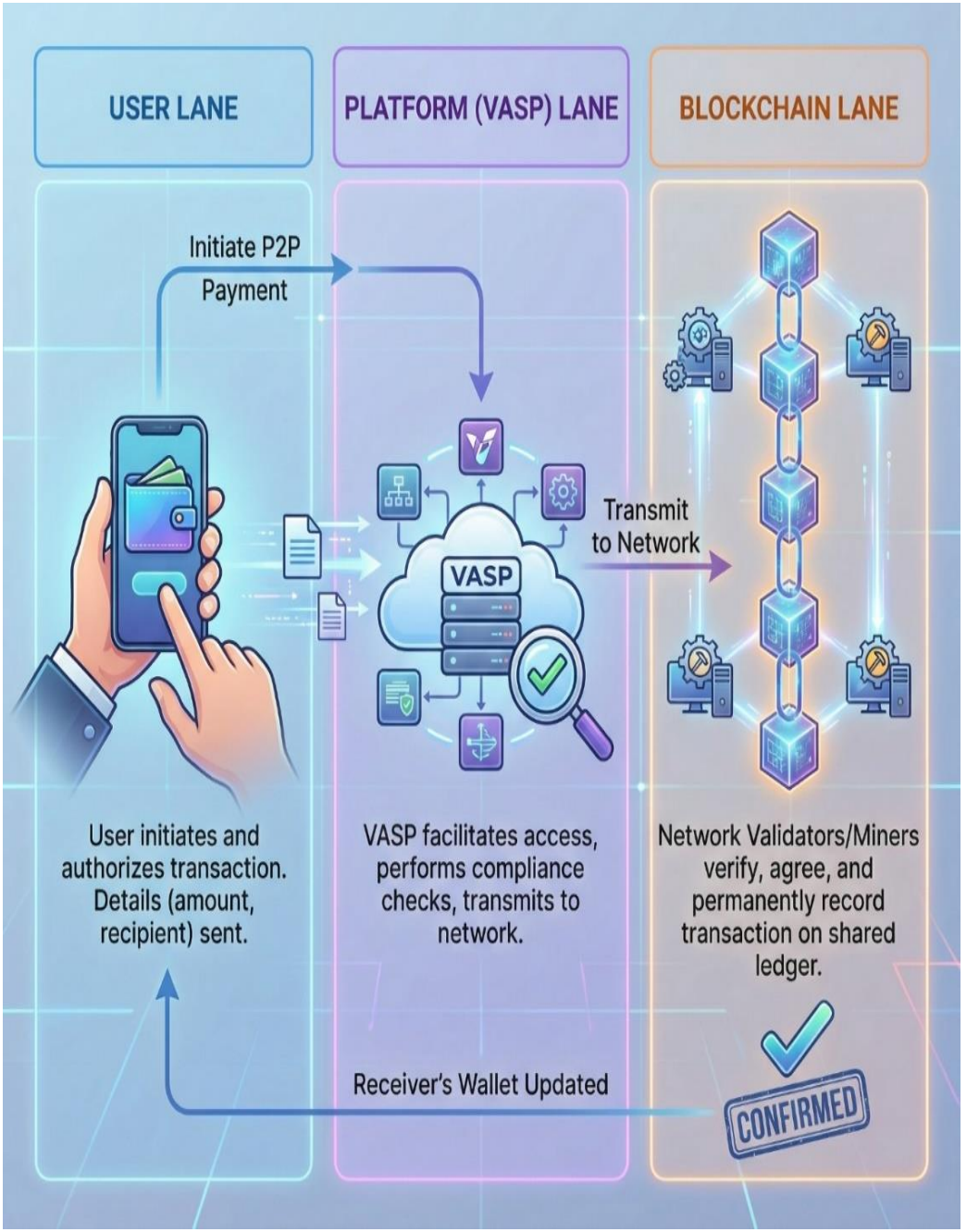
The transaction process can be understood through a three-lane workflow:

User Lane: A peer-to-peer (P2P) payment is initiated from the user's wallet.

Platform (VASP) Lane: The VASP facilitates access, performs checks where applicable, and transmits the transaction to the network.

Blockchain Lane: The blockchain validates transactions, records them permanently, and updates the shared ledger.

This layered interaction explains how user actions, service platforms, and blockchain infrastructure combine to complete a transaction securely and transparently.


USER LANE
PLATFORM (VASP) LANE
BLOCKCHAIN LANE
Initiate P2P Payment
VASP
Transmit to Network
User initiates and authorizes transaction. Details (amount, recipient) sent.
VASP facilitates access, performs compliance checks, transmits to network.
Network Validators/Miners verify, agree, and permanently record transaction on shared ledger.
Receiver's Wallet Updated
CONFIRMED

Understanding the Blockchain Technology Stack

Blockchain systems are best understood as a stack of layers, where each layer supports the one above it. This structure explains how technology becomes digital value, and how users interact with that value through applications.

a. The Three Layers Explained

i. Base Layer: DLT / Blockchain (Infrastructure Layer)

This is the foundation of the entire system.

- ✓ It provides the core technology that allows digital records to be created, shared, and protected.
- ✓ Security, decentralisation, and trust are achieved through distributed consensus among many computers.
- ✓ This layer ensures that records are tamper-resistant and verifiable.

Examples: Bitcoin blockchain, Ethereum, Hyperledger, Corda

ii. Middle Layer: Virtual Assets (Digital Value Layer)

This layer represents value built on top of blockchain infrastructure.

- ✓ Virtual assets exist because the underlying blockchain allows value to be recorded and transferred securely.
- ✓ Different virtual assets serve different purposes, such as payment, savings, access to services, or investment.
- ✓ Ghana's eCedi sits in this layer as a digital representation of the national currency.

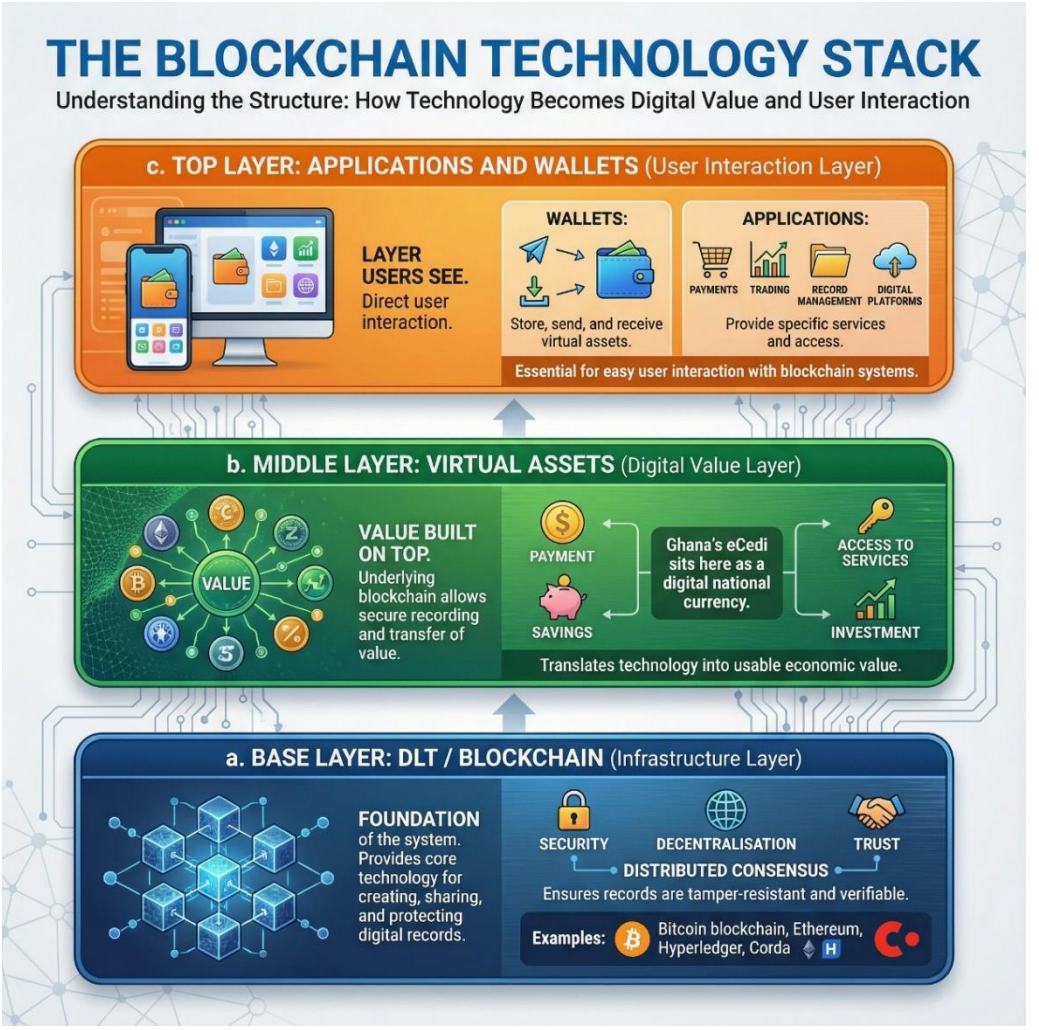
This layer translates technology into usable economic value.

iii. Top Layer: Applications and Wallets (User Interaction Layer)

This is the layer users see and interact with directly.

- ✓ Wallets allow users to store, send, and receive virtual assets.
- ✓ Applications provide specific services such as payments, trading, record management, or access to digital platforms.

- ✓ Without this layer, users would not be able to interact easily with blockchain systems.



b. How the Layers Work Together

Foundation Upward Support

- ✓ DLT / Blockchain enables Virtual Assets
- ✓ Virtual Assets enable Applications and Wallets

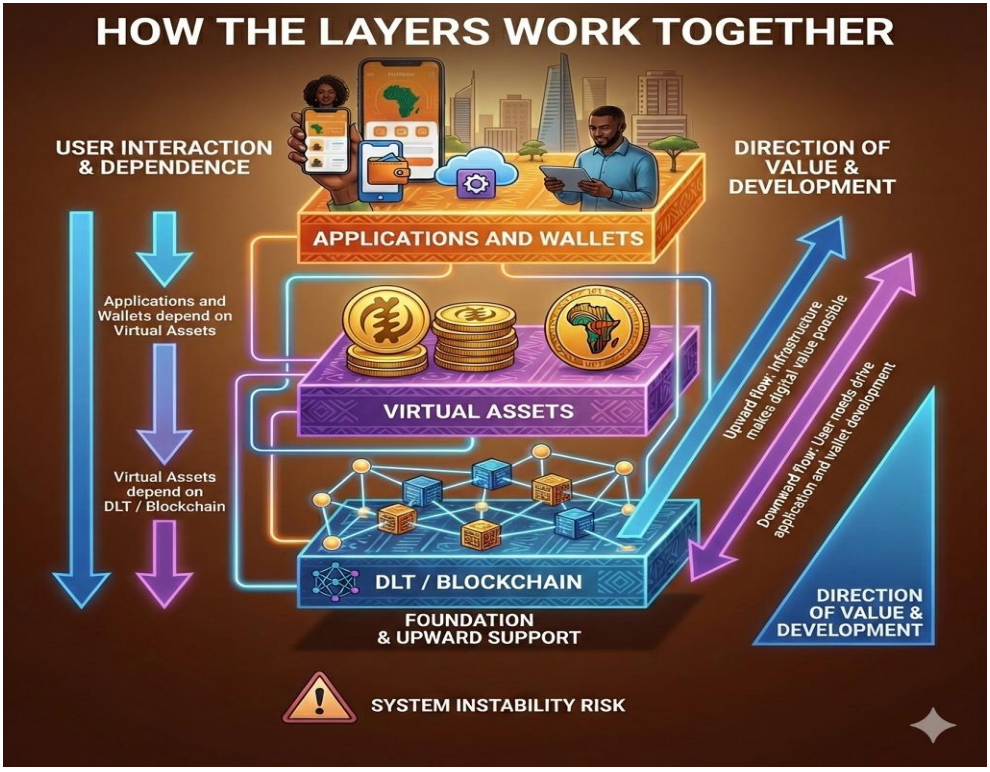
User Interaction Downward Dependence

- ✓ Applications and Wallets depend on Virtual Assets
- ✓ Virtual Assets depend on DLT / Blockchain

Direction of Value and Development

- ✓ Upward flow: Infrastructure makes digital value possible
- ✓ Downward flow: User needs drive application and wallet development

If any layer is weak, the entire system becomes unstable.



Why This Stack Matters

- ✓ A strong blockchain foundation ensures security and trust
- ✓ Well-designed virtual assets ensure reliable value representation
- ✓ Effective applications ensure accessibility and ease of use

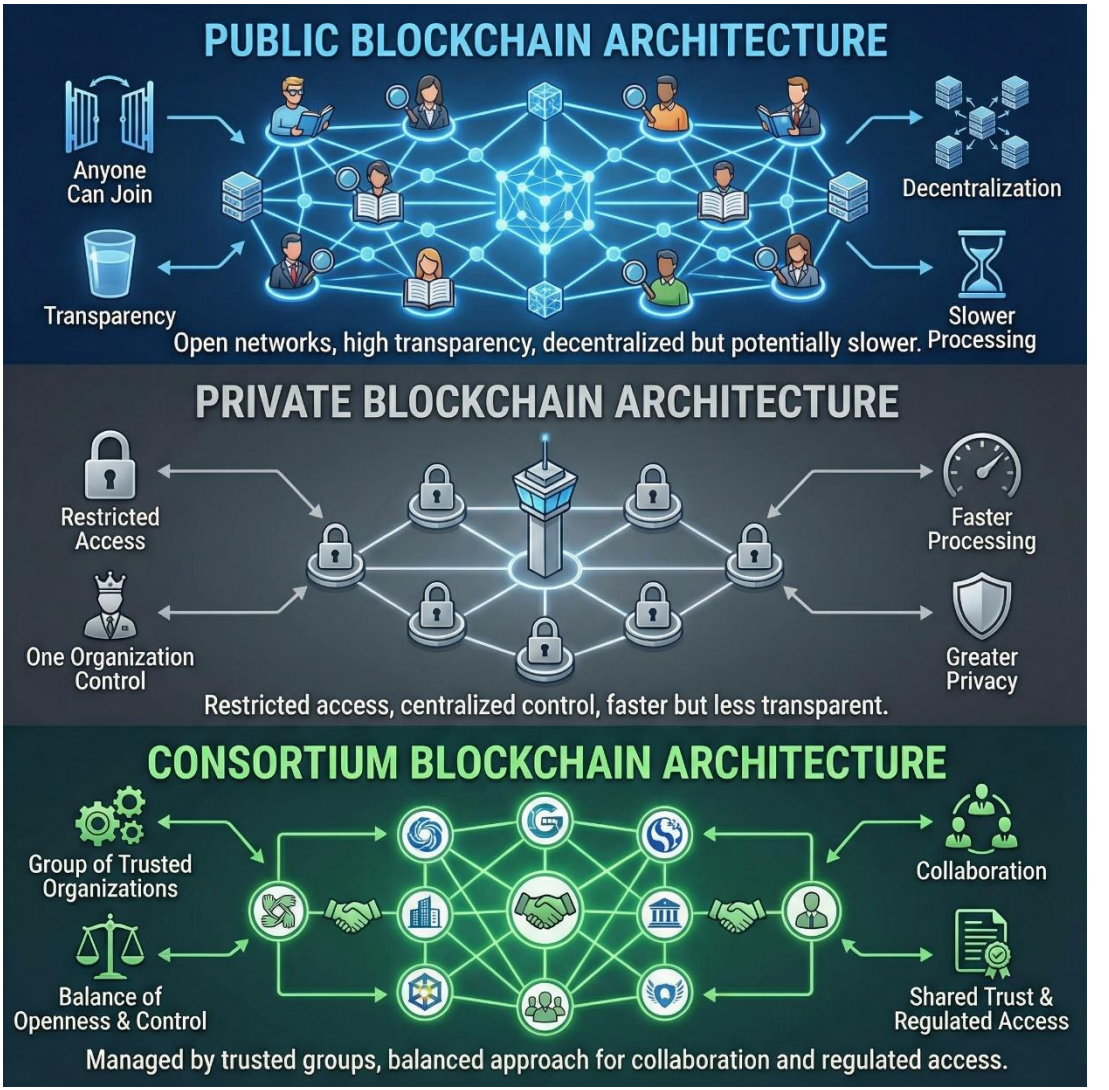
Weaknesses in any layer can lead to security risks, poor user experience, or loss of confidence.

Public vs Private / Consortium Blockchain Architectures

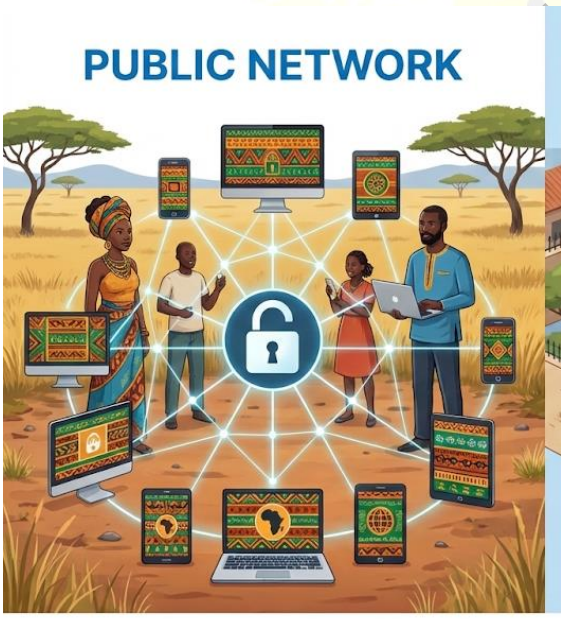
Public blockchains are open networks where anyone can join, view transactions, and help validate records. They promote transparency and decentralisation, but may be slower because many participants are involved.

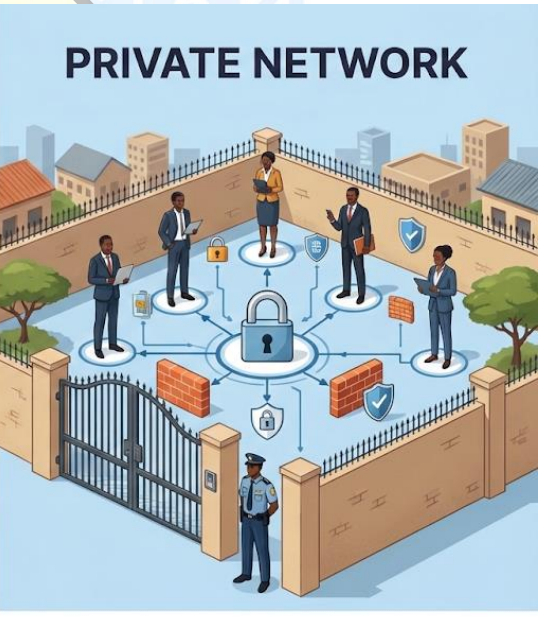
Private blockchains restrict access to approved participants and are usually controlled by one organisation. They offer faster processing and greater privacy but rely on centralised control.

Consortium blockchains are managed by a group of trusted organisations. They balance openness and control, making them suitable for industries that require collaboration, shared trust, and regulated access.


PUBLIC BLOCKCHAIN ARCHITECTURE
Anyone Can Join
Transparency
Decentralization
Slower Processing
Open networks, high transparency, decentralized but potentially slower.
PRIVATE BLOCKCHAIN ARCHITECTURE
Restricted Access
One Organization Control
Faster Processing
Greater Privacy
Restricted access, centralized control, faster but less transparent.
CONSORTIUM BLOCKCHAIN ARCHITECTURE
Group of Trusted Organizations
Balance of Openness & Control
Collaboration
Shared Trust & Regulated Access
Managed by trusted groups, balanced approach for collaboration and regulated access.


Public Road
Consortium Road
Private Road
COOPERATION
PRIVATE ACCESS ONLY


PUBLIC NETWORK


PRIVATE NETWORK

SECTION 4: LEGAL AND POLICY CONTEXT

Institutional Mandates: The roles of the Bank of Ghana (BoG) and the Securities and Exchange Commission (SEC) in licensing and oversight.
a. The BoG is responsible for licensing and overseeing VASPs whose activities involve payments, transfers, or storing value, focusing on financial integrity and systemic risk.

b. The SEC licenses and regulates VASPs whose activities involve virtual assets classified as securities, such as investment products or asset-backed tokens.

c. The specific regulator for a VASP depends on the nature of its business activities, with some potentially requiring authorisation from both institutions.

d. Together, BoG and SEC enforce anti-money laundering rules and ensure market conduct to protect consumers and maintain financial stability in the virtual asset space.

SECTION 5: RISK AND ASSURANCE

Risk and assurance in the use of virtual assets involve understanding where mistakes, failures, or misuse can occur and knowing what actions reduce those risks. This section highlights key professional risk areas and the assurance mechanisms that help manage them.

Professional Risk Categories

Conceptual Risks

These arise from a misunderstanding of how virtual assets and blockchain systems work. When users confuse different asset types, platforms, or technologies, they may make poor decisions. Examples include assuming all digital assets are the same, believing blockchain automatically

guarantees safety, or misinterpreting price movements as guaranteed returns.

Operational Risks
Operational risks occur when users fail to follow proper procedures. This includes sending assets to the wrong address, poor password management, ignoring transaction fees, or failing to test transactions before large transfers.

Platform and Counterparty Risks
These risks arise from reliance on platforms, exchanges, custodians, or intermediaries. Even licensed providers can experience technical failures, cyber attacks, or operational breakdowns. Users who depend on unverified or poorly governed platforms face higher exposure to loss.

Information Risks
Information risk involves acting on inaccurate, outdated, or misleading information. This includes advice from social media, unverified online groups, or unofficial announcements. Misinformation can lead to panic actions, rushed investments, or engagement with fraudulent schemes.

Control Mechanisms

Use of Authorised Information Sources
Reliable decisions depend on information from official and recognised sources such as regulators, central banks, licensed service providers, and formal guidance documents. These sources provide verified updates, warnings, and regulatory clarity.

Engagement with Licensed and Supervised Entities
Licensed entities are subject to oversight, reporting requirements, and compliance standards. While licensing does not remove all risk, it

provides an assurance baseline and access to formal complaint and reporting channels.

Internal Controls and Personal Safeguards
Users should apply basic control practices such as record keeping, transaction verification, fee review, and use of security features like two-factor authentication. These controls reduce exposure to avoidable loss.

Oversight Responsibilities
Individual Responsibility
Each user has a responsibility to verify information, confirm platform legitimacy, and understand the risks involved before engaging. This includes checking authorisation status, reviewing terms of service, and questioning offers that appear unusual or urgent.

Ongoing Vigilance
Risk management is not a one-time action. Users must remain alert to changes in platforms, regulations, fees, and security threats. Regularly reviewing activities and staying informed helps detect problems early.

Escalation and Reporting
When issues arise, users must know when and how to escalate concerns through proper channels. Prompt reporting supports resolution, limits harm, and contributes to system-wide assurance.

Key Assurance Message
Risk cannot be eliminated, but it can be managed through understanding, verification, and responsible engagement.

SECTION 6: PRACTICAL APPLICATIONS

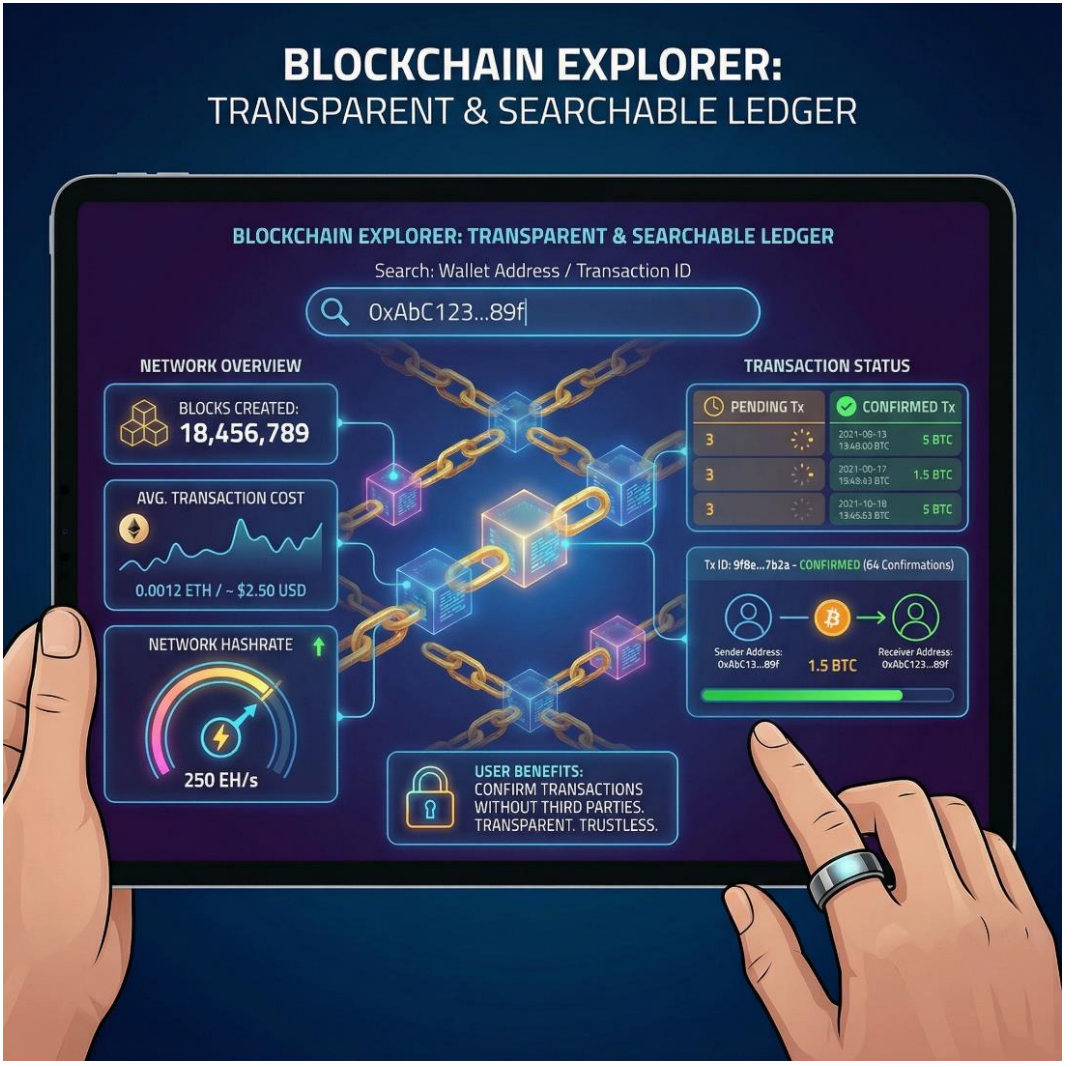
a. Practical Tools: Using Blockchain Explorers

A blockchain explorer is an online tool that allows anyone to view transactions recorded on a public blockchain. It provides a transparent, searchable ledger that shows how transactions move through the network.

Blockchain explorers allow users to:

- ✓ View the number of blocks created
- ✓ Check average transaction costs
- ✓ See pending or confirmed transactions
- ✓ Observe network activity, such as hashrate
- ✓ Search for a specific transaction using a wallet address or transaction ID

These tools help users confirm whether a transaction has been sent, received, or confirmed, without relying on a third party.


BLOCKCHAIN EXPLORER:
TRANSPARENT & SEARCHABLE LEDGER
BLOCKCHAIN EXPLORER: TRANSPARENT & SEARCHABLE LEDGER
Search: Wallet Address / Transaction ID
0xAbC123...89f
NETWORK OVERVIEW
BLOCKS CREATED:
18,456,789
AVG. TRANSACTION COST
0.0012 ETH / ~ $2.50 USD
NETWORK HASHRATE
250 EH/s
TRANSACTION STATUS
PENDING Tx
CONFIRMED Tx
5 BTC
1.5 BTC
5 BTC
Tx ID: 9f8e...7b2a - CONFIRMED (64 Confirmations)
Sender Address:
0xAbC13...89f
1.5 BTC
Receiver Address:
0xAbC123...89f
USER BENEFITS:
CONFIRM TRANSACTIONS
WITHOUT THIRD PARTIES.
TRANSPARENT. TRUSTLESS.

b. Practical Procedures: Fact-Checking Virtual Asset Claims

Before engaging with or promoting any virtual asset project, users should follow basic fact-checking steps.

Key procedures include:

- ✓ Checking for official warnings or notices from recognised authorities such as the Bank of Ghana or the Securities and Exchange Commission
- ✓ Reviewing whether the project has a clear whitepaper that explains what it does, how it works, and why it exists
- ✓ Confirming whether the project has a verifiable team, real contact details, and a visible track record

c. Evaluating Scenarios: Real Problem or Buzzwords?

Not every virtual asset project solves a real problem. Some projects rely heavily on technical language and marketing terms but fail to deliver real value.

A legitimate project will:

- ✓ Clearly identify a specific problem, such as slow cross-border payments, lack of financial access, or poor supply-chain transparency
- ✓ Explain how the solution works in simple, practical terms
- ✓ Show why blockchain is genuinely needed for that solution

- ✓ Focus on actual use and adoption, not just token price

A buzzword-driven project often:

- ✓ Uses vague promises like "revolutionising finance" without precise details
- ✓ Emphasises token price growth rather than product utility
- ✓ Lacks evidence of real users or working systems

The key test is whether the project provides measurable value, even if the token itself is removed from the discussion.

d. Good Practice Guide: "Look Before You Leap"

Good practice requires careful thinking before any engagement. Users should:

- Research before investing, recommending, or promoting any virtual asset product
- Take time to read, verify, and compare information
- Avoid pressure-driven decisions
- Seek independent confirmation from trusted sources

This approach reduces risk exposure and supports responsible participation in virtual asset systems.

SECTION 7: DISCUSSION POINTS AND REFLECTION

- ✓ Points for Deeper Thinking: Should the eCedi replace physical cash? What are the pros and cons?
- ✓ Policy Questions: How can Ghana balance innovation in digital assets with consumer protection?
- ✓ Ethical Considerations: What is a professional's duty if they suspect a colleague is falling for a Virtual Asset scam?
- ✓ Sector-specific Reflections: 1. How to address student questions on crypto?, 2. How do Virtual Assets relate to traditional banking products?

Assessment Strategy

Analytical quiz on Virtual Asset categories and DLT basics

I. Scenario: Akosua wants to send GHS 100 to her cousin in Kumasi instantly. Compare the operational role of a Mobile Money agent versus a Blockchain network node in processing her transaction.

II. Diagram Analysis: Given a simple diagram of a public blockchain ledger, explain why altering a past transaction is said to be "extremely difficult."

III. Compare & Contrast: How is an eCedi fundamentally similar to and different from a stablecoin like USDT?

IV. True or False (with justification): A Non-Fungible Token (NFT) is primarily designed to be used as a currency for daily purchases.

V. Ordering: Sequence the flow of a cryptocurrency payment: a) Receiver shares public address, b) Sender's wallet signs transaction, c) Transaction is recorded on a block, d) Sender enters amount and address.

VI. Real-World Link: How might DLT's feature of transparent tracking be applied to reduce fraud in Ghana's cocoa supply chain?

VII. Identify the Misconception: A friend says, "Investing in Bitcoin is safe because it's based on mathematics." What key risk is he overlooking?

VIII. Matching: Match the asset type (Payment Token, Utility Token, Stablecoin) to its best description (e.g., "Used to pay for transaction fees on a specific network").

IX. Short Answer: In one sentence, explain why "virtual asset" is a broader category than "cryptocurrency."

X. Prediction: If Ghana sees widespread eCedi adoption, what is one potential impact on the use of physical cash for small market transactions?

MODULE SUMMARY PAGE

- Key Insights: Virtual assets are diverse digital tools, not a monolithic category. Understanding their basic mechanics demystifies them. Ghana has an active regulatory landscape focused on safety.
- Applications to Professional Roles: Enables informed conversations with clients, students, or the public; provides a foundation for recognising potentially fraudulent schemes.
- Key Risks: Risk of acting on misconceptions; engaging with unlicensed platforms.
- Next Steps: Proceed to Module 2 to understand the specific tools and platforms used to interact with Virtual Assets.

END OF MODULE

Module 2

Model Title: Key Tools and Components

Module Purpose

This module is the practical implementation guide for the NaVALI project. It moves from the "what" of Virtual Assets to the critical "how." Participants will gain hands-on knowledge of the essential technologies, software, and processes needed to operate, regulate, and secure a virtual asset market in Ghana under the forthcoming VASP framework. The content is delivered through a combination of theoretical explanation, case studies, live demonstrations, and role-specific practical scenarios. Essentially, it seeks;

- To introduce the principal tools, interfaces, and operational components for accessing and managing virtual assets, moving from concept to practical interaction.
- To empower participants to distinguish between different access and custody methods, understand the role of platforms, recognise associated costs, and implement foundational operational safeguards to reduce avoidable errors and losses.

Module Learning Outcomes

By the end of this module, participants will be able to:

1. Distinguish between the primary forms of access and custody arrangements (custodial vs. non-custodial, hot vs. cold wallets) at a high level.
2. Explain the general role of platforms and intermediaries (VASPs) and the implications for user responsibilities and security.
3. Recognise typical sources of cost (transaction fees, spread) and friction (network congestion, verification delays) in Virtual Asset transactions and how they influence user experience.

4. Outline baseline operational safeguards (strong authentication, verification, and small test transactions) appropriate for varied user contexts.

SECTION 1: CONCEPT OVERVIEW

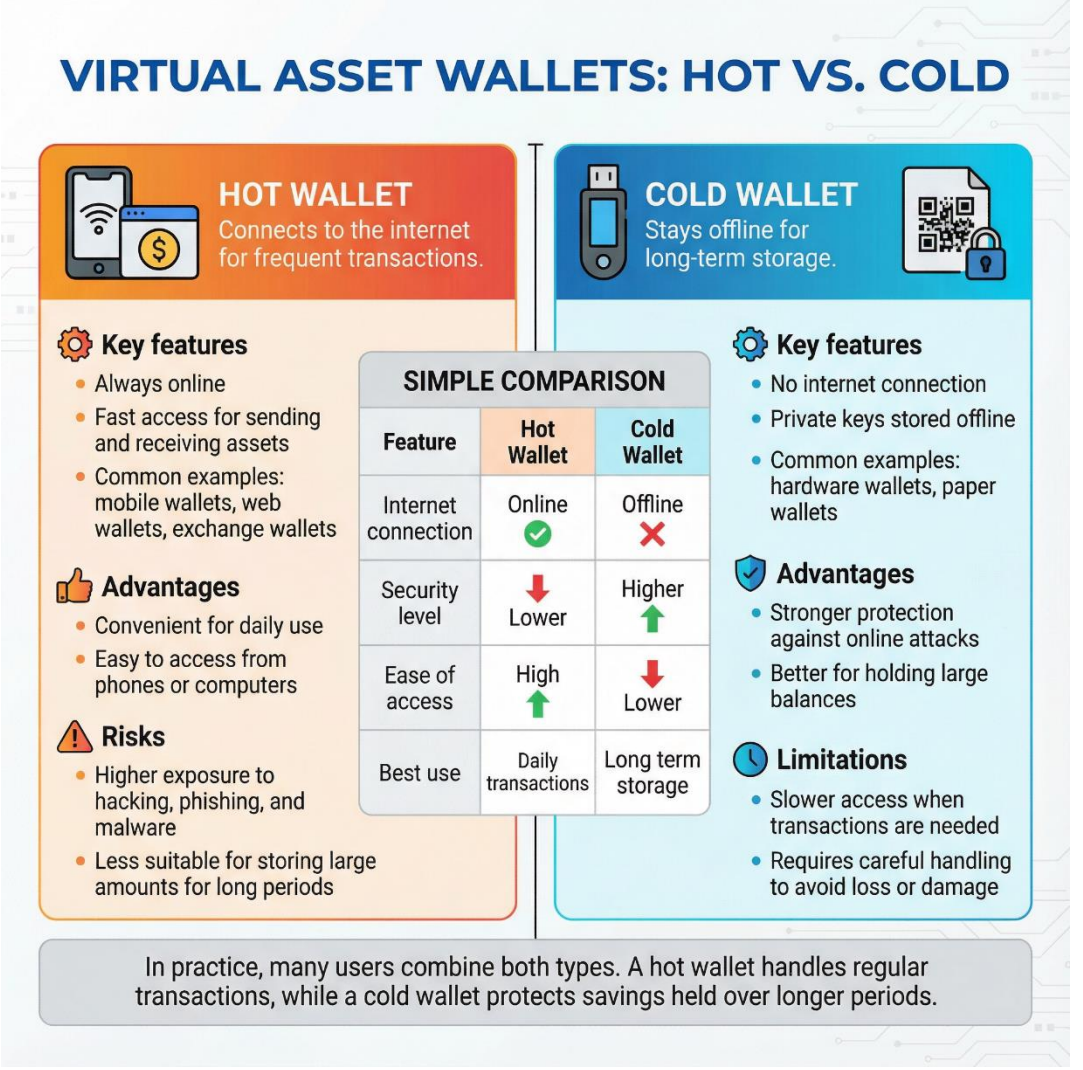
This section introduces the core concepts that underpin the safe access, storage, and use of virtual assets. These concepts explain the tools people interact with, how control and security are managed, and how virtual assets connect to traditional money systems.

Core Concepts in Virtual Asset Use

a. Hot Wallets vs Cold Wallets

Hot wallets are connected to the internet. They are commonly used for everyday transactions because they allow quick access and convenience. However, being online increases exposure to cyber risks.

b. Cold wallets store private keys offline. They are primarily used for long-term asset storage. Because they are not connected to the internet, they offer stronger protection against hacking, though they are less convenient for frequent use.



c. Managing Seed Phrases Securely

A seed phrase, also known as a recovery phrase, is a series of words that provides full access to a wallet. Anyone who has this phrase can control the assets in the wallet. Best practices include:

- Writing the seed phrase on paper
- Storing it offline in a secure location

- Never sharing it
- Never storing it digitally through photos, email, or chat applications

Loss or exposure of a seed phrase can result in permanent loss of assets.

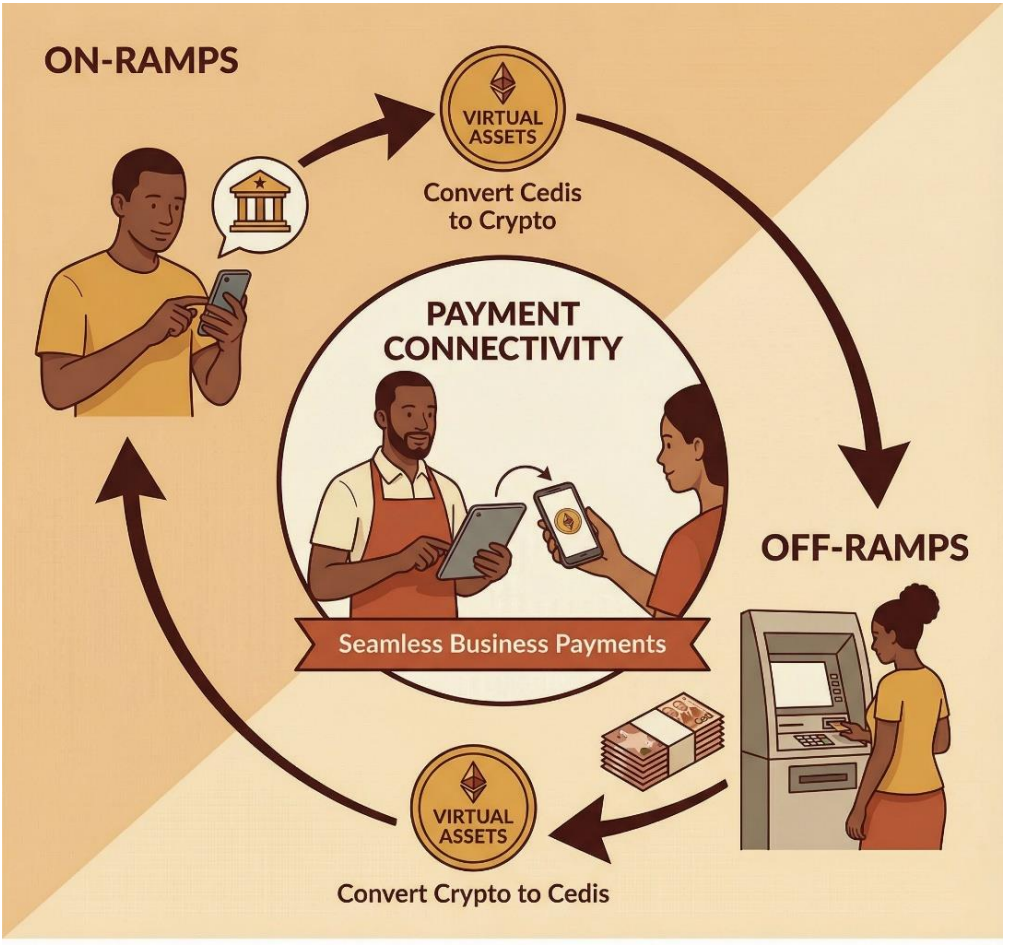
d. On-Ramps, Off-Ramps, and Payment Connectivity

On-ramps allow users to convert traditional money, such as cedis from a bank account or mobile money wallet, into virtual assets.

Off-ramps allow users to convert virtual assets back into traditional money.

These services act as bridges between the traditional financial system and virtual asset networks. In Ghana, they are essential for practical adoption and inclusion.

Payment APIs provide digital infrastructure that enables businesses to accept virtual asset payments seamlessly. This could allow Ghanaian merchants to trade faster and more cheaply across borders.



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

e. Secure Device Practices

Safe use of virtual assets depends heavily on device security. Users should:

- Use strong, unique passwords
- Enable two-factor authentication
- Keep devices updated
- Avoid unsafe links and unknown apps
- Verify all sources before acting

Key Technical Definitions

- ✓ Hot Wallet: Online wallet for frequent use
- ✓ Cold Wallet: Offline wallet for secure storage
- ✓ Seed Phrase / Recovery Phrase: Backup access to wallet
- ✓ Transaction Fee (Gas): Cost paid to process a transaction
- ✓ Multi-Signature: Wallet requiring multiple approvals to authorise transactions

SECTION 2: KEY PRINCIPLES

Foundational Principles of Virtual Asset Use

- ✓ "Not your keys, not your coins": If you don't control your private keys, you don't truly control your digital money. Custody matters.
- ✓ Custody trade-off: Holding your own keys gives control but requires responsibility. Using platforms is easier but riskier.

Security vs. convenience spectrum

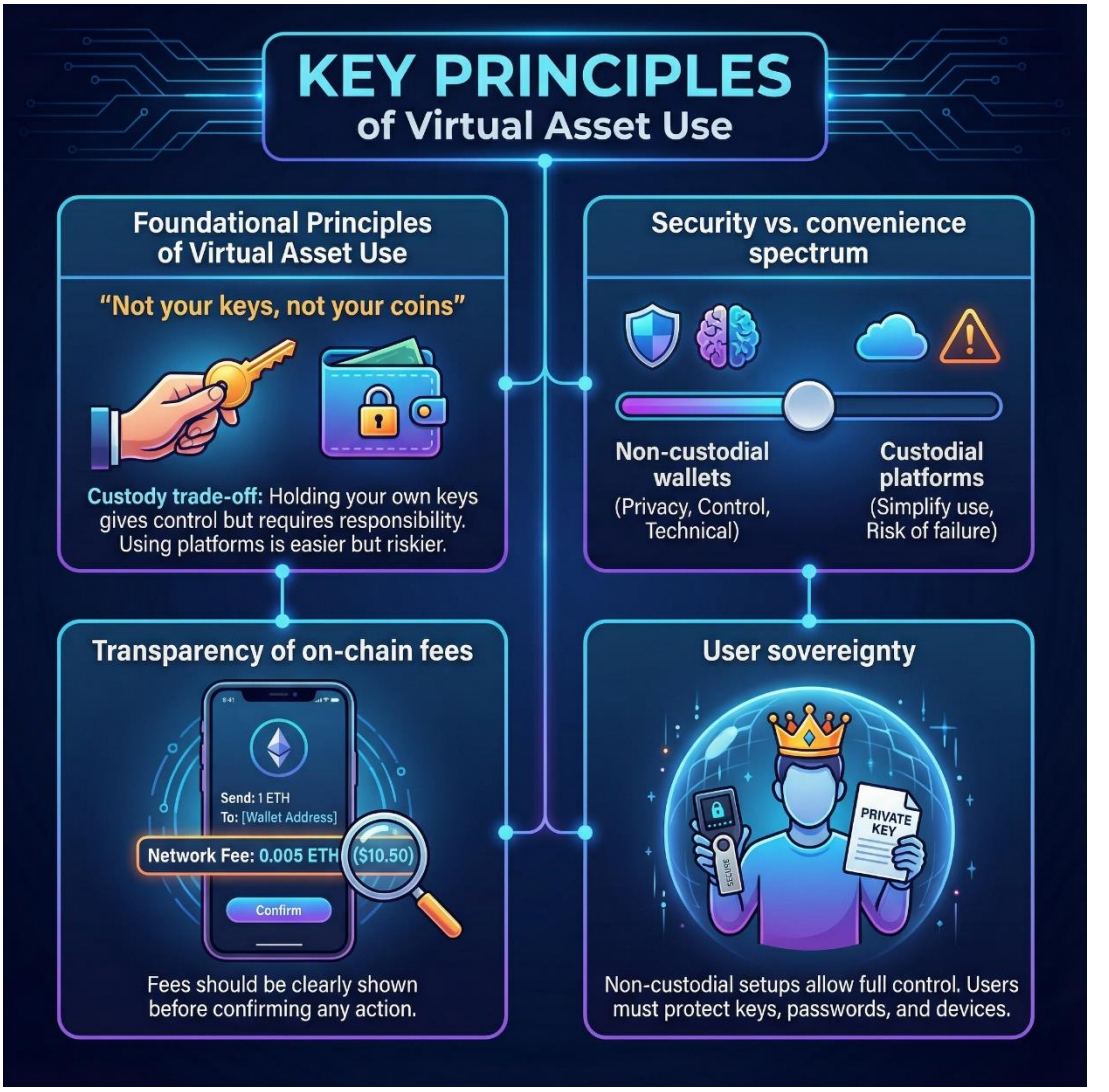
- ✓ Non-custodial wallets offer privacy and control but demand technical skill.
- ✓ Custodial platforms simplify use but expose users to platform failure or fraud.

Transparency of on-chain fees

- ✓ Every blockchain transaction has a fee.
- ✓ Fees should be clearly shown before confirming any action.

User sovereignty

- ✓ Non-custodial setups allow complete control over assets.
- ✓ Users must protect their keys, passwords, and devices to avoid loss.


KEY PRINCIPLES
of Virtual Asset Use
Foundational Principles of Virtual Asset Use
"Not your keys, not your coins"
Custody trade-off: Holding your own keys gives control but requires responsibility. Using platforms is easier but riskier.
Security vs. convenience spectrum
Non-custodial wallets
(Privacy, Control, Technical)
Custodial platforms
(Simplify use, Risk of failure)
Transparency of on-chain fees
Send: 1 ETH
To: [Wallet Address]
Network Fee: 0.005 ETH ($10.50)
Confirm
Fees should be clearly shown before confirming any action.
User sovereignty
PRIVATE KEY
SECURE
Non-custodial setups allow full control. Users must protect keys, passwords, and devices.

Links to National Consumer Protection Frameworks

- ✓ Correct tool usage is the first line of defence: Knowing how to use wallets, apps, and platforms safely protects users from scams and mistakes.

- ✓ Licensing of Virtual Asset Service Providers (VASPs): VASPs include exchanges, wallet providers, and platforms. Licensing ensures they meet safety, transparency, and accountability standards.

- ✓ Custodial tools require strong oversight: When users entrust their money to a platform, regulators must ensure that the platform is secure and lawful.

- ✓ Regulation supports safe innovation: Ghana's frameworks aim to protect citizens while allowing responsible digital growth.

SECTION 3: OPERATIONAL MECHANICS

How Systems Function

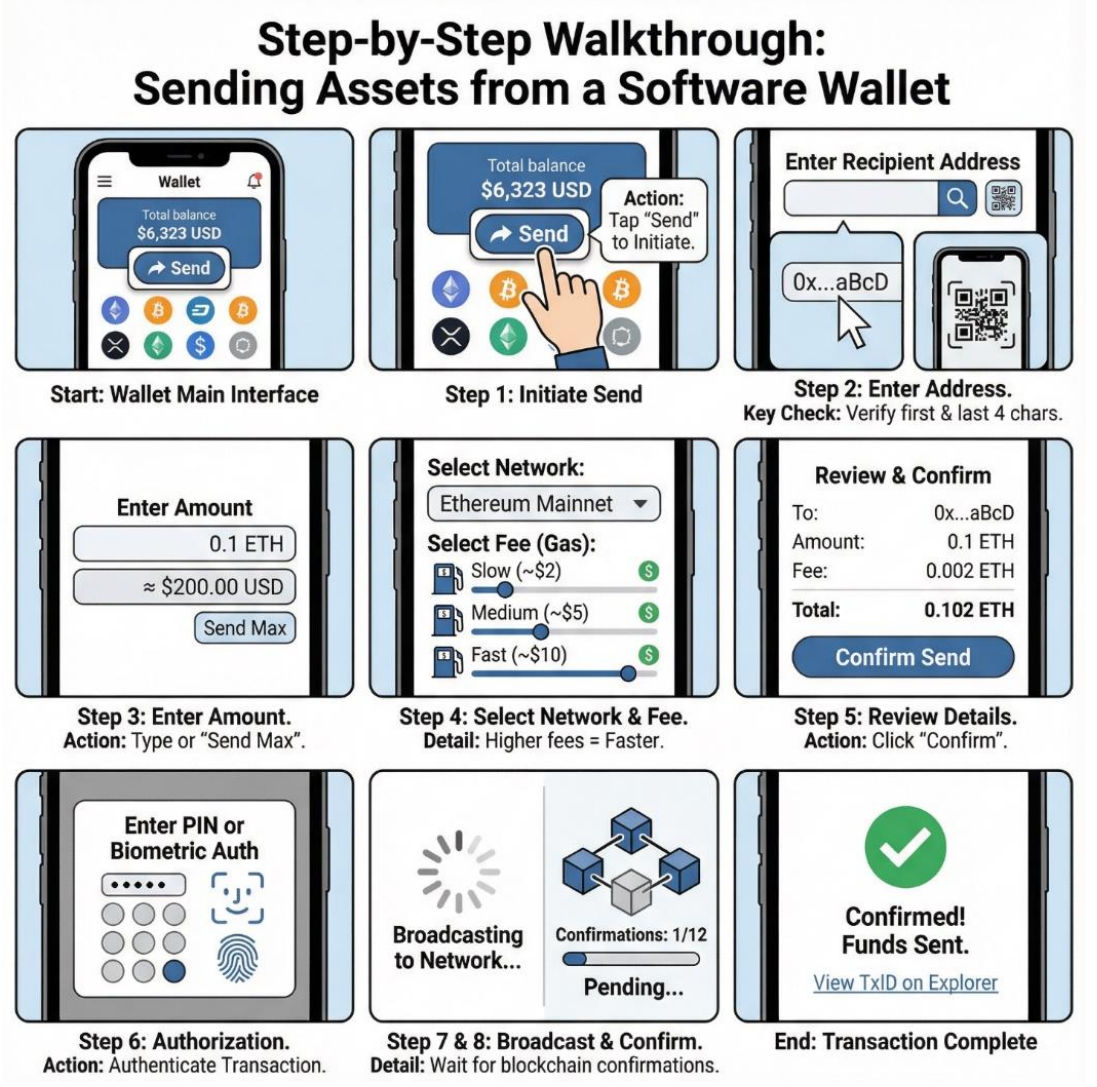
Sending digital assets from a software wallet to another address follows a structured process that balances user control, security, and network efficiency. The transaction begins when the user initiates a "Send" command within their wallet application. From there, the system guides the user through entering the recipient's address, specifying the amount, selecting the appropriate network and fee, and confirming the details before broadcasting the transaction to the blockchain. Each step is designed to ensure accuracy, prevent fraud, and provide transparency about costs and status.

This process also highlights the interactions among different actors: the user with their wallet software, the wallet communicating with the blockchain network, and, in custodial cases, the Virtual Asset Service Provider (VASP) maintaining internal records alongside blockchain transactions.

Step-by-Step Walkthrough: Sending Assets from a Software Wallet

1. Start: The process begins with the wallet's main interface.
2. Step 1: Initiate Send
    - ✓ Visual: Wallet home screen with "Send" or "Transfer" button.
    - ✓ Action: User taps/clicks to start a transaction.
3. Step 2: Enter Recipient Address
    - ✓ Visual: Address field with QR code icon.
    - ✓ Action: User pastes the recipient's public address (e.g., 0x…) or scans a QR code.
    - ✓ Key Check: Always verify the first and last four characters to avoid errors.
4. Step 3: Enter Amount
    - ✓ Visual: Input fields showing crypto amount and fiat equivalent.
    - ✓ Action: User types the amount or selects "Send Max."
5. Step 4: Select Network & Fee (Critical Step)
    - ✓ Visual: Dropdown for network choice and fee selector (Slow, Medium, Fast).
    - ✓ Detail: Fees (gas) pay miners/validators; higher fees = faster confirmation.
    - ✓ Action: User chooses fee tier based on urgency and cost.
6. Step 5: Review & Confirm
    - ✓ Visual: Summary screen showing recipient address, amount, estimated fee, and total debit.
    - ✓ Action: User clicks "Confirm" or "Approve."

7. Step 6: Authorisation
    - ✓ Visual: Pop-up requesting password, PIN, or biometric scan.
    - ✓ Action: User authenticates transaction.
8. Step 7: Broadcast & Pending
    - ✓ Visual: Loader icon with "Transaction Signed. Broadcasting to Network…"
    - ✓ Status: Transaction ID (TxID) generated; user can copy it.
9. Step 8: Network Confirmation
    - ✓ Visual: Blockchain blocks graphic with confirmation counter (e.g., 1/12).
    - ✓ Status: Exchanges typically require 3–12 confirmations before funds are considered final.
10. Step 9: Completion
    - ✓ Visual: Green checkmark icon.
    - ✓ Status: "Confirmed! Funds Received."
    - ✓ Detail: TxID becomes a clickable link to a blockchain explorer for verification.
11. End: Transaction is complete.


Step-by-Step Walkthrough:
Sending Assets from a Software Wallet
Wallet
Total balance
$6,323 USD
Send
Start: Wallet Main Interface
Total balance
$6,323 USD
Send
Action:
Tap "Send"
to Initiate.
Step 1: Initiate Send
Enter Recipient Address
0x...aBcD
Step 2: Enter Address.
Key Check: Verify first & last 4 chars.
Enter Amount
0.1 ETH
≈ $200.00 USD
Send Max
Step 3: Enter Amount.
Action: Type or "Send Max".
Select Network:
Ethereum Mainnet
Select Fee (Gas):
Slow (~$2)
Medium (~$5)
Fast (~$10)
Step 4: Select Network & Fee.
Detail: Higher fees = Faster.
Review & Confirm
To: 0x...aBcD
Amount: 0.1 ETH
Fee: 0.002 ETH
Total: 0.102 ETH
Confirm Send
Step 5: Review Details.
Action: Click "Confirm".
Enter PIN or
Biometric Auth
Step 6: Authorization.
Action: Authenticate Transaction.
Broadcasting
to Network...
Confirmations: 1/12
Pending...
Step 7 & 8: Broadcast & Confirm.
Detail: Wait for blockchain confirmations.
Confirmed!
Funds Sent.
View TxID on Explorer
End: Transaction Complete


Sending Assets from a Software Wallet:
A Step-by-Step Walkthrough
SEND
1. ENTER ADDRESS
2. ENTER AMOUNT
0 ETH
≈ $200.00 USD
3. SELECT FEE


Part 2: Review & Confirm
4. REVIEW DETAILS
To: 0x...aBCD
Amount: 0.1 ETH
Fee: 0.002 ETH
Total: 0.102 ETH
5. AUTHORIZE
6. BROADCASTING
7. CONFIRMED
FUNDS SENT

Technical Workflows

There are two primary transaction workflows:

Non-Custodial Flow (User-Led):

- ✓ The user directly controls their wallet and private keys.
- ✓ Transactions are signed locally and broadcast to the blockchain.
- ✓ The blockchain itself serves as the record of ownership and transfer.

Custodial Flow (Platform-Led)

- ✓ The user instructs a VASP (exchange or platform) to execute a transaction.
- ✓ The VASP updates its internal database to reflect balances.
- ✓ The platform then manages blockchain interactions on behalf of the user.

SECTION 4: LEGAL AND POLICY CONTEXT

Regulatory Foundations

Licensed Virtual Asset Service Providers (VASPs) are subject to strict consumer protection obligations. These obligations ensure that platforms handling digital assets maintain transparency, safeguard user funds, and provide clear information about risks. VASPs must comply with Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) requirements, which include monitoring transactions, reporting suspicious activity, and verifying customer identities.

A critical global standard is the Financial Action Task Force (FATF) Travel Rule, which requires VASPs to share sender and recipient information when transferring digital assets above certain thresholds. This rule helps prevent illicit flows of money and enables regulators to trace transactions when necessary. Compliance with these frameworks strengthens trust in the system and aligns Ghana with international best practices.

Institutional Mandates

Several national institutions play key roles in safeguarding consumers and overseeing virtual asset activity:

- Bank of Ghana (BoG):
  - ✓ Issues consumer warnings about unlicensed platforms.
  - ✓ Oversees licensing and supervision of VASPs.
  - ✓ Ensures that payment systems operate within legal boundaries.
- Securities and Exchange Commission (SEC):
  - ✓ Publishes alerts about fraudulent investment schemes.
  - ✓ Monitors platforms offering securities-like products in the crypto space.
  - ✓ Protects investors from scams promising unrealistic returns.
- Ghana Police Service – Cybercrime Unit:

- ✓ Investigates digital fraud, hacking, and scams.
- ✓ Provides enforcement support when criminal activity is detected.
- ✓ Works with regulators to protect the public from cyber threats.

Together, these institutions form a coordinated framework that balances innovation with consumer safety.

Applicable Guidelines

Regulators regularly issue public advisories, warning lists, and educational materials to guide consumers. These advisories highlight:

- ✓ Platforms operating without licenses.
- ✓ Known scams or fraudulent schemes.
- ✓ Safety practices for using wallets, exchanges, and mobile money services.

Warning lists are published to help consumers identify risky platforms before engaging with them. These guidelines serve as a practical tool for everyday decision-making, especially for individuals with limited technical knowledge.

Interpretation Considerations

While regulators provide oversight, advisories, and enforcement, the irreversible nature of blockchain transactions places a strong responsibility on individual users. Once a transaction is confirmed on the blockchain, it cannot be reversed or cancelled. This means that personal due diligence, such as verifying addresses, avoiding suspicious offers, and using licensed platforms, is essential.

Consumers must understand that regulatory protections exist, but they cannot undo mistakes made by users themselves. The safest approach combines institutional oversight with individual caution, ensuring that digital participation is both lawful and secure.

SECTION 5: RISK AND ASSURANCE

Professional Risk Categories

When dealing with virtual assets, professionals must be aware of the different categories of risk that can affect both individuals and institutions.

- *Operational Risk:* This arises from human error or technical mistakes. Common examples include sending assets to the wrong address, mistyping a wallet string, or losing access to private keys and seed phrases. Because blockchain transactions are irreversible, even minor errors can result in permanent loss of funds.

- *Counterparty Risk:* This occurs when a platform, exchange, or service provider fails to deliver on its obligations. For example, if a Virtual Asset Service Provider (VASP) becomes insolvent, is hacked, or engages in fraudulent activity, users may lose access to their funds. Counterparty risk is especially significant in custodial arrangements where users rely on third parties to safeguard their assets.

- *Cyber Risk:* This involves threats from malicious actors who compromise devices, networks, or accounts. Examples include phishing attacks, malware infections, SIM-swapping, or unauthorised access to wallets. Cyber risk is heightened because once an attacker gains control of private keys, they can drain funds instantly with no recourse.

Control Mechanisms

To mitigate these risks, professionals and institutions must adopt layered safeguards that combine technical tools with disciplined practices.

- *Double-Checking Addresses:* Always verify the first and last four characters of a recipient's wallet address before sending funds. Fraudsters often use look-alike addresses to trick users.

- *Hardware Wallets:* For significant sums or long-term storage, hardware wallets provide offline protection against cyberattacks. They isolate private keys from internet-connected devices, reducing exposure to malware.

- *Two-Factor Authentication (2FA):* Enabling 2FA on all accounts adds an extra layer of security. Even if passwords are compromised, attackers cannot access accounts without the second factor (e.g., an SMS code, an authenticator app, or a biometric scan).

- *Regular Updates and Patches:* Keeping wallet software, mobile apps, and operating systems updated ensures that known vulnerabilities are patched.

- *Segregation of Funds:* Professionals should separate operational funds from reserve holdings, reducing exposure if one wallet or account is compromised.

Oversight Responsibilities

Risk management is not only an individual duty but also an institutional obligation.

- *Individual Responsibility:* Every user must safeguard their private keys and seed phrases. These are the ultimate access credentials to digital assets, and losing them means permanently losing control. Individuals should store seed phrases offline, in secure physical formats, and never share them electronically.

- *Institutional Responsibility:* For banks, financial institutions, and corporate entities, oversight extends to procurement and governance. Staff and administrators must follow approved procurement channels when acquiring or deploying virtual asset tools. This ensures that only licensed, vetted, and secure platforms

are used. Institutions must also enforce internal policies for wallet management, access control, and audit trails to prevent misuse or fraud.

- *Shared Accountability:* While regulators provide frameworks and oversight, the irreversible nature of blockchain transactions means that both individuals and institutions must act responsibly. Institutions should train staff on safe practices, while individuals must remain vigilant in their personal use. Together, these responsibilities create a culture of security and compliance.


VIRTUAL ASSET PROFESSIONAL RISKS & SAFEGUARDS
PROFESSIONAL RISK CATEGORIES
OPERATIONAL RISK
WALLET ADDRESS
LOST
HUMAN ERROR, TECHNICAL MISTAKES, IRREVERSIBLE LOSS
COUNTERPARTY RISK
PLATFORM FAILURE, HACKS, FRAUD, THIRD-PARTY RELIANCE
CYBER RISK
MALICIOUS ACTORS, COMPROMISED DEVICES, PRIVATE KEY THEFT
CONTROL MECHANISMS
DOUBLE-CHECKING ADDRESSES
HARDWARE WALLETS
OFFLINE STORAGE
TWO-FACTOR AUTHENTICATION (2FA)
6006
REGULAR UPDATES
SEGREGATION OF FUNDS
TREAS
FUNDS
OVERSIGHT RESPONSIBILITIES
INDIVIDUAL RESPONSIBILITY
SAFEGUARD PRIVATE KEYS, OFFLINE STORAGE
INSTITUTIONAL RESPONSIBILITY
CORPORATE
GOVERNANCE, PROCUREMENT, INTERNAL POLICIES
SHARED ACCOUNTABILITY
REGULATORY FRAMEWORKS, STAFF TRAINING, VIGILANCE, CULTURE OF SECURITY

SECTION 6: Practical Applications

- **Tools:** Demonstration of a reputable software wallet (e.g., Trust Wallet demo mode); exploration of a licensed Ghanaian VASP's public website/app interface.
- **Procedures:** Checklist for setting up a new wallet securely: download from the official source, write down the seed phrase offline, enable all security features, and send a tiny test transaction first.
- **Evaluation of Scenarios:** Given two platform options, which has clearer fee structures, better security features, and verifiable licensing?
- **Good Practice Guides: The "1% Test Rule"**: Before committing significant funds, test the entire process (deposit, trade, withdrawal) with a minimal amount (1% or less).

SECTION 7: Discussion Points and Reflection

- **Points for Deeper Thinking:** Is the convenience of a custodial platform worth the trust you place in it?
- **Policy Questions:** Should there be public awareness campaigns on seed phrase security, similar to PIN security for ATM cards?
- **Ethical Considerations:** As a technician or IT officer, what advice should you give to colleagues about storing wallet backups on work computers?
- **Sector-specific Reflections: Bank Staff**: How do bank-grade custodial services for Virtual Assets compare to traditional asset custody? **NGO Officers:** What are the tool considerations for receiving/disseminating aid in digital assets?

Assessment Strategy

- Hands-on exercise: Successfully set up a demo wallet and explain the security steps taken.
- Checklist activity: Evaluate the safety features of a provided screenshot of a platform interface.
- Quiz on wallet types, key terminology, and sources of transaction costs.
    i. Scenario Analysis: Kwame stores his crypto on an exchange for easy trading. Ama uses a hardware wallet she keeps at home. Compare their exposure to platform risk vs. personal security risk.
    ii. Screenshot Analysis: Given an image of a wallet transfer screen with a pre-filled, very low network fee, what is the likely trade-off the user is facing?
    iii. Checklist Creation: List three essential checks you must perform before depositing funds into a new virtual asset platform.
    iv. True or False (with justification): "A multi-signature wallet setup is only necessary for large businesses, not for individual users."
    v. Compare & Contrast: What is the core difference between a "public key" and a "private key" in terms of their function and secrecy?
    vi. Ordering: Sequence these steps for securing a new software wallet: a) Test a slight recovery, b) Write down the 12-word phrase, c) Choose a strong app password, d) Generate a new wallet.
    vii. Identify the Risk: A platform offers "guaranteed 20% monthly returns" if you lock your tokens in their wallet. Which specific risk type from the module does this most clearly signal?
    viii. Matching: Match the custody type (Custodial, Non-Custodial) to its characteristic (e.g., "User is responsible for own backup and security").

ix. Short Answer: Why might transaction fees on a blockchain network like Bitcoin sometimes become very high?
x. Prediction: If you lose the device containing your non-custodial wallet but have your recovery phrase, what can you do?

MODULE SUMMARY PAGE

- *Key Insights:* The choice of tools involves a direct trade-off between user control/security and convenience. All interactions incur costs and require careful verification steps.
- *Applications to Professional Roles:* Enables safe personal engagement and provides criteria for assessing or recommending tools in a professional capacity.
- *Key Risks:* Irreversible loss from lost keys or mistaken addresses; loss from using unsecured or fraudulent platforms.
- *Next Steps:* Proceed to Module 3 to understand the specific risks, scams, and consumer protection strategies in the virtual asset ecosystem.

END OF MODULE

Module 3

Title: Markets, Risks, and Consumer Protection

Module Purpose

This module is the essential **"reality check"** for Ghana's journey into virtual assets. It explores the two sides of the coin: the transformative economic potential of this technology and the critical risks that must be managed to protect consumers and ensure financial stability. It will move from understanding sophisticated scams to designing practical solutions, all within the Ghanaian context. Specifically, it will;

- Frame the principal risk domains (user, firm, system-level) and prevalent abuse patterns in the virtual asset ecosystem.
- Equip participants with a high-level pathway for prevention, incident response, and escalation, instilling practical habits for safe participation consistent with good consumer-protection practice.

Module Learning Outcomes

By the end of this module, participants will be able to:

1. Classify key risk types relevant to users, firms, and the wider financial system.
2. Recognise hallmark behavioural and technical indicators of fraud, scams, and market misconduct.
3. Describe general pre-engagement behaviours and digital hygiene practices that reduce exposure to harm.
4. Outline a structured incident-response and escalation pathway, including steps for evidence preservation and reporting to appropriate authorities in Ghana.

The Risk Landscape: Familiar Threats and New Challenges

The risks facing users of virtual assets fall into two broad categories. Some are well-known from traditional finance. Others are new and arise from the unique features of virtual asset systems.

Traditional Financial Risks

These risks have existed for many years and are already addressed by established financial controls and regulatory experience.

- ✓ Fraud: Deliberate deception where criminals lie or misrepresent information to take money from others.
- ✓ Ponzi Schemes: Fraudulent arrangements where early participants are paid using money from new participants instead of real profits.
- ✓ Money Laundering: Attempts by criminals to hide the origin of illegally obtained funds by moving them through financial systems.

Financial regulators and institutions have built long-standing systems to detect, prevent, and respond to these threats.

Crypto-Native Risks

Virtual assets introduce risks that do not exist in traditional financial systems. These risks require new awareness, new skills, and new safety practices. Virtual assets are powerful tools. Like any powerful tool, they can be used productively or cause serious harm if handled without care. The goal is not avoidance, but informed and responsible use.

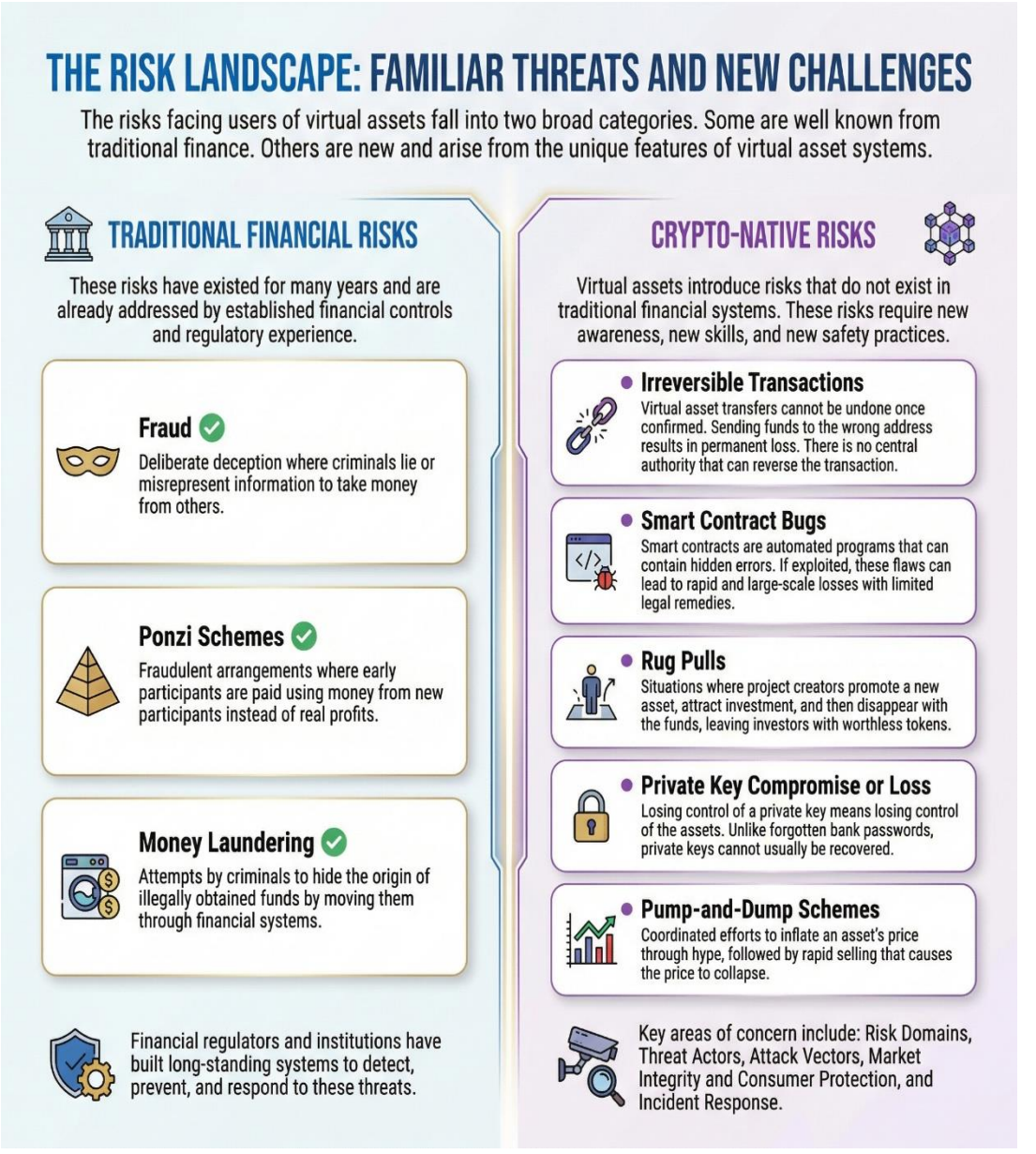
Key areas of concern include:

- ✓ Risk Domains: User-level risks, platform risks, and market-level risks.
- ✓ Threat Actors: Hackers, scammers, dishonest developers, and organised fraud groups.
- ✓ Attack Vectors: Techniques such as phishing, social engineering, and fake platforms are used to trick users.
- ✓ Market Integrity and Consumer Protection: Risks that affect fairness, transparency, and trust in virtual asset markets.
- ✓ Incident Response: The actions required when something goes wrong, including evidence collection and reporting.

Key Technical Risk Concepts

- ✓ Irreversible Transactions: Virtual asset transfers cannot be undone once confirmed. Sending funds to the wrong address results in permanent loss. There is no central authority that can reverse the transaction.
- ✓ Smart Contract Bugs: Smart contracts are automated programmes that can contain hidden errors. If exploited, these flaws can lead to rapid and large-scale losses with limited legal remedies.
- ✓ Rug Pulls: Situations where project creators promote a new asset, attract investment, and then disappear with the funds, leaving investors with worthless tokens.
- ✓ Private Key Compromise or Loss: Losing control of a private key means losing control of the assets. Unlike forgotten bank passwords, private keys cannot usually be recovered.
- ✓ Pump-and-Dump Schemes: Coordinated efforts to inflate an asset's price through hype, followed by rapid selling that causes the price to collapse.

- ✓ Two-Factor Authentication (2FA): A critical security measure that requires two forms of verification, such as a password and a one-time code, to reduce unauthorised access.



Professional Relevance

Understanding these risks is essential for protecting both personal and organisational assets. For individuals working in administration, education, and frontline services, this knowledge supports informed decision-making, practical guidance to others, and strong operational security.

SECTION 2: KEY PRINCIPLES

- ✓ "If it seems too good to be true, it probably is": Fraudsters often lure victims with promises of unusually high returns or guaranteed profits. Any scheme offering unrealistic benefits should be treated with suspicion.
- ✓ Security is a layered practice (defence in depth): Protecting digital assets requires multiple safeguards: strong passwords, PIN protection, biometric authentication, secure devices, and trusted platforms. No single measure is enough; layers of defence reduce risk.
- ✓ Time pressure is a key weapon for fraudsters: Scammers frequently create urgency ("Act now or lose out!") to prevent victims from thinking carefully. Users should pause, verify, and consult trusted sources before making decisions.
- ✓ Personal responsibility in decentralised systems: In non-custodial setups, users are their own "bank." Losing private keys, sharing PINs, or ignoring safety practices can result in permanent loss of funds. Responsibility cannot be outsourced.
- ✓ Transparency and vigilance: Always check transaction details, fees, and recipient addresses. Fraud often exploits small mistakes, such as mis-typed addresses or hidden charges.
- ✓ Awareness of evolving risks: Fraud tactics change over time, from fake apps to phishing links. Continuous learning and scepticism are essential for safe participation in digital markets.

Links to Frameworks

- ✓ National Cybersecurity Awareness Initiatives: Ghana's cybersecurity programmes emphasise safe digital practices, including password hygiene, device protection, and scam awareness. Virtual asset safety aligns directly with these national campaigns.
- ✓ Financial Consumer Protection Regulations: Regulatory bodies such as the Bank of Ghana and the Securities and Exchange Commission (SEC) enforce rules to protect consumers from fraud, mismanagement, and unsafe platforms. Licensing requirements ensure that service providers meet minimum accountability standards.
- ✓ Law Enforcement Mandates: Agencies like the Cybercrime Unit of the Ghana Police Service and the Economic and Organised Crime Office (EOCO) investigate fraud, scams, and illegal financial activities. Users are encouraged to report suspicious activity promptly to these authorities.
- ✓ Integration with Global Standards: Ghana's frameworks align with international best practices, such as the Financial Action Task Force (FATF) guidelines on anti-money laundering and combating the financing of terrorism. This ensures consistency and credibility in global financial markets.
- ✓ Community-Level Protection: Consumer protection is not only institutional but also communal. Trusted agents, community leaders, and peer educators play a vital role in spreading awareness and guiding safe practices, especially for low-literacy groups.

How Abuse and Attacks Work in Practice

Virtual asset misuse often follows predictable patterns. Understanding these patterns helps users and professionals recognise danger early and respond correctly.

a. How a Phishing Attack Works

A phishing attack is designed to trick a user into giving away access details. It usually unfolds in three main stages.

Stage 1: Deceptive Message

The attacker sends a message that looks legitimate. This message may appear to come from a wallet provider, an exchange, a bank, a regulator, or a trusted contact.

Common tactics include:

- Urgent warnings such as "Your account is at risk"
- Requests to "verify" or "secure" an account
- Fake links that look similar to real websites

The goal at this stage is to create fear, urgency, or trust.

Stage 2: Credential Harvesting

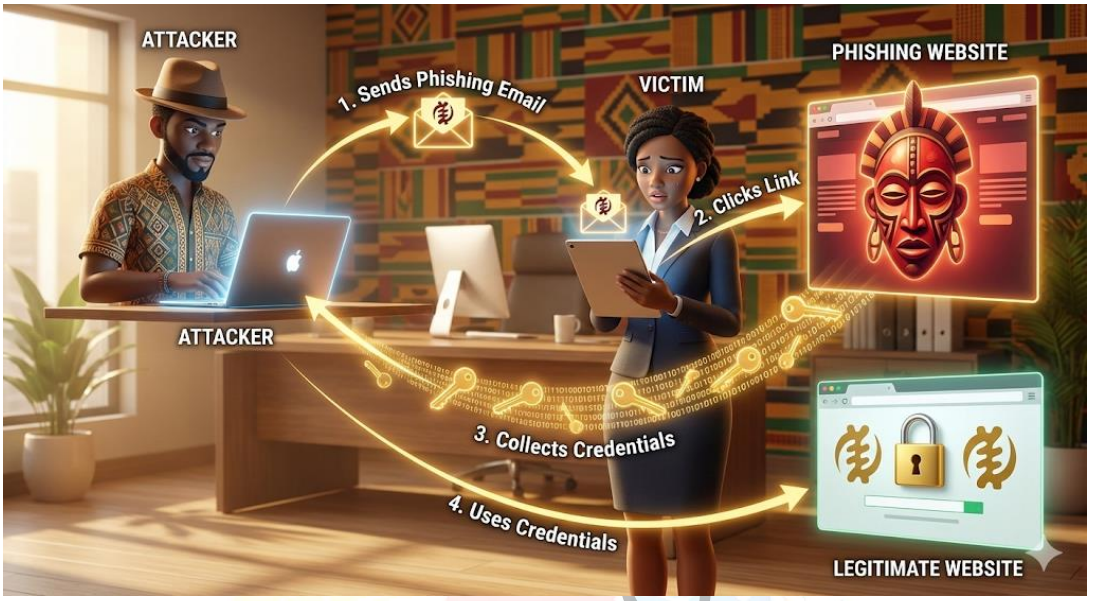
When the victim clicks the link or responds, they are taken to a fake website or app. This page is designed to copy the real platform's appearance. The victim is asked to enter:

- Passwords
- PINs
- Private keys
- Seed phrases
- One-time codes

Once entered, the attacker captures this information.

Stage 3: Asset Theft

With valid credentials, the attacker immediately gains access to the victim's wallet or account. Virtual assets are transferred out, often to multiple addresses, making tracing difficult. Because virtual asset transactions are irreversible, recovery is usually impossible.



b. How a "Rug Pull" Unfolds

A rug pull is a form of project-based fraud that often involves newly launched tokens or platforms.

Stage 1: Malicious Project Development

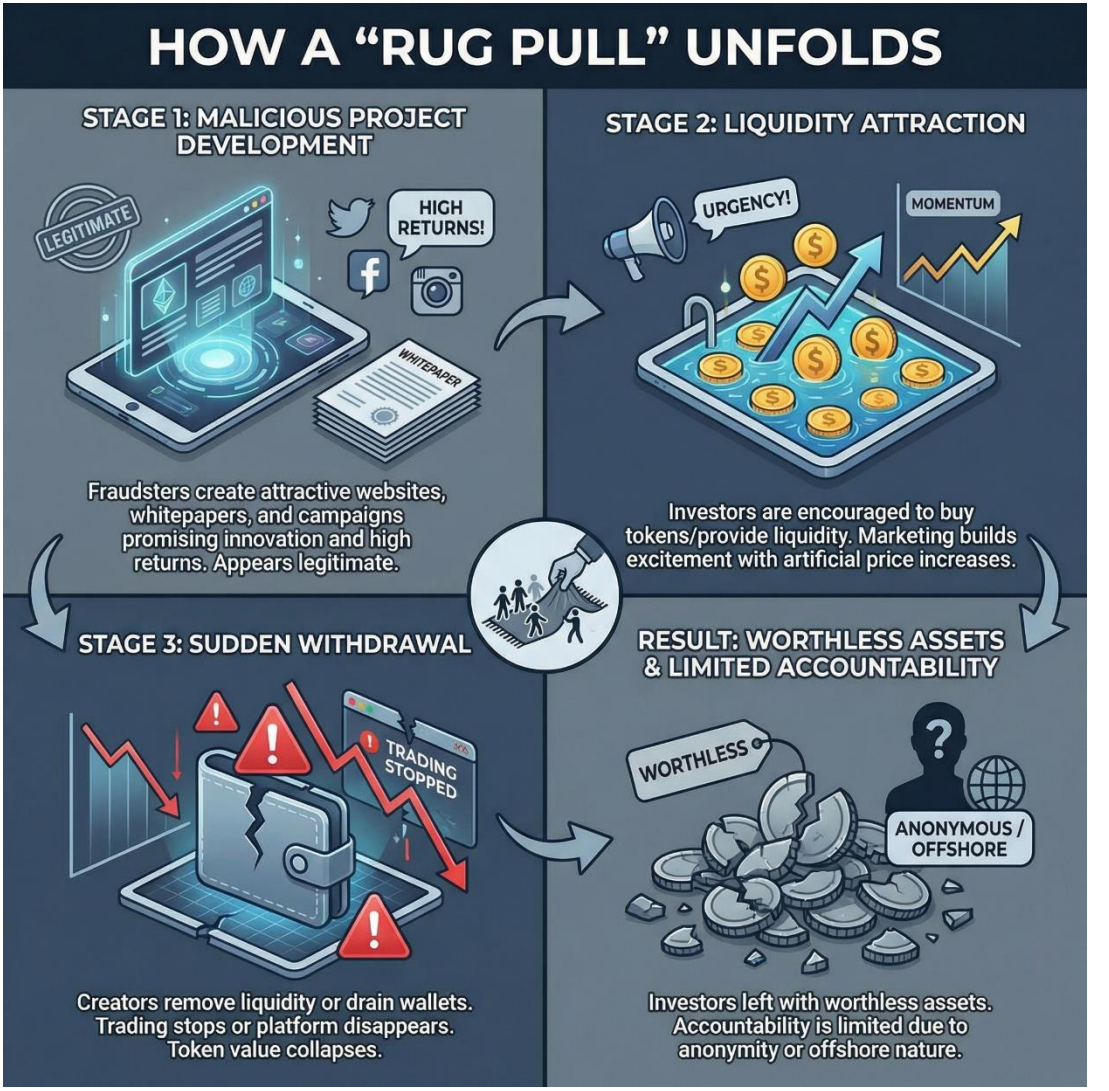
The fraudsters create a new virtual asset project. They publish attractive websites, whitepapers, and social media campaigns. The project promises innovation, high returns, or exclusive early access. At this stage, the project appears legitimate.

Stage 2: Liquidity Attraction

Investors are encouraged to buy the token or provide liquidity. Marketing focuses on urgency and early participation. Price increases are often artificially supported to build excitement and trust. More users join, believing the project is gaining momentum.

Stage 3: Sudden Withdrawal

Once enough funds are locked in, the creators remove liquidity or drain project wallets. Trading stops, or the platform disappears. The token's value collapses, leaving investors with worthless assets. Because the project was often anonymous or offshore, accountability is limited.



c. Interactions Among Key Actors

Understanding who interacts with whom clarifies how these incidents play out.

Fraudster ↔ Victim

The fraudster directly targets the victim through messages, fake platforms, or investment offers. This interaction relies on deception, pressure, and manipulation.

Fraudster ↔ Platform

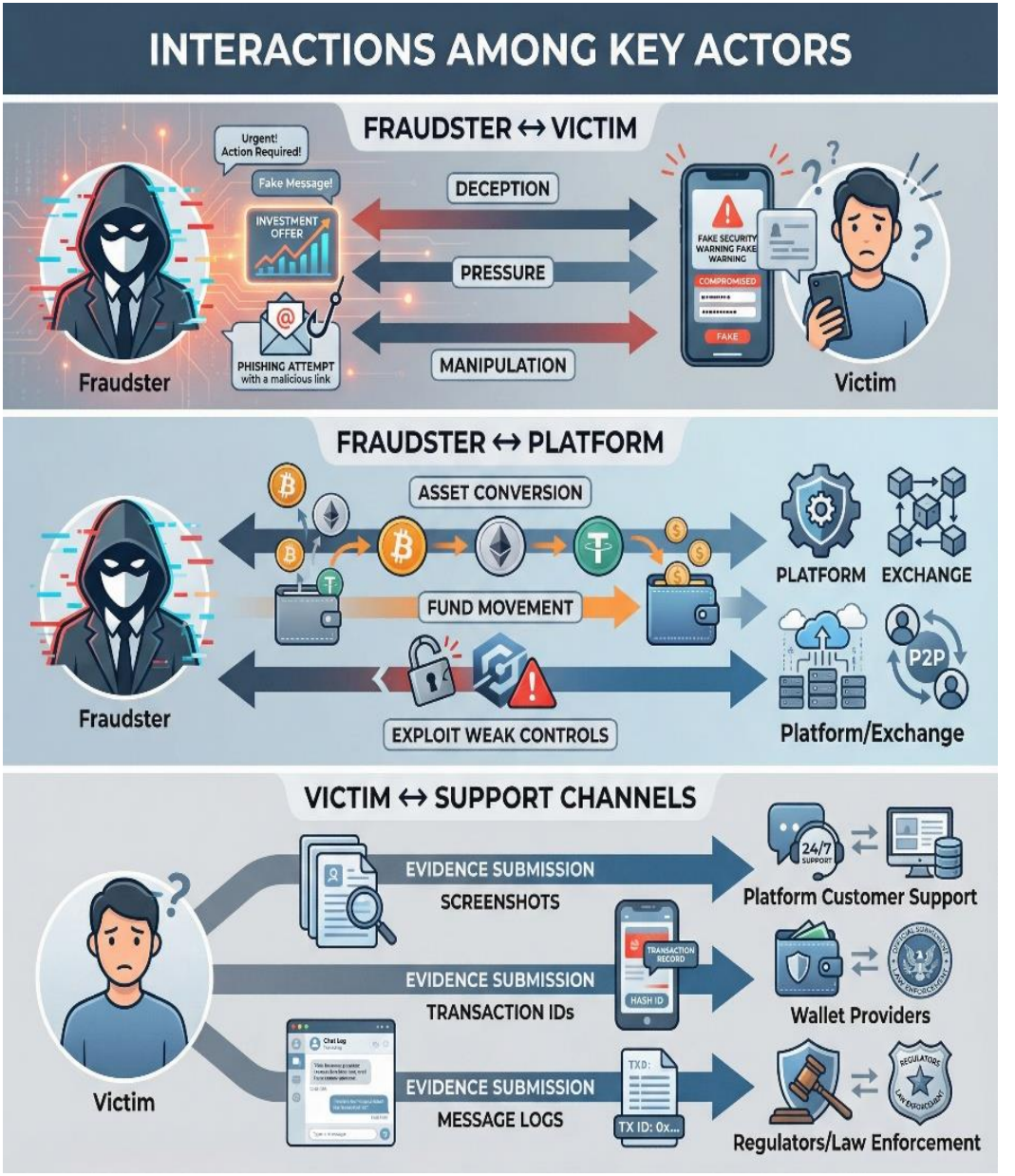
After stealing assets, the fraudster may use platforms or exchanges to convert or move funds. They may exploit weak controls, poor monitoring, or multiple platforms to cash out.

Victim ↔ Support Channels

Once the victim realises something is wrong, they interact with:

- Platform customer support
- Wallet providers
- Regulators or law enforcement

At this stage, evidence such as screenshots, transaction IDs, and message logs becomes critical.


INTERACTIONS AMONG KEY ACTORS
FRAUDSTER ↔ VICTIM
Urgent! Action Required!
Fake Message!
INVESTMENT OFFER
PHISHING ATTEMPT with a malicious link
Fraudster
DECEPTION
PRESSURE
MANIPULATION
FAKE SECURITY WARNING FAKE WARNING
COMPROMISED
FAKE
Victim
FRAUDSTER ↔ PLATFORM
ASSET CONVERSION
FUND MOVEMENT
EXPLOIT WEAK CONTROLS
Fraudster
PLATFORM
EXCHANGE
P2P
Platform/Exchange
VICTIM ↔ SUPPORT CHANNELS
Victim
EVIDENCE SUBMISSION
SCREENSHOTS
EVIDENCE SUBMISSION
TRANSACTION IDs
EVIDENCE SUBMISSION
MESSAGE LOGS
TRANSACTION RECORD
HASH ID
TX ID: 0x...
24/7 SUPPORT
Platform Customer Support
Wallet Providers
Regulators/Law Enforcement

Key Takeaway

Phishing and rug pulls do not happen by accident. They follow clear, repeatable steps that rely on urgency, trust, and lack of verification. Understanding these mechanics helps individuals and institutions spot warning signs early, reduce losses, and respond effectively when incidents occur.

SECTION 4: LEGAL AND POLICY CONTEXT

- **Regulatory Foundations**: Consumer protection obligations of licensed VASPs. Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) reporting requirements are all in compliance with the FATF Travel Rule.
- **Institutional Mandates:** Roles of the Bank of Ghana (consumer warnings, VASP oversight), Securities and Exchange Commission (investment scam alerts), and the Police Cybercrime Unit (investigation).
- **Applicable Guidelines:** Public advisories and warning lists published by regulators.
- **Interpretation Considerations:** Understanding that while regulators provide warnings and oversight, the irreversible nature of many transactions places a strong onus on individual due diligence.

SECTION 5: RISK AND ASSURANCE

Professional Risk Categories

Professionals working with virtual assets face several categories of risk that can affect both individuals and institutions.

- ✓ Financial Loss: The most immediate risk is the loss of funds due to errors, fraud, or theft. Sending assets to the wrong address, falling for phishing schemes, or engaging with unlicensed platforms can result in irreversible financial losses.
- ✓ Identity Theft: Cybercriminals often target personal information such as login credentials, identification documents, or biometric data. Once stolen, these details can be used to impersonate professionals, open fraudulent accounts, or authorise unauthorised transactions.
- ✓ Reputational Damage: For businesses and professionals, association with scams, failed transactions, or poor security practices can erode trust among clients, partners, and regulators. Reputation is a critical asset in financial services, and damage can have long-term consequences.
- ✓ Compliance Failure: Staff in regulated roles must adhere to strict rules around anti-money laundering (AML), combating the financing of terrorism (CFT), and consumer protection. Failure to comply, whether through negligence or lack of training, can lead to regulatory penalties, legal consequences, and institutional risk.

Control Mechanisms

To mitigate these risks, organisations and individuals must adopt robust control mechanisms that combine technical safeguards with disciplined practices.

- ✓ Pre-Engagement Verification Checklists: Before engaging with a platform, transaction, or client, professionals should verify

licenses, regulatory status, and authenticity. Checklists ensure that no critical step is overlooked.

- ✓ Hardware Security Keys: For high-value accounts or sensitive roles, hardware security keys provide strong protection against phishing and unauthorised access. They act as a physical second factor, making it nearly impossible for attackers to compromise accounts remotely.
- ✓ Regular Security Training: Continuous education ensures that staff remain aware of evolving threats such as ransomware, social engineering, and new scam tactics. Training should include simulations, case studies, and updates on regulatory requirements.
- ✓ Adherence to Organisational IT Policies: Institutions must enforce policies covering password hygiene, device management, access control, and data handling. Compliance with these policies ensures consistency and reduces vulnerabilities across the organisation.

Oversight Responsibilities

Risk assurance requires clear delineation of responsibilities at both the individual and institutional levels.

- ✓ Individual Responsibility: Each professional is accountable for their own digital hygiene. This includes safeguarding passwords, private keys, and seed phrases, avoiding suspicious links, and ensuring devices are secure. Personal vigilance is the first line of defence against fraud and cyberattacks.
- ✓ Supervisory Responsibility: Supervisors and administrators must ensure that staff handling virtual assets or sensitive data are adequately trained and equipped. This includes verifying that employees follow approved procurement channels, adhere to IT policies, and understand compliance obligations.
- ✓ Institutional Responsibility: Organisations must establish governance frameworks that include monitoring, audits, and incident response protocols. Institutions should also provide

resources, such as secure infrastructure, licensed platforms, and clear escalation procedures, to address suspected fraud or breaches.

Assurance Outcomes

When these risk categories, control mechanisms, and oversight responsibilities are properly integrated, institutions achieve stronger assurance outcomes. These include:

- ✓ Reduced likelihood of financial and reputational losses.
- ✓ Greater resilience against cyber threats.
- ✓ Improved compliance with national and international regulations.
- ✓ Enhanced trust among clients, regulators, and the wider community.

SECTION 6: PRACTICAL APPLICATIONS

- **Tools:** Password managers, authenticator apps for 2FA, official regulator websites for scam alerts.
- **Procedures:** Step-by-step guide for verifying a platform: 1) Check BoG/SEC register. 2) Google "[Platform Name] + scam". 3) Verify official website URL. 4) Look for professional whitepaper/team info.
- **Evaluation of Scenarios**: Workshop analysing sample scam messages (email, SMS, social media) to identify red flags.
- **Good Practice Guides: The "24-Hour Rule":** Impose a mandatory 24-hour reflection period before acting on any unsolicited financial opportunity.

SECTION 7: DISCUSSION POINTS AND REFLECTION

- **Points for Deeper Thinking**: Why are even financially literate professionals vulnerable to sophisticated scams?
- **Policy Questions:** What more can be done to improve the speed and public awareness of regulator-issued scam alerts?
- **Ethical Considerations**: What is your responsibility if you see a family member or client about to fall for a virtual asset scam?
- **Sector-specific Reflections**: Nurses/Teachers: How to discuss these risks with less tech-savvy community members? Junior

Military/Police Officers: How does this relate to general crime prevention duties?

Assessment Strategy

i. **Scenario:** You receive a WhatsApp message from a number claiming to be "BoG Support," asking you to validate your wallet to avoid suspension. Based on common fraud patterns, list two immediate red flags.
ii. **Evidence Preservation:** What three pieces of information are most critical to screenshot and save if you suspect a fraudulent transaction?
iii. **Compare & Contrast:** How does a "Ponzi scheme" differ from a legitimate, albeit high-risk, business investment?
iv. **True or False** (with justification): "Enabling Two-Factor Authentication (2FA) using SMS is just as secure as using an authenticator app."
v. **Ordering:** Prioritise these immediate actions after discovering unauthorised access to your exchange account: a) Post about it on social media, b) Change your password and enable 2FA, c) Contact the platform's official support, d) Run a full antivirus scan.
vi. **Identify the Tactic**: A social media group constantly posts about a coin's "imminent explosion" and urges members to buy now. What market manipulation scheme is this?
vii. F**OMO:** In the "rug pull" case studied, what behaviour by the project developers before the collapse could have been a warning sign to investors?
viii. **Matching**: Match the risk category (Operational, Cyber, Social Engineering) to an example (e.g., "A hacker exploits a bug in a wallet's code").
ix. **Short Answer:** Why is "pressure to act quickly" such a common element in scams?

x. **Prediction:** If you report a scam to the Police Cybercrime Unit, what kind of evidence (from your preserved records) will be most useful to them?

MODULE SUMMARY PAGE

- **Key Insights:** Risk is inherent and multifaceted; however, most losses stem from exploitable behaviours, not technical failures. A cautious, informed, and verified approach is the most vigorous defence.
- **Applications to Professional Roles:** Empowers participants to protect themselves, their families, and their organisations. Provides a framework for educating others and contributing to a safer digital environment.
- **Key Risks:** Financial loss from scams, identity theft, and making rushed decisions under pressure.
- **Next Steps:** Proceed to Module 4 to understand the formal regulatory structures, licensed entity obligations, and official recourse channels that underpin consumer protection in Ghana.

END OF MODULE

Module 4

Module Title: Law and Regulatory Perimeter

Module Purpose

We have journeyed from the "what" and "how" of virtual assets to the crucial question of "how should they be governed?" This module provides the essential "rulebook," exploring the universal principles and models that guide nations in building their regulatory frameworks. The approach here is strictly policy-neutral, as the intention is not to debate Ghana's specific choices. Instead, the aim is to equip Ghanaians with the foundational knowledge to understand why specific rules exist and to engage thoughtfully with any future regulatory framework. In particular, the purpose is;

- To provide a clear, policy-neutral overview of Ghana's regulatory framework for virtual assets, focusing on the Virtual Asset Service Provider (VASP) Bill and related guidelines.
- To clarify the high-level obligations of regulated entities, distinguish between entity authorisation and asset treatment, and map the official channels for consumer recourse and staying informed.

Module Learning Outcomes

By the end of this module, participants will be able to:

1. Identify, in broad terms, the activities typically within the scope of virtual assets regulation (e.g., exchange, custody, transfer).
2. Differentiate the authorisation (licensing) of entities from the treatment of specific virtual assets or offerings.

3. Summarise shared governance, conduct, and financial crime control expectations for licensed Virtual Asset Service Providers (VASPs).
4. Describe practical steps to verify the authorisation status of a service provider and stay updated as national policies and guidance evolve.

SECTION 1: CONCEPT OVERVIEW

Why Virtual Asset Rules Exist

Regulation is not about stifling innovation. It is about building the guardrails and traffic lights that allow a new, high-speed digital highway to be used safely by everyone. This module explores the blueprint for those guardrails.

Part 1: The "Why" - Core Public Policy Objectives

Nations regulate virtual assets for four fundamental reasons that protect the public and ensure stability:

i. Market Integrity & Investor Protection: To ensure markets are fair and transparent, and to protect citizens from fraud, manipulation, and the extreme volatility we discussed in Module 3. This is about creating a level playing field.
ii. Financial Stability & Prudential Soundness: To prevent the failure of a major virtual asset company from causing a domino effect that could destabilise the entire traditional financial system. This means ensuring these companies are well-managed and have adequate financial buffers.
iii. Combating Illicit Finance (AML/CFT): To prevent virtual assets from being used as a tool for money laundering or terrorist

financing. This involves creating transparent trails that law enforcement can follow.

iv. Monetary Sovereignty & Consumer Protection: To preserve the central bank's role in managing the national currency and to ensure consumers are treated fairly, with clear rights and avenues for recourse.

Part 2: The "What" - Defining the Playing Field

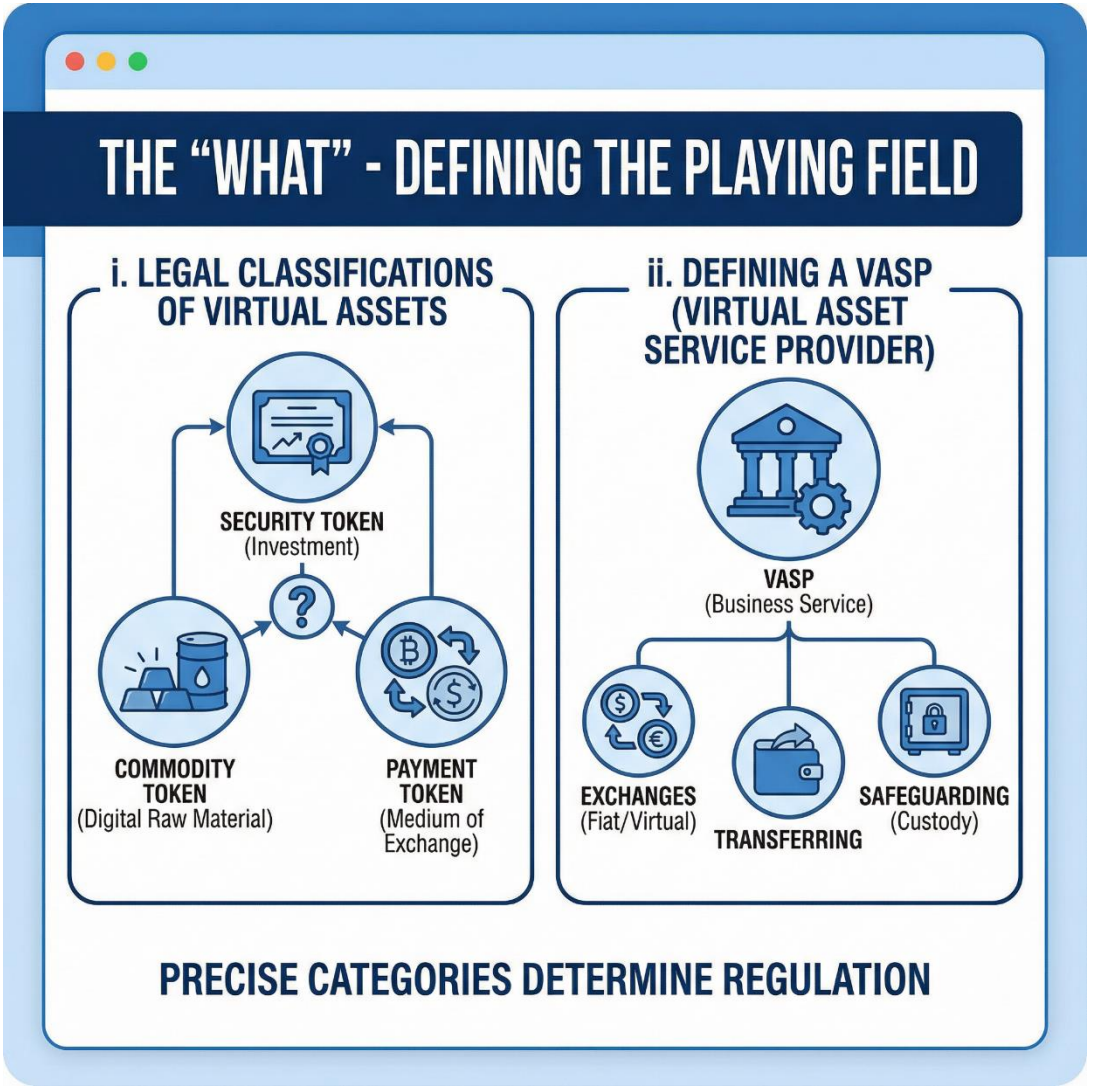
Before something can be regulated, it must first be defined. The law creates precise categories.

i. Legal Classifications of Virtual Assets: Is a token, a security, a commodity, or a payment token? This is not an academic question; it determines which regulator is in charge and what rules apply. Various aspects of this classification are defined as follows

- ✓ A Security Token is treated like a stock or bond, as it represents an investment in a common enterprise.
- ✓ A Commodity Token is treated like a digital raw material, such as gold or oil.
- ✓ A Payment Token (like bitcoin) is primarily designed to be used as a medium of exchange.

ii. Defining a VASP (Virtual Asset Service Provider) is the law that focuses on the service, not the asset. A VASP is any business that provides a service on behalf of others, such as:

- ✓ Exchanges between virtual assets and fiat currencies.
- ✓ Transferring virtual assets.
- ✓ Safeguarding and administering virtual assets (custody).

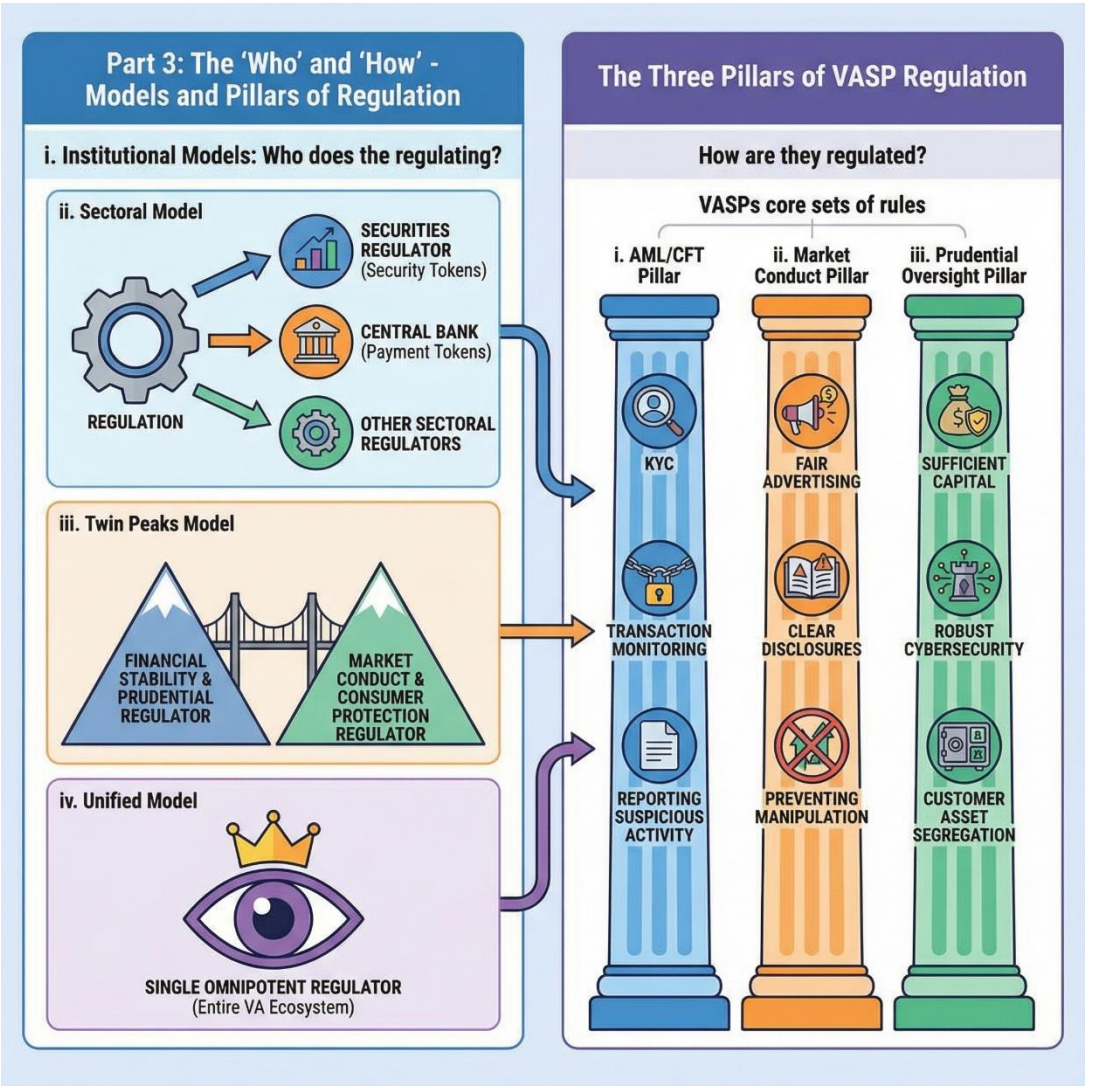

THE "WHAT" - DEFINING THE PLAYING FIELD
i. LEGAL CLASSIFICATIONS OF VIRTUAL ASSETS
SECURITY TOKEN
(Investment)
?
COMMODITY TOKEN
(Digital Raw Material)
PAYMENT TOKEN
(Medium of Exchange)
ii. DEFINING A VASP (VIRTUAL ASSET SERVICE PROVIDER)
VASP
(Business Service)
EXCHANGES
(Fiat/Virtual)
TRANSFERRING
SAFEGUARDING
(Custody)
PRECISE CATEGORIES DETERMINE REGULATION

Part 3: The "Who" and "How" - Models and Pillars of Regulation

i. Institutional Models: Who does the regulating?
ii. Sectoral Model: Different regulators oversee different activities (e.g., the securities regulator handles security tokens, the central bank handles payment tokens).
iii. Twin Peaks Model: One regulator focuses on financial stability and prudential soundness, while another focuses on market conduct and consumer protection.
iv. Unified Model: A single, omnipotent regulator oversees the entire virtual asset ecosystem.

The Three Pillars of VASP Regulation: How are they regulated? Regardless of the model, VASPs are typically subject to three core sets of rules:

i. AML/CFT Pillar: Strict "Know Your Customer" (KYC) checks, transaction monitoring, and reporting of suspicious activity.
ii. Market Conduct Pillar: Rules on fair advertising, clear disclosures of risk, and preventing market manipulation.
iii. Prudential Oversight Pillar: Requirements to hold sufficient capital, implement robust cybersecurity, and keep customer assets safely segregated.



Part 4: The Global Challenge - Enforcement Without Borders

Virtual assets operate across borders, but laws remain confined within national jurisdictions. This mismatch creates a fundamental enforcement challenge. For example, if a company based in Asia or Europe offers services to Ghanaian citizens without authorisation, how can Ghana's regulators intervene? The answer lies in cross-border cooperation, information sharing between regulators, and the creation of mutual legal

assistance frameworks. No single country can regulate virtual assets effectively in isolation. International collaboration is therefore the final, essential piece of the regulatory puzzle.

Core Concepts

i. *Regulatory Perimeter:* The boundary that defines which activities fall under a regulator's authority. For virtual assets, this perimeter includes services such as exchanges, custody, and transfers. Activities outside the perimeter may remain unregulated, creating risks for consumers.

ii. *Licensing vs. Registration:*

- ✓ Licensing requires formal approval from a regulator before a business can operate, often with ongoing compliance obligations.
- ✓ Registration is a lighter process where businesses notify regulators of their activities, but may not undergo rigorous vetting. Licensing provides stronger consumer protection.

iii. *Regulated Activities:* Specific functions that require oversight, such as trading, custody, issuance of tokens, or providing payment services. These activities are defined by law to ensure clarity and accountability.

iv. *Consumer Recourse:* Mechanisms that allow consumers to seek redress if they suffer harm, such as complaint procedures, compensation schemes, or dispute resolution channels.

v. *Supervisory Authority:* The designated regulator (e.g., Bank of Ghana, SEC) responsible for monitoring compliance, issuing licenses, and enforcing rules within the regulatory perimeter.

Technical Definitions

- *Virtual Asset Service Provider (VASP):* Under the Ghanaian VASP Act, a VASP is any business entity that provides services such as the exchange, transfer, or custody of virtual assets. VASPs are subject to the new regulatory regime, which ensures accountability and consumer protection.
- *Regulatory Sandbox:* A controlled environment established by regulators where innovative VASPs can test new products or services under temporary regulatory relief. The sandbox fosters responsible innovation while allowing regulators to monitor risks before full-scale deployment.
- *Financial Action Task Force (FATF) Travel Rule:* An international standard requiring VASPs to collect, verify, and share information about the originator (sender) and beneficiary (receiver) of virtual asset transfers above a specified threshold. This rule combats money laundering and terrorist financing by ensuring transparency in cross-border transactions.
- *Market Conduct Rules:* Regulations that govern how VASPs interact with consumers and the market. These rules cover issues such as fair advertising, risk disclosure, conflict-of-interest avoidance, and transparent fee structures.

Why Enforcement Without Borders Matters

The irreversible nature of blockchain transactions and the global reach of virtual assets make it easy for fraud, scams, and illicit activity to cross national boundaries. Without international cooperation, enforcement becomes fragmented and ineffective. Ghana's regulators must therefore work with counterparts abroad, participate in global forums such as the FATF, and adopt harmonised standards. This ensures that Ghanaian consumers are protected even when engaging with platforms based outside the country.

SECTION 2: KEY PRINCIPLES

Foundational Principles

The regulation of virtual assets is designed to mitigate risk, not to endorse or promote any particular technology. Regulators focus on protecting consumers, ensuring financial stability, and preventing misuse of digital assets for criminal purposes such as money laundering (AML) **or** terrorist financing (CFT)**.**

A guiding principle in this space is "same activity, same risk, same regulation." This means that if a virtual asset service performs functions similar to traditional financial services, such as payments, custody, or investment, it should be subject to the same regulatory standards and oversight. This approach ensures fairness, consistency, and protection across the financial system.

Equally important is regulatory clarity**.** When rules are clear and transparent, innovators can design products responsibly, and consumers can engage with confidence. Clear regulations foster safer innovation by reducing uncertainty, discouraging fraudulent schemes, and encouraging legitimate businesses to operate within the law.

Links to Frameworks

These principles are firmly grounded in Ghana's evolving regulatory landscape and its commitments to international standards:

- ✓ Passed VASP Act: Establishes the legal framework for licensing and supervising Virtual Asset Service Providers (VASPs), ensuring they meet compliance obligations before offering services.
- ✓ Bank of Ghana Notices: Provide consumer warnings, guidance on safe practices, and oversight of payment systems to protect users from unlicensed or fraudulent platforms.
- ✓ Securities and Exchange Commission (SEC) Regulations: Focus on investment-related risks, including fraudulent schemes and

unregistered offerings, ensuring investor protection in the virtual asset space.

- ✓ International Standards (FATF): Ghana aligns with the Financial Action Task Force (FATF) recommendations, including the Travel Rule, which requires VASPs to collect and share sender and recipient information for certain transactions. This global alignment strengthens Ghana's ability to combat financial crime and integrate safely into international markets.

SECTION 3: OPERATIONAL MECHANICS

How Systems Function: Licensing, Oversight, and Consumer Pathways

Virtual asset systems do not operate in isolation. They function within a regulatory environment designed to protect users, support market integrity, and enable lawful innovation. Understanding how licensing, oversight, and reporting work helps users and professionals know where responsibility lies.

a. How a VASP Applies for a License

A Virtual Asset Service Provider (VASP) must go through a structured process before operating legally.

Step 1: Application Submission

The VASP submits a formal application to the relevant authority, such as the Bank of Ghana or the Securities and Exchange Commission. This application includes business details, ownership structure, proposed services, and risk controls.

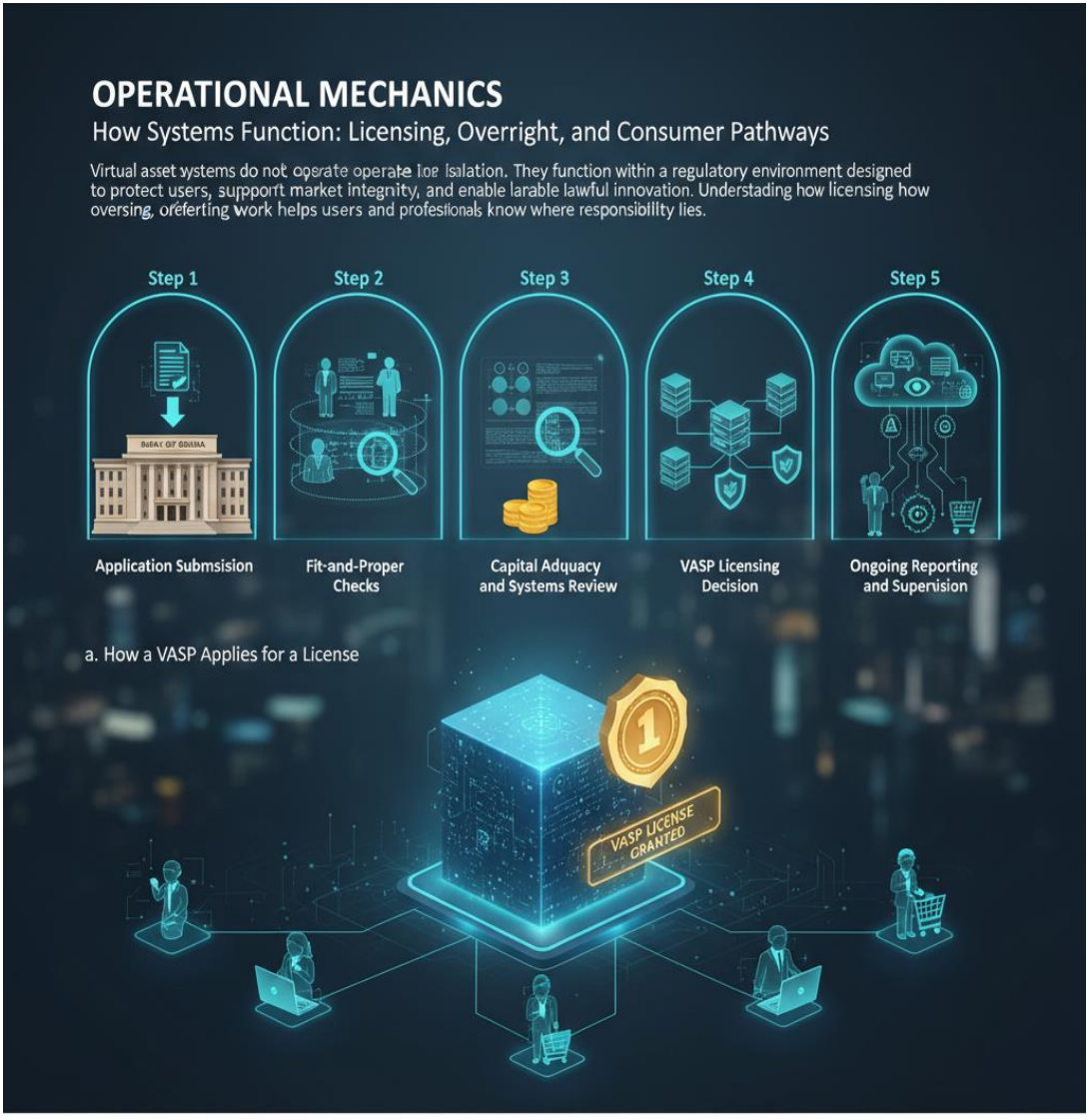
Step 2: Fit-and-Proper Checks

Regulators assess whether the owners and managers are suitable to operate a financial service. This includes background checks, professional competence, integrity, and experience. The aim is to prevent unqualified or dishonest actors from running platforms.

Step 3: Capital Adequacy and Systems Review
The regulator checks whether the VASP has enough financial resources to operate safely and absorb losses. Technical systems, cybersecurity controls, and customer protection mechanisms are also reviewed.

Step 4: Licensing Decision
If requirements are met, the regulator issues a license or registration. This allows the VASP to operate within defined limits and conditions.

Step 5: Ongoing Reporting and Supervision
Licensing is not the end of the process. Licensed VASPs must submit regular reports, comply with rules, and cooperate with inspections. Regulators continue to monitor operations to detect risks early.



Consumer Pathways

b. Interactions Among Key Actors

Several actors interact continuously to maintain safety and accountability.

- Regulator ↔ Licensed VASP
  Regulators set rules, grant licenses, and supervise compliance. VASPs report activities, incidents, and financial information to regulators.

- Licensed VASP ↔ Consumer
  VASPs provide services such as wallets, exchanges, or custody. Consumers use these services and rely on the VASP for support, disclosures, and complaint handling.

- Regulator ↔ Law Enforcement
  When fraud, theft, or other crimes are suspected, regulators work with law enforcement agencies. Information sharing supports investigations and enforcement action.

These interactions ensure that risks are managed and misconduct is addressed.


REGULATOR
Information sharing
Supports investigations
Set rules, grant licenses, supervise
Report activities, incidents, financial info
LAW ENFORCEMENT
SAFETY & ACCOUNTABILITY
LICENSED VASP
These interactions ensure that risks are managed and misconduct is addressed
Use services, lodge complaints
Provide services, support, disclosures
CONSUMER

c. Technical Workflow: The Consumer's Pathway

Consumers also follow a clear pathway when engaging with virtual asset services.

Step 1: Encountering a Service

The consumer sees an app, website, or advertisement offering virtual asset services.

Step 2: Verification

Before engaging, the consumer checks the official public register or guidance issued by the regulator to confirm whether the service is licensed or authorised.

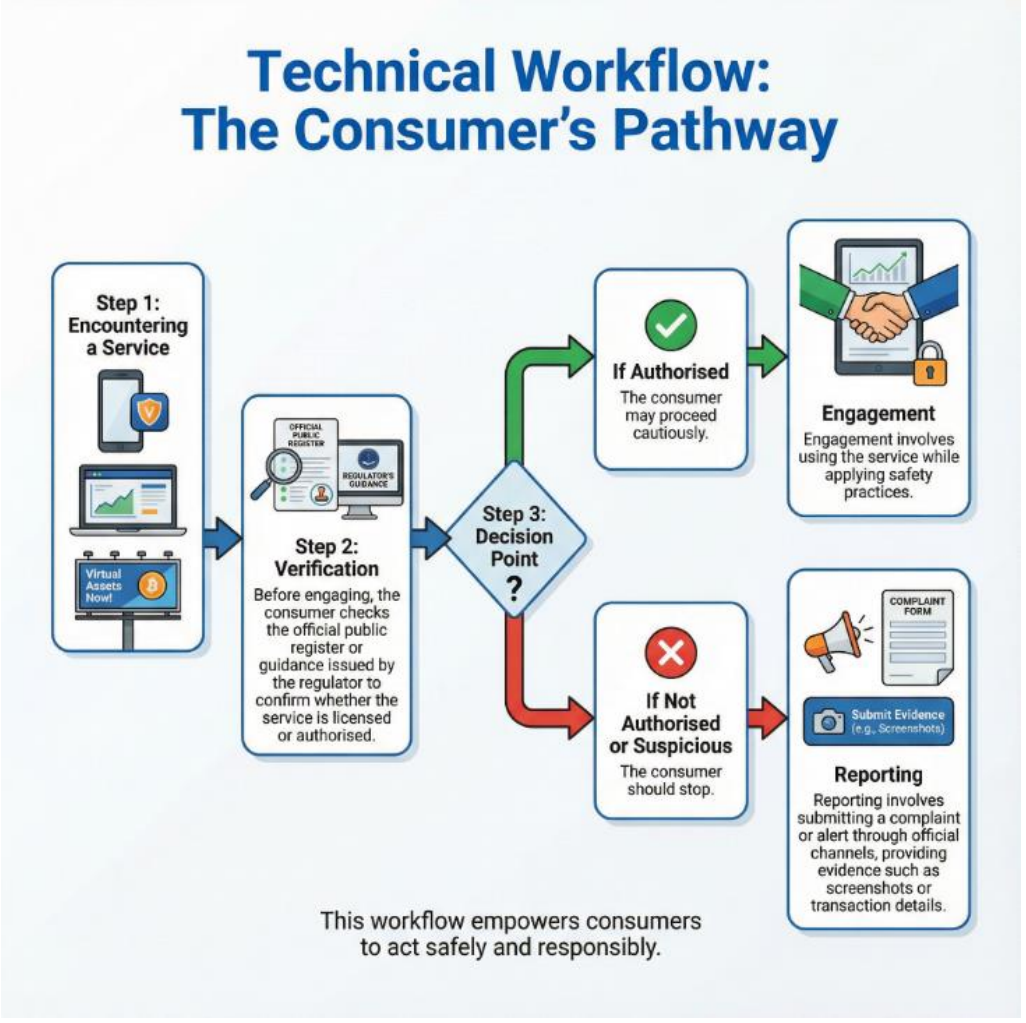
Step 3: Decision Point

- If the service is authorised, the consumer may proceed cautiously.
- If the service is not authorised or appears suspicious, the consumer should stop.

Step 4: Engagement or Reporting

- Engagement involves using the service while applying safety practices.
- Reporting involves submitting a complaint or alert through official channels, providing evidence such as screenshots or transaction details.

This workflow empowers consumers to act safely and responsibly.


Technical Workflow:
The Consumer's Pathway
Step 1: Encountering a Service
Virtual Assets Now!
Step 2: Verification
Before engaging, the consumer checks the official public register or guidance issued by the regulator to confirm whether the service is licensed or authorised.
OFFICIAL PUBLIC REGISTER
REGULATOR'S GUIDANCE
Step 3: Decision Point ?
If Authorised
The consumer may proceed cautiously.
Engagement
Engagement involves using the service while applying safety practices.
If Not Authorised or Suspicious
The consumer should stop.
COMPLAINT FORM
Submit Evidence (e.g., Screenshots)
Reporting
Reporting involves submitting a complaint or alert through official channels, providing evidence such as screenshots or transaction details.
This workflow empowers consumers to act safely and responsibly.

SECTION 4: LEGAL AND POLICY CONTEXT

- **Regulatory Foundations:** The draft VASP Act as the prospective primary legislation. Existing regulatory powers of the Bank of Ghana (for payment systems) and the Securities and Exchange Commission (for securities).
- **Institutional Mandates:** Clear delineation: Bank of Ghana oversees VASPs engaged in payments and storage; SEC to oversee those dealing in investment-like assets. The Cybercrime Unit investigates criminal activity.
- **Applicable Guidelines:** Public warnings, lists of licensed entities, and guidelines on AML/CFT compliance for VASPs.
- **Interpretation Considerations:** Understanding that regulation is evolving. A lack of specific prohibition does not equal endorsement. Personal transactions (peer-to-peer) may fall outside the regulated perimeter but are not risk-free.

SECTION 5: RISK AND ASSURANCE

- **Professional Risk Categories:** Compliance risk (using unlicensed services), legal risk (inadvertently facilitating illicit activity), consumer risk (lack of recourse with unlicensed entities).
- **Control Mechanisms:** The primary control is verifying authorisation before engagement. Secondary controls include using regulated channels for fiat on/off ramps and reviewing a VASP's published policies.
- **Oversight Responsibilities:** The regulator's role is supervisory and enforcement. The licensed VASP's role is operational compliance. The consumer's role is to perform due diligence.

SECTION 6: PRACTICAL APPLICATIONS

How to Verify a Virtual Asset Service Provider (VASP) in Ghana

Verifying whether a Virtual Asset Service Provider (VASP) is licensed and legitimate is a critical step in protecting yourself from fraud, scams, or unregulated platforms. Ghana's regulatory framework requires VASPs to operate under authorisation from designated financial regulators such as the Bank of Ghana (BoG) and the Securities and Exchange Commission (SEC). The following step-by-step procedure ensures that individuals and institutions can confirm the legitimacy of any VASP before engaging with its services.

Step 1: Identify the Service Type

Begin by clarifying the type of service the VASP is offering.

- ✓ Exchange Services: Platforms that allow users to buy, sell, or trade cryptocurrencies.
- ✓ Custody Services: Entities that hold digital assets on behalf of clients.
- ✓ Transfer Services: Businesses that facilitate sending or receiving virtual assets across wallets or borders.

- ✓ Investment Services: Platforms offering crypto-related investment products or schemes.

Identifying the service type helps determine which regulator has jurisdiction and what rules apply.

Step 2: Go to the Correct Regulator's Website

Different regulators oversee different aspects of virtual asset activity in Ghana:

- ✓ Bank of Ghana (BoG): Supervises payment systems, custody services, and licensed exchanges.
- ✓ Securities and Exchange Commission (SEC): Oversees investment-related activities, including platforms offering securities-like products or schemes.
- ✓ Financial Intelligence Centre (FIC): Monitors compliance with Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) obligations.

Visit the official website of the relevant regulator to access their notices, registers, and consumer advisories.

Step 3: Search the Official Register/List

Regulators maintain official registers or lists of licensed entities.

- ✓ Look for the VASP Register or Licensed Institutions List published by the regulator.
- ✓ Confirm that the VASP's name appears exactly as advertised.
- ✓ Check the license status (active, suspended, or revoked).

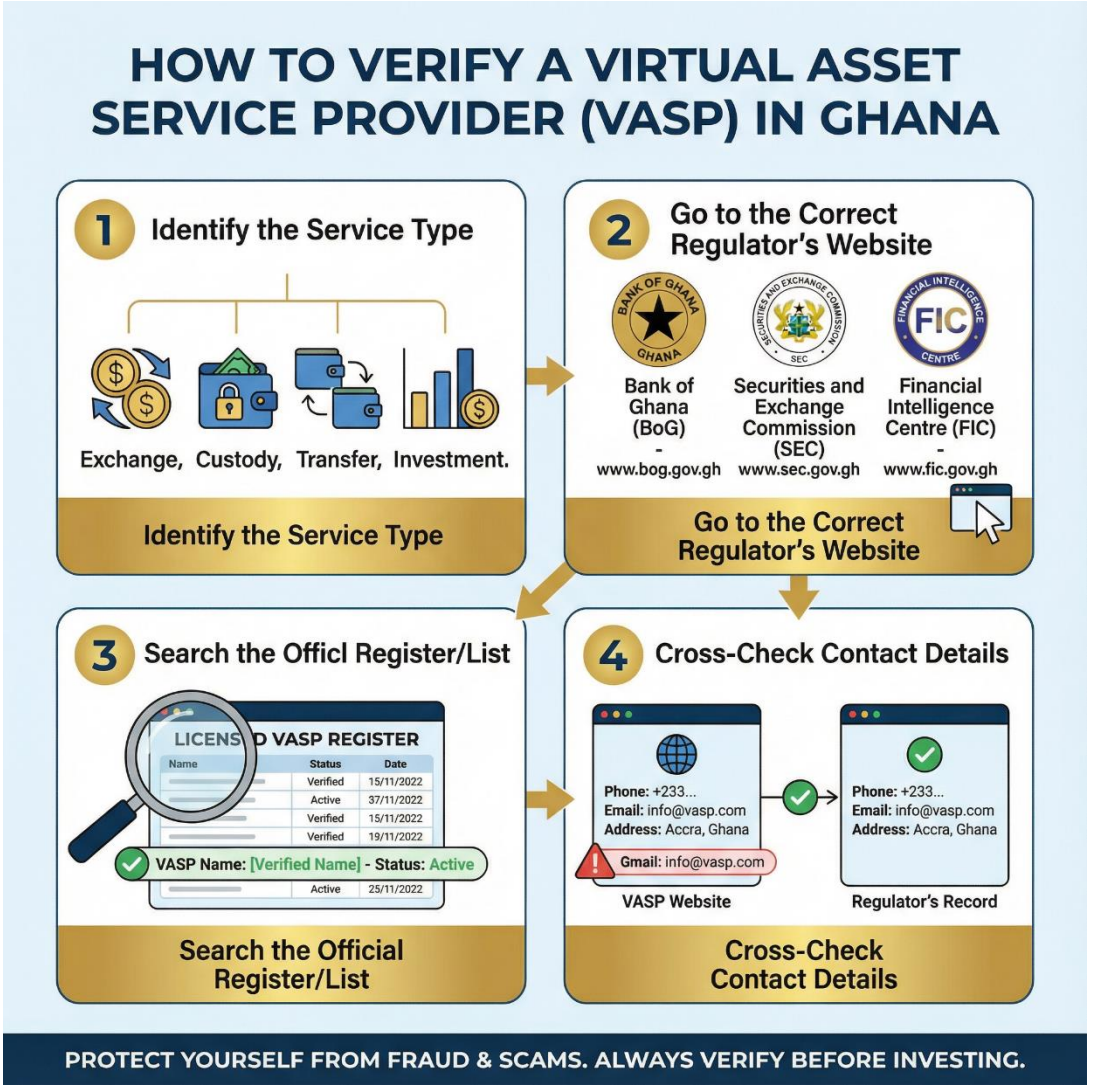
If the VASP is not listed, it is not authorised to operate in Ghana.

Step 4: Cross-Check Contact Details

Fraudulent platforms often impersonate legitimate businesses. To avoid this:

- ✓ Compare the VASP's contact details (phone numbers, email addresses, office locations) with those published on the regulator's website.

- ✓ Verify that the website domain matches the official records.
- ✓ Be cautious of platforms using free email services (e.g., Gmail, Yahoo) instead of official business domains.
- ✓ If in doubt, call the regulator directly to confirm authenticity.



Why This Procedure Matters

Virtual assets are irreversible once transferred. Engaging with an unlicensed or fraudulent VASP can result in permanent financial loss. By following these steps, identifying the service type, consulting the correct regulator, checking the official register, and cross-verifying contact

details, users can protect themselves and ensure they only interact with legitimate, regulated providers.

SECTION 7: DISCUSSION POINTS AND REFLECTION

- *Points for Deeper Thinking:* Does strict regulation stifle innovation or enable it by building public trust?
- *Policy Questions:* How should Ghana balance attracting fintech business with enforcing strong consumer protection rules?
- *Ethical Considerations:* As an administrator or procurement officer, what is your duty if a superior suggests using a cheaper, unlicensed platform for a corporate crypto transaction?
- *Sector-specific Reflections: Finance practitioners/NGO Officers*: What are the enhanced due diligence requirements for handling transactions potentially linked to VASPs?

Assessment Strategy

Quiz on regulated activities and the entity vs. asset distinction.

i. Scenario: A company based online claims to be "registered in Ghana" and offers crypto investment plans. What is the most authoritative source to verify if they are a licensed VASP?
ii. Scope Analysis: You buy Bitcoin from a friend with cash. Your cousin operates a website that buys bitcoin from people and sells it for mobile money. Whose activity is more likely to require a VASP license, and why?
iii. Compare & Contrast: What is the key difference between a regulator warning the public about an unlicensed entity and a regulator prosecuting that entity?
iv. True or False (with justification): "If the Bank of Ghana licenses a VASP, it means all investments offered on its platform are government-guaranteed."

v. Ordering: Sequence the logical steps of regulatory development: a) Public consultation, b) Law enforcement action against bad actors, c) Drafting of a bill (e.g., VASP Act), d) Passage of an Act by Parliament.

vi. Identify the Protection: Which consumer protection principle is upheld when a licensed VASP is required to keep customer funds separate from its own operating funds (segregation of funds)?

vii. Matching: Match the agency (Bank of Ghana, Securities and Exchange Commission, Police Cybercrime Unit) to its potential role regarding Virtual Assets (e.g., "Investigates cases of fraud and theft").

viii. Recourse Pathway: If your complaint to a licensed VASP about an unauthorised transaction is ignored, what is the next official channel you should approach?

ix. Short Answer: Why is Anti-Money Laundering (AML) verification required by licensed platforms, even if it feels inconvenient?

x. Prediction: How might the official list of licensed VASPs change over the next year, and what should that tell you as a consumer?

- Scenario-based task: For a given user scenario, determine if the activity is likely regulated and outline verification steps.
- Short written reflection: Describe how you will stay informed about regulatory updates in Ghana.
- Role-play assessment: Effectively report a simulated issue through the correct channels.

MODULE SUMMARY PAGE

- **Key Insights**: Ghana is building a formal regulatory framework to govern virtual asset services. Safety is significantly enhanced by using licensed entities. Regulation focuses on service providers rather than on each asset.
- **Applications to Professional Roles:** Enables compliant personal engagement and provides the knowledge to make institutionally sound decisions, advise the public correctly, and know where to turn when problems arise.
- **Key Risks:** Engaging with unlicensed entities (no recourse, higher fraud risk), misinterpreting the scope of regulation.
- **Next Steps**: Integrate knowledge from all four modules into daily professional practice. Continue lifelong learning by following official regulatory channels for updates.

-End of MANUAL-

Discussion Points and Reflections from the group

Reference

- ✓ Anti-Money Laundering Act, 2020 (Act 1044), Ghana

- ✓ Bank of Ghana (2022), *Notice to the general public on a digital and virtual currency operation in Ghana called "Freedom Coin"* (Notice No. BG/GOV/SEC/2022/03).
- ✓ Bank of Ghana (2025), *Press release: Passage of the Virtual Asset Service Providers Bill.*

- ✓ Centre for Finance, Technology and Entrepreneurship. (2023), *What is public blockchain: Definition, use cases and examples.*

- ✓ Centre for Finance, Technology and Entrepreneurship. (2023), *Types of digital assets explained with examples and use cases.*

- ✓ DashDevs. (2024), *DLT technology: Centralised and distributed ledgers comparison*

- ✓ Data Protection Act, 2012 (Act 843) (Ghana)

- ✓ European Parliament & Council of the European Union. (2023). Regulation (EU) 2023/1114 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. Official Journal of the European Union, L 150, 40–205.

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

- ✓ Financial Crimes Enforcement Network. (2019). *Application of FinCEN's regulations to specific business models involving convertible virtual currencies* (FIN-2019-G001).

- ✓ Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* https://bitcoin.org/bitcoin.pdf

- ✓ New York State Department of Financial Services. (n.d.). *Virtual currency business activity license (BitLicense).*

- ✓ Payment Systems and Services Act, 2019 (Act 987) (Ghana).

- ✓ Securities Industry Act, 2016 (Act 929) (Ghana).

- ✓ SEC v. W. J. Howey Co., 328 U.S. 293 (1946).

- ✓ Weston, G. (2022), *Custodial vs non-custodial wallets: Key differences.*

- ✓ Yoshikawa, M. (2022). Chess Superhero. The Missouri Review. https://doi.org/10.1353/mis.2022.0039

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. Website: www.sec.gov.gh Phone: +233 302 768 970 / 08001000	Report if you encounter an investment-like Virtual Asset product promising 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 the native currency of 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.
Tokenization	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, 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 capable of swinging dramatically in short periods.
Market Risk	The risk of investors experiencing losses due to factors affecting overall financial market performance, primarily price volatility.
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 its 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 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., NYDFS BitLicense in New York) for VASPs to legally operate within their jurisdiction often involve 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: 978-9988-41-654-6