

NATIONAL VIRTUAL ASSETS EDUCATION MANUAL

National Virtual Assets Literacy Initiative (NaVALI)

Foundational Knowledge in Virtual Assets



NATIONAL VIRTUAL ASSETS

LITERACY INITIATIVE (NaVALI)

Empowering Ghana for the Digital Future

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



Manual Title
National Virtual Assets Education Manual

Programme Name
National Virtual Assets Literacy Initiative

Foundational Knowledge in Virtual Assets

Disclaimer

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

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



Copyright © Bank of Ghana, 2026

All rights reserved. No part of this material may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording or by any information storage and retrieval system, without permission in writing from the publisher.

Printed in Ghana

Main Authors

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

¹Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development, Faculty of Business Education, Department of Economics

²Lead, Virtual Assets Regulation, Bank of Ghana

Contributors

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

Cover Design by: Evans Opong

ISBN: 978-9988-41-656-0

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.

PUBLIC



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 Dako 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 Content

Contents	Page
Dedication	IV
Acknowledgement.....	V
Preface	VIII
Foreword	X
Introductory Remarks	XII
How to Use This Manual.....	XIII
Programme Overview.....	1
Module 1: Virtual Assets: Concepts and Context	4
SECTION 1: Definitions and Concepts of Virtual Assets	4
SECTION 2: How Virtual Assets are Stored and Used	15
SECTION 3: Practical Uses of Virtual Assets and Safe Steps.....	19
SECTION 4: Risks and Safe Practices.....	20
Section 5: Ghana’s Guidelines for Safe Use	22
Assessment Strategy: Group Discussion	25
Module 2: Key Tools and Components	26
SECTION 1: Accessing Virtual Assets	26
Section 2: Sending and Receiving Funds	30
SECTIONS 3: Platforms and Intermediaries	32
SECTION 4: Costs and Fees	33
SECTION 5: Basic Operational Safeguards.....	36
SECTION 6: Simple Risk Awareness	38



Module 3: Markets and Consumer Risks.....	43
SECTION 1: Risks Everyone Should Know	43
SECTION 2: Common Scams and Misconduct.....	46
SECTION 3: How to Protect Yourself	54
SECTION 4: Cybersecurity Basics.....	54
SECTION 5: What to Do if Something Goes Wrong.....	58
Module 4: Law and Regulatory Perimeter (Policy-Neutral).....	63
SECTION 1: Why Regulation Exists	63
SECTION 2: Activities Covered by Regulation	63
SECTION 3: Who Is Licensed or Authorised.....	64
SECTION 4: Consumer Protections and Reporting.....	64
SECTION 5: Staying Safe and Informed	64
Assessment Strategy.....	65
References	68
Appendices	69
1. Key Laws and Regulations.....	69
2. National Contacts and Reporting Channels.....	71
General Advice for Reporting:	72



Preface

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

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

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

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



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

PUBLIC



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

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

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



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

Johnson Pandit Asiamah (PhD)
Governor, Bank of Ghana

PUBLIC



Introductory Remarks

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

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

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

James Klutse Amedzi (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 with all levels of education.

i. *Follow the order of sections*

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

ii. *Focus on examples and illustrations*

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

iii. *Encourage discussion and clarification*

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

iv. *Apply learning through practice*

Practical demonstrations and role-play activities should be carried out using small amounts. 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.

PUBLIC



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 is carried out. 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 manual is designed for people whose daily work depends mainly on practical skills. Members of this group read and write at a basic level and prefer learning that is clear, short, and directly linked to everyday life. They understand ideas better when lessons use familiar situations, spoken explanations, pictures, and demonstrations. Long text and technical language reduce understanding, so content is presented in simple steps with repeated examples. Training for this group focuses on what they need to know to stay safe and make informed choices. Emphasis is placed on recognising risks, avoiding scams, and using digital and virtual asset services with care in daily activities.

3. Learning Philosophy

The learning approach for this group centres on practical understanding and daily use. Participants learn best through clear examples drawn from familiar situations. Lessons focus on actions people meet in everyday life, such as sending money, receiving payments, or responding to unexpected messages. Learning builds from what participants already know and connects new ideas to everyday experiences.

Teaching follows a step-by-step method. Each topic begins with a simple explanation, followed by a demonstration and guided practice. Trainers explain slowly, repeat key points, and confirm understanding before moving forward. Short sessions, explicit language, and frequent pauses support steady learning without overload.

This manual places strong emphasis on risk awareness. Learning activities highlight common mistakes, unsafe behaviour, and warning



signs of fraud. Stories and role-play show how people lose money and how such losses happen. Participants learn safe habits through observation and practice rather than theory.

Participation plays a vital role in learning. Group discussions, questions, and shared experiences help reinforce lessons. Trainers encourage learners to speak, observe, and practise together. Confidence grows through repetition and support rather than speed.

Conclusively, the learning philosophy values clarity, relevance, and protection. The aim is to help participants make careful choices, avoid harm, and stay alert when digital money or virtual assets appear in daily life.

4. Programme Learning Outcomes

The aim is 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
- vi. Boost regulatory readiness and institutional capacity, and
- v. source feedback for incorporation into regulatory frameworks



MODULE STRUCTURE

Module 1

Module Title - Virtual Assets: Concepts and Context

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

Module Learning Outcomes

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

SECTION 1: Definitions and Concepts of Virtual Assets

What are Virtual Assets?

Virtual assets are forms of money or value that exist on phones, computers, or other electronic devices. People do not hold them in their hands like cash. They see them on a screen and use them through simple digital tools. When someone sends or receives a virtual asset, the value moves through a network instead of passing from hand to hand.





Types of Virtual Assets and examples

i. Payment Virtual Assets (Cryptocurrencies)

Used mainly to send and receive money.

Examples: Bitcoin (BTC), Litecoin (LTC), etc.





**PAYMENT VIRTUAL ASSETS
(CRYPTOCURRENCIES)**

Used mainly to send and receive money.





ii. Stable Virtual Assets

Designed to keep a steady value close to normal money.

Examples:

USDT – Tether,

USDC – USD Coin



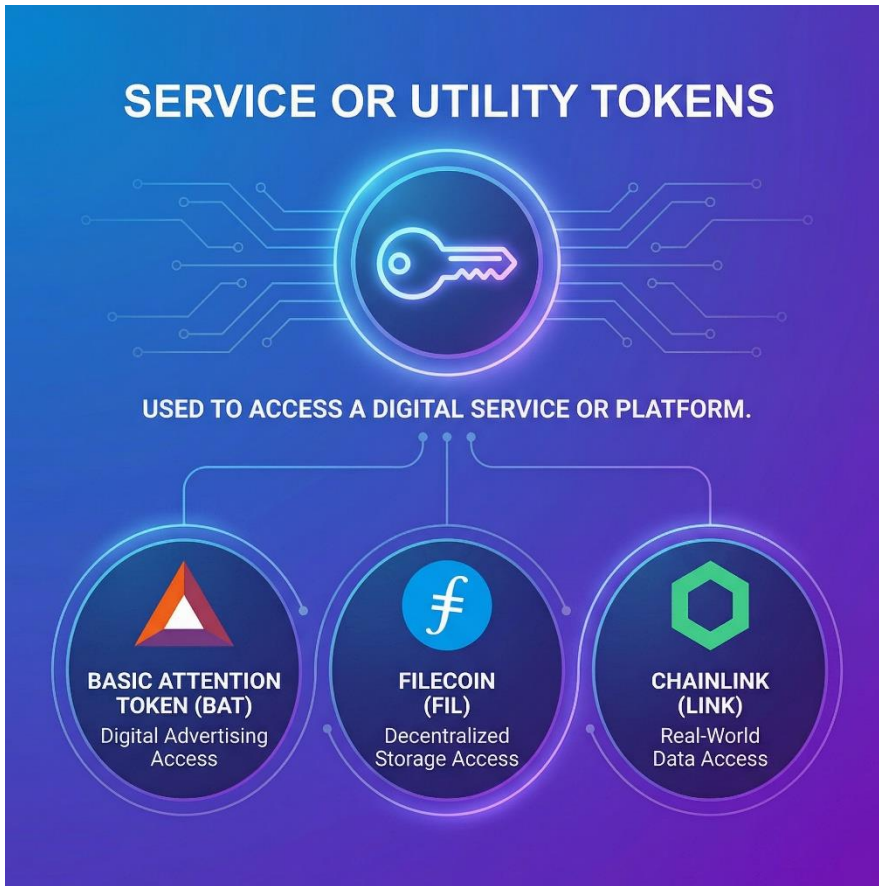


iii. Service or Utility Tokens

Used to access a digital service or platform.

Examples: Basic Attention Token, Filecoin, Chainlink, etc.





iv. Asset-Backed Tokens

Linked to real-world items or financial value.

Examples: Gold-backed tokens, real estate tokens, commodity-backed tokens, etc.





v. Unique Virtual Assets

Each one is different and cannot be replaced by another. These NFTs are not used as money. They are used to prove ownership, access, or records.

Examples: Digital art Non-Fungible Tokens, Event ticket Non-Fungible Tokens, Certificate or record Non-Fungible Tokens.



A scene illustrating NFT art and event tickets. A large smartphone displays "NFT ART" and various digital assets. A man and a woman are interacting with the phone. To the right, there are icons for "AFRICAN MUSIC FESTIVAL" tickets and a "CERTIFICATE".

- **Unique Virtual Assets example**
 - Digital art Non-Fungible Tokens.
 - Event ticket Non-Fungible Tokens.
 - Certificate or record Non-Fungible Tokens.
- **EVENT TICKET NFTS**
- **CERTIFICATE/RECORD NFTS**
 - Secure, verified digital diplomas
 - Land titles with blockchain
 - Certificate or record Non-Fungible Tokens.)



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	Often treated under FATF's



		specific AML/CFT implications.	“virtual asset” framework, with specific AML/CFT implications.
--	--	--------------------------------	--

How are Virtual Assets used in everyday life?

- ✓ People send money to family members in another town or country to support food, school fees, or medical needs.
- ✓ Small payments are made for goods and services such as transport, phone credit, or items in local shops.
- ✓ Some people receive wages, allowances, or community support through digital systems instead of cash.
- ✓ Traders and small business owners accept digital payments to avoid carrying large amounts of cash.
- ✓ Savings groups or cooperatives use digital tools to record contributions and payments.
- ✓ Some digital payments are used to pay for utilities, subscriptions, or online services.
- ✓ Digital records or certificates are sometimes issued to show proof of payment or participation.





Many of these actions feel similar to mobile money because a phone is used to send and receive value. The main difference is that virtual assets move through digital networks and shared records rather than telecom systems.



SECTION 2: How Virtual Assets are Stored and Used

Virtual assets are kept in a **wallet**.

What is a Wallet? A wallet is a digital place on a phone or computer where virtual assets are stored. It is needed because virtual assets do not exist in cash form. The wallet allows people to see their balance, send value to others, and receive value safely. Without a wallet, virtual assets cannot be used.

What is a Wallet?

A wallet is a digital place on a phone or computer where virtual assets are stored. It is needed because virtual assets do not exist as cash. The wallet allows people to see their balance, send value to others, and receive value safely. Without a wallet, virtual assets cannot be used.

Without a wallet, virtual assets cannot be used.

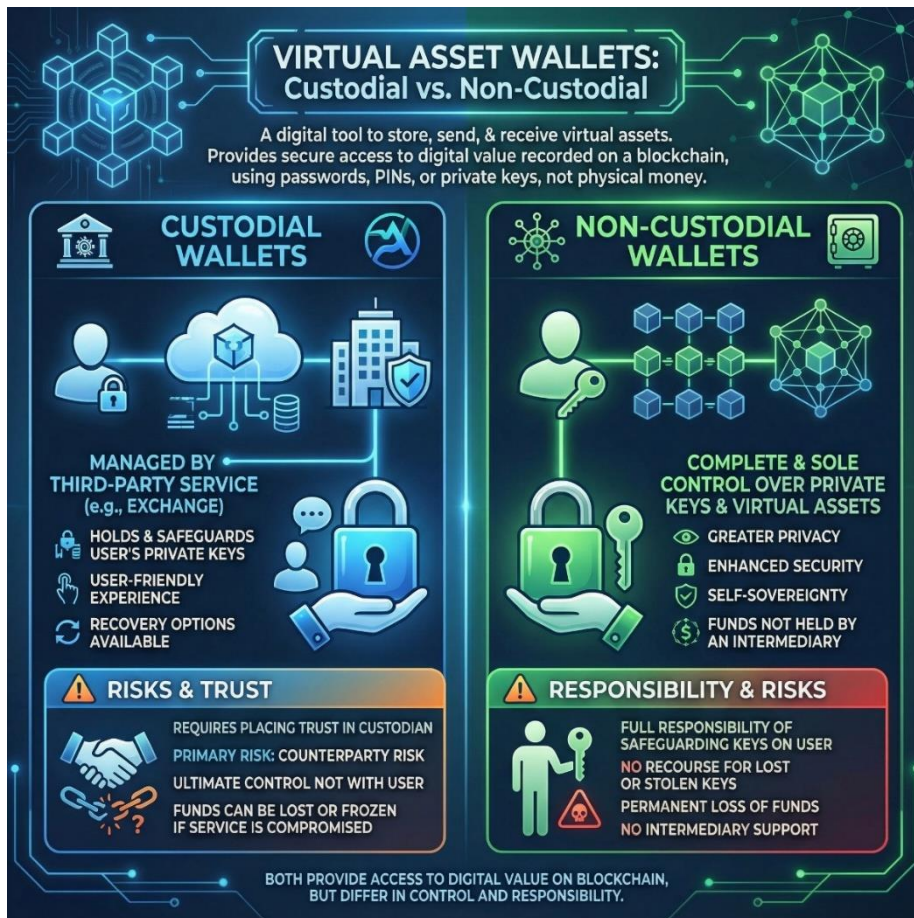
The infographic features a hand holding a smartphone displaying a Bitcoin balance of 0.50 BTC with a USD value of 31,227.90. Next to it is a laptop displaying a balance of 150.00 USDT. Several physical Bitcoin coins are shown in front of the laptop. The background is a dark blue space with glowing particles and a golden circular path.



There are two main types of wallets: *a Custodial Wallet and Non-Custodial Wallet.*

A custodial wallet is one where a service or app helps keep the wallet safe on behalf of the user. This works similarly to mobile money apps, where the service provider manages the system and supports users.

A non-custodial wallet is one in which the user retains complete control over the wallet and its security details. This means the user has more responsibility for protecting passwords or recovery details.





Using a wallet to send or receive virtual assets follows simple steps:

To send, the user opens the wallet, selects the recipient or address, enters the amount, and confirms the transaction.

To receive, the user shares their wallet address or number, and the virtual asset appears in their wallet after it is sent. For safety, users are advised to start with small amounts, check details carefully before confirming, and ask for help if anything looks unclear.



VIRTUAL ASSET WALLET GUIDE

SENDING, RECEIVING, & SAFETY FOR VIRTUAL ASSETS



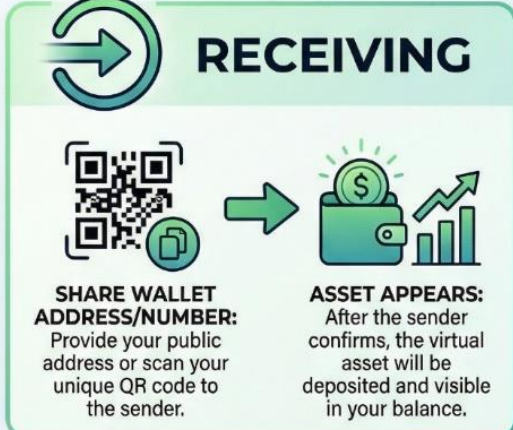
SENDING

1. OPEN WALLET: Launch your digital wallet application.

2. SELECT RECIPIENT/ADDRESS: Choose the intended recipient's address or select from contacts.

3. ENTER AMOUNT: Input the quantity of virtual asset to send.

4. CONFIRM: Review details and authorize the transaction with security steps.



RECEIVING

SHARE WALLET ADDRESS/NUMBER: Provide your public address or scan your unique QR code to the sender.

ASSET APPEARS: After the sender confirms, the virtual asset will be deposited and visible in your balance.



SAFETY TIPS

- 
START WITH SMALL AMOUNTS: Begin with minimal transactions to understand the process and minimize risk.
- 
VERIFY DETAILS CAREFULLY: Double-check recipient addresses, network fees, and all transaction details before confirming.
- 
ASK FOR HELP IF UNCLEAR: Consult official resources, customer support, or trusted communities if any part of the process is confusing.

Educational Guide for Digital Asset Beginners. Always Prioritize Security.



SECTION 3: Practical Uses of Virtual Assets and Safe Steps

- ✓ People send money to family members in another town or country to support food, school fees, or medical needs.
- ✓ Small payments are made for goods and services such as transport, phone credit, or items in local shops.
- ✓ Some people receive wages, allowances, or community support through digital systems instead of cash.
- ✓ Traders and small business owners accept digital payments to avoid carrying large amounts of cash.
- ✓ Savings groups or cooperatives use digital tools to record contributions and payments.
- ✓ Some digital payments are used to pay for utilities, subscriptions, or online services.
- ✓ Digital records or certificates are sometimes issued to show proof of payment or participation.

Safe ways to participate in small digital transactions.

- ✓ Start with a small amount when sending digital money for the first time.
- ✓ Check the phone number or wallet address carefully before pressing send.
- ✓ Keep your phone and PIN safe at all times.
- ✓ Do not rush when sending money. Take your time and confirm the details.
- ✓ If anything looks strange or confusing, stop, and ask a trusted person for help.





SECTION 4: Risks and Safe Practices

Common Risks and Scams

- ✓ Fake platforms: Apps or websites that look real but are created to steal money.
- ✓ Phishing messages: Messages on SMS, WhatsApp, or social media that ask for your PIN, password, or wallet details.
- ✓ Fraudulent links: Links that take you to fake pages designed to collect your information.



- ✓ False helpers: People pretending to be agents, helpers, or officials to gain your trust.
- ✓ Quick money promises: Messages that promise free money, bonuses, or fast profits.



Safe Practices to Follow

- ✓ Use only platforms or wallets you know and trust.
- ✓ Do not click links from unknown messages or people.
- ✓ Never share your PIN, password, or recovery details with anyone.
- ✓ Take your time before sending money and confirm all details on the screen.
- ✓ If something feels strange or confusing, stop, and ask a trusted person for help.

These steps help protect your money and personal information and reduce the chance of loss.



Section 5: Ghana's Guidelines for Safe Use

Advice from the Bank of Ghana/Securities and Exchange Commission

- ✓ The Bank of Ghana/Securities and Exchange Commission advise people to use only approved and trusted digital money services.
- ✓ Users should protect their phones, PINs, and passwords at all times.
- ✓ People should avoid messages or offers that promise quick or free money.
- ✓ Digital money should be used carefully, just like cash.





How to Check if a Platform or App Is Legitimate

- ✓ Use apps or services recommended by trusted agents or official sources.
- ✓ Check that the app comes from a known provider and not from a stranger.
- ✓ Avoid downloading apps from links sent through unknown messages.
- ✓ If unsure, ask a trusted person or agent before using the platform.

Who to Contact if Something Goes Wrong

Bank of Ghana (BoG), FinTech & Innovation Office; Financial Stability Department; Consumer Protection Office. For inquiries and reporting related to licensed Payment System Providers, the eCedi, and general warnings on virtual assets.

Website: www.bog.gov.gh, Phone: +233 593974486



Securities and Exchange Commission (SEC), 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

Knowing where to get help early can reduce loss and protect your money.

PUBLIC



Assessment Strategy: Group Discussion

Group Discussion Questions

1. From what we have learnt, where do people in our community already use virtual assets or digital money in daily life, and what benefits do they see from using them instead of cash?
2. Looking at the different types of virtual assets, which ones seem most common or useful in everyday activities, and why is it important to know the difference between them?
3. Based on the risks and scams discussed, what signs would make you stop and ask for help before sending money, and who would you contact in such a situation?

PUBLIC



Module 2

Module Title: Key Tools and Components

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

Module Learning Outcomes

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

SECTION 1: Accessing Virtual Assets

Virtual assets are accessed and stored using a wallet. A wallet is a digital storage space on a phone or computer where virtual assets are safely stored. It allows people to see how much they have, send value to others, and receive value when someone sends to them. Because virtual assets do not exist in cash form, a wallet is needed to use them.



There are simple wallet types beginners can use.

- ✓ *Mobile wallets* are apps on a phone that allow users to store and use digital money easily. These are similar to mobile money apps that many people already know.
- ✓ *Agent-assisted wallets* are wallets where a trained agent helps the user open, manage, or use the wallet. This option is helpful for people who are new to digital tools or prefer face-to-face support.

Simple demonstration: opening and using a wallet safely

a. Prepare the Phone

- ✓ Ensure the phone is charged and the screen is clean.
- ✓ Confirm that the phone is locked with a secure PIN, pattern, or biometric option.

b. Unlock the Phone Safely

- ✓ Hold the phone so only you can see the screen.
- ✓ Enter your PIN or use your fingerprint/face unlock without exposing it to others.

c. Locate and Open the Wallet App

- ✓ Find the wallet icon on the home screen or app list.
- ✓ Tap the icon once to open it.
- ✓ The trainer demonstrates this slowly so participants can follow.

d. Enter the Wallet PIN Securely

- ✓ Cover the screen with your hand while typing your PIN.
- ✓ Never say your PIN out loud.
- ✓ Ensure no one is standing too close or watching.

e. Check the Wallet Balance



- ✓ Once inside the app, navigate to the balance section.
- ✓ The trainer pauses to show where the balance appears and how to read it.

f. Close the Wallet Properly

- ✓ Tap the “Back” or “Close” button until you exit the app.
- ✓ Lock the phone immediately after closing the wallet.

g. Keep the Phone Secure

- ✓ Store the phone in a safe pocket or bag.
- ✓ Avoid leaving it on tables, in public places, or with strangers.

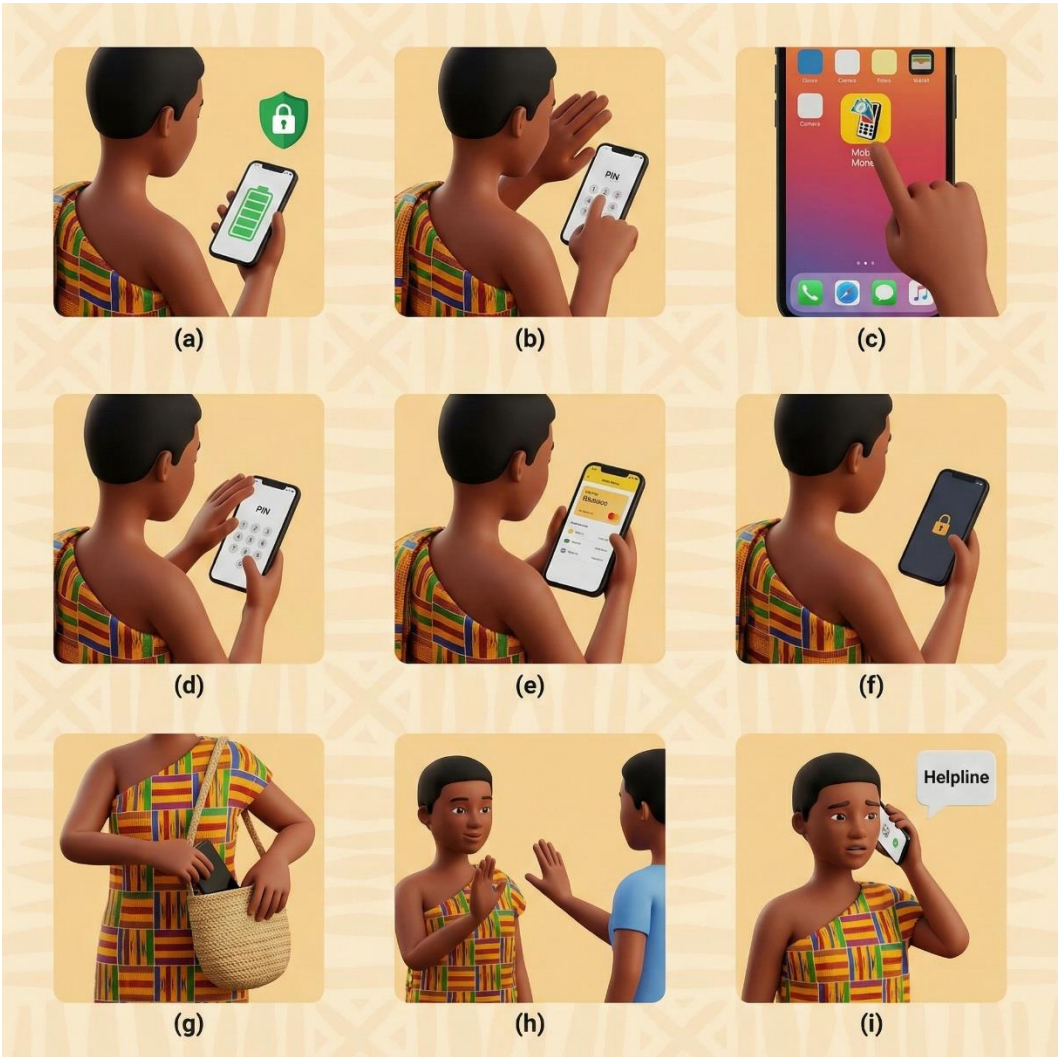
h. Protect Your PIN and Wallet Access

- ✓ Never share your PIN with anyone, not friends, family, or agents.
- ✓ Do not allow others to handle your phone when the wallet is open.
- ✓ If someone insists, politely decline and keep control of your device.

i. Report Any Suspicious Activity

- ✓ If you notice strange transactions or think someone saw your PIN, report it immediately to the appropriate support channel.





Section 2: Sending and Receiving Funds

Sending and receiving virtual assets is done through a wallet on a phone or device. The steps are simple, but careful attention is essential to avoid mistakes or loss.

How to Send Money Safely

- Open your wallet and choose the option to send money.
- Enter the phone number or wallet address of the person you want to send to.
- Check the number or address slowly and carefully before you continue.
- Enter the amount you want to send and confirm that it is correct.
- Look at the name or details shown on the screen before pressing send.

Taking time at this stage helps prevent sending money to the wrong person.

How to Receive Money Securely

- To receive money, share your correct phone number or wallet address with the sender.
- Wait for the message or notification that shows the money has arrived.
- Check that the amount received is what you expected.
- Do not allow strangers to handle your phone when receiving money.

Why Small Test Transactions Matter

- When sending money to someone new, start with a minimal amount.
- This helps you confirm that the number or wallet address is correct.
- Once the small amount goes through safely, you can send a larger amount if needed.



Using small test transactions and carefully checking details helps protect your money and reduce mistakes.

Section 2: Sending and Receiving Funds (Virtual Assets)





SECTIONS 3: Platforms and Intermediaries

Virtual assets are used through platforms and intermediaries. These are the apps, services, or agents that help people send, receive, or store digital money. Using the right platform is essential because it affects the safety of your money.

Licensed Wallets and Approved Agents

- ✓ Licensed wallets are apps or services that national authorities have approved.
- ✓ Approved mobile money agents are trained people who help users send, receive, or manage digital money safely.
- ✓ These services follow rules meant to protect users and reduce fraud.
- ✓ Using licensed wallets or known agents gives users a better chance of getting help if something goes wrong.



Avoiding Unlicensed Platforms or Apps

- ✓ Some apps or platforms operate without approval and are unsafe.
- ✓ These platforms may disappear suddenly or refuse to help when problems occur.
- ✓ Avoid apps sent through random links, social media messages, or strangers.
- ✓ Never trust platforms that promise quick profits or special bonuses for joining.

Recognising Trustworthy Providers

- ✓ Trustworthy providers are usually listed or mentioned by official bodies such as the Bank of Ghana/ Securities and Exchange Commission.
- ✓ They have clear names, contact details, and customer support.
- ✓ Their apps are found on official app stores, not through private messages.
- ✓ If unsure, ask a trusted agent, community leader, or service provider before using a platform.

Choosing safe platforms and intermediaries helps protect your money and reduces the risk of scams or loss.

SECTION 4: Costs and Fees

When using virtual assets, small fees are often charged during transactions. These fees are a regular part of digital payments and should be expected.

Why Fees Are Charged

- ✓ Fees help keep the digital system working correctly.
- ✓ Fees also help service providers maintain security and customer support.



- ✓ Paying a small fee is similar to paying transport or service charges when using other services.

How to Check Fees Before Sending Money

- ✓ Before you press send, look carefully at the screen on your phone or device.
- ✓ Most wallets show the fee clearly before you confirm the transaction.
- ✓ Check the total amount, including the fee, so you know exactly how much will be taken from your wallet.
- ✓ If the fee looks too high or confusing, stop and ask a trusted person or agent for help.

Understanding costs and checking fees before sending money helps prevent surprise charges and protects your balance.

PUBLIC



Costs and Fees

When using virtual assets, small fees are often charged during transactions. These fees are a normal part of digital payments and should be expected.



Why Fees Are Charged



Fees help keep the digital system working properly.



Fees also help service providers maintain security and customer support.



Paying a small fee is similar to paying transport or service charges when using other services.



How to Check Fees Before Sending Money



Before you press send, look carefully at the screen on your phone or device.



Most wallets show the fee clearly before you confirm the transaction.



Check the total amount, including the fee, so you know exactly how much will be taken from your wallet.



If the fee looks too high or confusing, stop and ask a trusted person or agent for help.

Understanding costs and checking fees before sending money helps prevent surprise charges and protects your balance.



SECTION 5: Basic Operational Safeguards

Basic safeguards help keep virtual assets safe from loss, theft, or misuse. These actions are simple but very important in daily use.

Using Strong Passwords and PINs

- ✓ A password or PIN is a secret number or code that protects your wallet.
- ✓ Choose a PIN that is not easy to guess. Avoid using birthdays or simple numbers.
- ✓ Never share your PIN or password with anyone, even people who say they want to help.
- ✓ Keep your PIN private when typing it on your phone.

Using Extra Protection Where Available

- ✓ Some wallets ask for an extra code after you enter your PIN.
- ✓ This extra step adds more protection to your wallet.
- ✓ If your wallet offers this option, allow it and follow the instructions.
- ✓ This helps stop strangers from entering your wallet even if they get your phone.

Protecting Your Phone or Device

- ✓ Keep your phone with you at all times. Do not leave it unattended.
- ✓ Lock your phone so others cannot open it easily.
- ✓ Do not install apps from unknown sources or strange links.
- ✓ If your phone asks for updates, allow them. Updates help keep the device safe.

Following these simple safeguards helps protect your virtual assets and reduces the risk of loss or fraud.



BASIC OPERATIONAL SAFEGUARDS FOR VIRTUAL ASSETS

USING STRONG PASSWORDS & PINS



- ✓ Secret code protects wallet
- ✓ Not easy to guess (avoid birthdays)
- ✓ Never share, keep private when typing



USING EXTRA PROTECTION (2FA)



- ✓ Asks for extra code after PIN
- ✓ Adds more protection
- ✓ Allow & follow instructions
- ✓ Stops strangers even with phone



PROTECTING YOUR PHONE OR DEVICE



- ✓ Keep phone with you, locked
- ✓ No apps from unknown sources/links
- ✓ Allow updates (keeps safe)



FOLLOWING THESE SIMPLE SAFEGUARDS HELPS PROTECT YOUR VIRTUAL ASSETS & REDUCES RISK OF LOSS OR FRAUD



SECTION 6: Simple Risk Awareness

Understanding basic risks helps people avoid losing money when using virtual assets. Many problems occur not because people intend to do wrong, but because of small mistakes or because they trust the wrong information.

Common Mistakes to Avoid

- Sending money to the wrong phone number or wallet address.
- Sending money to a wallet that has not been checked or confirmed.
- Rushing through a transaction without reading what is on the screen.
- Allowing someone else to handle your phone during a transaction.

Once money is sent to the wrong place, it is often difficult or impossible to recover it.

PUBLIC



SIMPLE RISK AWARENESS

Understanding basic risks helps people avoid losing money when using virtual assets.



COMMON MISTAKES TO AVOID



Sending money to the wrong phone number or wallet address.



Sending money to a wallet that has not been checked or confirmed.



Rushing through a transaction without reading what is on the screen.



Allowing someone else to handle your phone during a transaction.

Once money is sent to the wrong place, it is often difficult or impossible to get it back.



Signs of Fraud to Watch For

- Messages that arrive unexpectedly asking you to send money or share details.
- Promises of very high returns or free money if you act quickly.
- Messages that create fear or urgency, telling you to send money immediately.



- People claiming to be helpers, agents, or officials without proof. These signs often mean someone is trying to trick you.

Asking for Help

- If you are unsure about a message, transaction, or app, stop and do not continue.
- Ask a trusted person, a known agent, or a family member for guidance.
- If a mistake happens, seek help immediately instead of hiding the problem.
- Asking early can prevent further loss and help protect others as well.

Being aware of these simple risks and knowing when to ask for help reduces mistakes and keeps your virtual assets safer.

PUBLIC



Assessment Strategy: Scenario Analysis

Scenario 1: Opening a Wallet with Help

Ama wants to start using digital money. She visits a nearby agent who helps her install a wallet on her phone. During the process, the agent asks Ama to share her PIN so he can finish setting it up more quickly. Ama hesitates but finally shares the PIN.

Discussion focus

- ✓ Was it safe to share the PIN?
- ✓ What should Ama have done differently?
- ✓ How should help from agents be handled safely?

Scenario 2: Sending Money to the Wrong Number

Kwame wants to send money to his sister in another town. He types the number quickly and presses send without checking the name on the screen. A few minutes later, he realised the money went to a different number.

Discussion focus

- ✓ What mistake did Kwame make?
- ✓ Which safety step was skipped?
- ✓ What should he do immediately after noticing the error?

Scenario 3: The Small Test Transaction

Adjoa is sending money to a new supplier for the first time. She remembers the advice to start small and sends a minimal amount first. The supplier confirms receipt, so she then sends the full payment safely.

Discussion focus

- ✓ What did Adjoa do right?
- ✓ Why is starting with a small amount important?
- ✓ How does this step protect users?



Scenario 4: Fake Platform Link

Yaw receives a WhatsApp message with a link saying, “Download this new wallet and get bonus money today.” The message looks urgent and promises quick profit. Yaw almost clicks the link.

Discussion focus

- ✓ What warning signs are present in this message?
- ✓ Why is clicking the link dangerous?
- ✓ What should Yaw do instead?

Scenario 5: Unexpected High Fees

Esi wants to send money using her wallet. Before pressing send, she notices a fee on the screen that looks higher than usual. She is confused but wants to rush because she is late.

Discussion focus

- ✓ What should Esi do before sending?
- ✓ Why is it essential to check fees?
- ✓ Who can she ask for help if she does not understand the fee?



Module 3

Module Title: Markets and Consumer Risks

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

Module Learning Outcomes

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

SECTION 1: Risks Everyone Should Know

When using virtual assets or digital money, there are different kinds of risks. Knowing these risks helps people avoid loss and stay safe.

Personal Risks

These risks come from individual actions or mistakes.

- Losing your password, PIN, or wallet key can stop you from accessing your money.
- Sending money to the wrong phone number or wallet address can lead to permanent loss.
- Trusting strangers or false helpers can result in scams.
- Allowing others to use your phone during transactions increases danger.



These risks can often be reduced by slowing down and following safety steps.

Platform Risks

These risks come from the apps or services used.

- Some apps or platforms may stop working suddenly.
- Unsafe platforms can be hacked and lose users' money.
- Fake platforms may be created only to steal funds and then disappear.
- Poor customer support can make it hard to get help when problems occur.

Using known and approved platforms helps reduce these risks.

System Risks

These risks affect the wider digital system.

- Prices of some virtual assets can change very quickly.
- Some platforms may fail or close without warning.
- Rules and guidance may not always be clear, confusing users.

Understanding that these risks exist helps people stay alert and avoid rushing into decisions. Being aware of personal, platform, and system risks is the first step toward safer use of virtual assets.



RISKS EVERYONE SHOULD KNOW

When using virtual assets or digital money, there are different kinds of risks. Knowing these risks helps people avoid loss and stay safe.

PERSONAL RISKS



Losing your password, PIN, or wallet key can stop you from accessing your money.



Sending money to the wrong phone number or wallet address can lead to permanent loss.



Trusting strangers or false helpers can result in scams.



Allowing others to use your phone during transactions increases danger.

These risks can often be reduced by slowing down and following safety steps.

PLATFORM RISKS



Some apps or platforms may stop working suddenly.



Unsafe platforms can be hacked and lose users' money.



Fake platforms may be created only to steal funds and then disappear.



Poor customer support can make it hard to get help when problems occur.

Using known and approved platforms helps reduce these risks.

SYSTEM RISKS



Prices of some virtual assets can change very quickly.



Some platforms may fail or close without warning.



Rules and guidance may not always be clear, causing confusion for users.



Understanding that these risks exist helps people stay alert and avoid rushing into decisions.

Being aware of personal, platform, and system risks is the first step toward safer use of virtual assets.



SECTION 2: Common Scams and Misconduct

Many people lose money because of scams and dishonest behaviour. These scams are often designed to look real and to pressure people into acting quickly. Knowing the common types helps people stay alert.

Fake Promises of Easy Money

- ✓ Some messages promise quick or guaranteed profits.
- ✓ They may say your money will double or grow fast with little effort.
- ✓ These promises are usually false and meant to trick people into sending money.





Impersonation

- ✓ Someone may pretend to be a friend, a known agent, or an official person.
- ✓ They may use a familiar name, picture, or voice to gain trust.
- ✓ Once trusted, they ask for money, PINs, or wallet details.



Common Scams and Misconduct

Impersonation



✓ Someone may pretend to be a friend, a known agent, or an official person.



✓ They may use a familiar name, picture, or voice to gain trust.



✓ Once trusted, they ask for money, PINs, or wallet details.





Fake Websites or Apps

- ✓ Some scammers create apps or websites that look exactly like real platforms.
- ✓ These fake platforms steal money or personal information.
- ✓ They are often shared through strange links or messages.

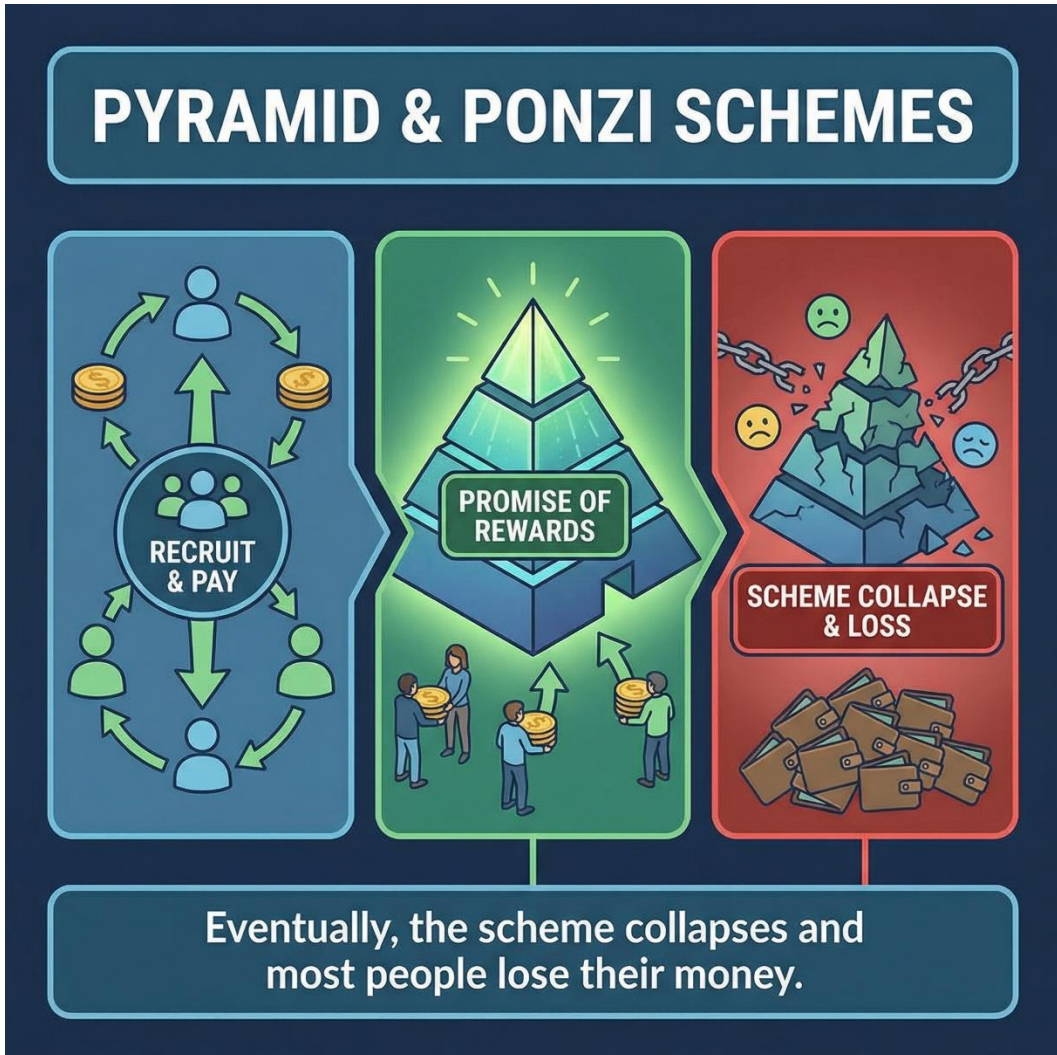






Pyramid or Ponzi Schemes

- ✓ These schemes ask you to send money and recruit other people.
- ✓ They promise rewards when you bring new members.
- ✓ Eventually, the scheme collapses and most people lose their money.





Warning Signs to Watch For

- Urgent messages asking you to send money immediately.
- Unknown links sent through SMS, WhatsApp, or social media.
- Offers that sound too good to be true.
- Requests for your PIN, password, or wallet details.

When any of these signs appear, stop and do not act. Asking for help early can prevent loss and protect others.





SECTION 3: How to Protect Yourself

Protecting yourself when using virtual assets or digital money is very important. Simple actions can prevent loss and keep your money safe.

- ✓ Use Only Licensed Apps and Platforms
- ✓ Check Who You Are Sending Money To
- ✓ Test with Small Amounts First
- ✓ Keep Your Passwords and PINs Safe
- ✓ Be Careful of Strangers

SECTION 4: Cybersecurity Basics

Cybersecurity is about keeping your phone and digital money safe from harm. Simple actions can prevent many problems.

Keep Your Device Updated

- ✓ Allow updates when your phone asks for them.



- ✓ Updates help fix weaknesses and remove harmful software.
- ✓ A well-updated phone is harder for scammers to attack.

CYBERSECURITY BASICS

KEEP YOUR DEVICE UPDATED

- ✓ Allow updates when your phone asks for them.
- ✓ Updates help fix weaknesses and remove harmful software.
- ✓ A well-updated phone is harder for scammers to attack.





Avoid Unknown Links and Apps

- ✓ Do not click links from messages you were not expecting.
- ✓ Be careful with links sent through SMS, WhatsApp, or social media.
- ✓ Do not download apps shared by strangers or unknown websites.
- ✓ Use only trusted app stores or get help from a known agent.



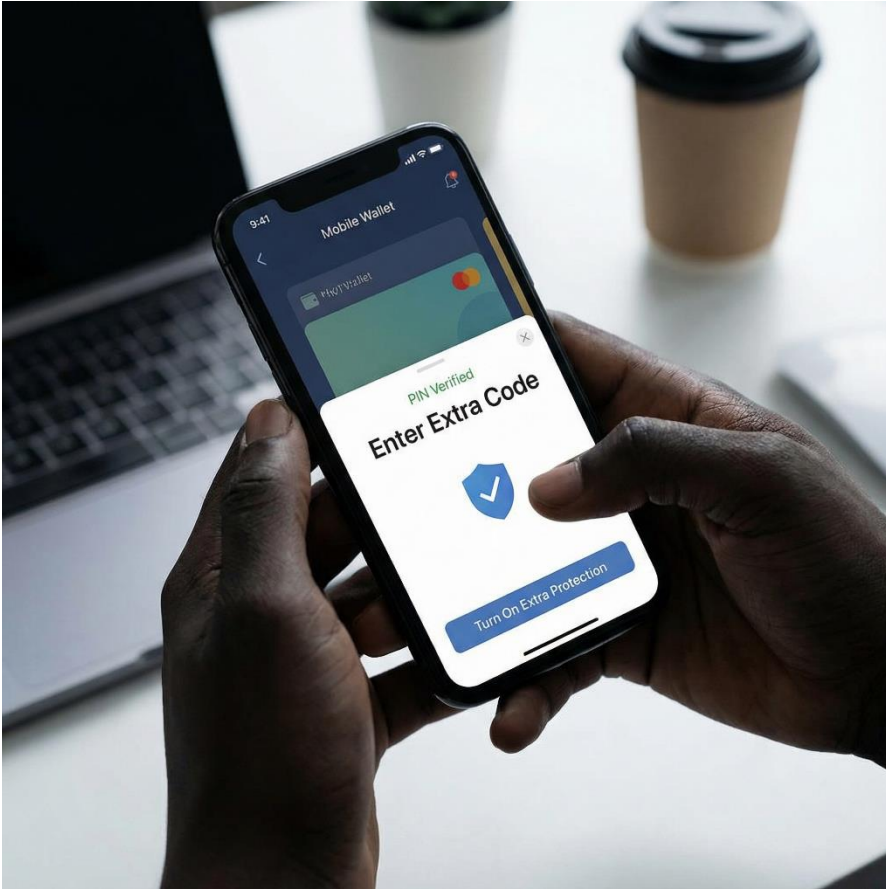


Use Extra Protection if Available

- ✓ Some apps ask for an extra code after you enter your PIN.
- ✓ This extra step gives more protection to your wallet.
- ✓ If your app offers this option, turn it on and follow the steps shown.

These basic habits help protect your device, your wallet, and your money from theft or misuse.





SECTION 5: What to Do if Something Goes Wrong

- ✓ Stop using the platform immediately.
- ✓ Keep proof: screenshots, messages, transaction numbers.
- ✓ Report to platform support, local authorities, or official hotlines.
- ✓ Ask for help from trusted friends, family, or community leaders.



Section 5: What to Do if Something Goes Wrong



1. STOP IMMEDIATELY



Stop using the platform immediately.



2. KEEP PROOF



Keep proof: screenshots, messages, transaction numbers.



3. REPORT IT



Report to platform support, local authorities, or official hotlines.



4. ASK FOR HELP



Ask for help from trusted friends, family, or community leaders.





Assessment Strategy Red Flag Exercise

Red Flag Exercise 1: The Urgent Message

Scenario

A person receives a WhatsApp message that says:
 “Your account has a problem. Send money now, or it will be blocked.
 Click this link to fix it quickly.”

Task for the Group

- Identify the red flags in the message.
- Decide whether to act immediately or stop.
- Discuss what the correct action should be.

Expected Red Flags

- Urgent pressure to act quickly.
- A link sent through a message.
- Threat of account blockage.
- No clear proof of who sent the message.



Key Lesson

Urgency and fear are common tricks used in scams.

Red Flag Exercise 2: The Helpful Stranger Scenario

At a market, a stranger offers to help someone send digital money. The stranger asks to hold the phone and says, “Tell me your PIN so I can help you faster.”

Task for the Group

- Identify what is unsafe in this situation.
- Discuss what should never be shared.
- Decide what the user should do instead.

Expected Red Flags

- Asking for a PIN or password.
- Taking control of the phone.
- Offering help without being a known agent.

Key Lesson

No one should ask for your PIN or handle your phone during a transaction.

Red Flag Exercise 3: The Easy Money Group Scenario

Someone is added to an online group where members are told to send a small amount of money and invite others. The message says, “Bring three people and your money will grow.”

Task for the Group

- Identify the warning signs in this offer.
- Discuss what will likely happen to the money.
- Decide whether to join or avoid the group.



Expected Red Flags

- Promise of quick or guaranteed profits.
- Requirement to recruit others.
- No clear information about the platform or owners.

Key Lesson

Schemes that ask you to bring others and promise fast returns are usually scams.

PUBLIC



Module 4

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

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

Module Learning Outcomes

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

SECTION 1: Why Regulation Exists

Regulation exists to protect people and their money. It helps reduce fraud, scams, and dishonest behaviour. Rules also guide how digital money services should operate so users are treated fairly. Regulation supports safety, order, and trust when people use virtual assets.

SECTION 2: Activities Covered by Regulation

Rules control some activities related to virtual assets. These include buying and selling digital money, storing digital cash for others, and helping people send or receive virtual assets. Services that manage money on behalf of users are expected to follow rules to protect customers.



SECTION 3: Who Is Licensed or Authorised

Licensed or authorised providers are services approved by authorities to operate. These providers follow specific rules and standards. Using licensed services gives users a better chance of support if something goes wrong. Not all apps or platforms are licensed, so checking is essential.

SECTION 4: Consumer Protections and Reporting

Consumer protections help users when problems occur. Platforms are expected to provide help, explain fees, and handle complaints. If a user faces fraud, loss, or suspicious activity, they should report it to the service provider first. Severe cases can also be reported to agents, local authorities, or official hotlines.

SECTION 5: Staying Safe and Informed

People should stay alert when using virtual assets. Always check information before acting. Avoid rushing into offers or messages that promise quick gains. Listen to advice from trusted sources and community leaders. Staying informed and careful helps prevent loss and protects both individuals and families.



Assessment Strategy

Quiz 1: Why Regulation Exists

Which of the following are reasons why regulation exists?

(Choose all that apply)

- A. To protect people and their money
- B. To reduce fraud and scams
- C. To help dishonest platforms operate freely
- D. To support safety and trust

Correct answers: A, B, D

Quiz 2: Activities Covered by Regulation

Which activities are usually controlled by rules?

(Choose all that apply)

- A. Buying and selling digital money
- B. Storing digital money for others
- C. Helping people send or receive virtual assets
- D. Sending money only to family members

Correct answers: A, B, C

Quiz 3: Licensed or Authorised Providers

Which statements about licensed providers are factual?

(Choose all that apply)

- A. The authorities approve them
- B. They follow rules and standards
- C. They can never have problems
- D. They give users better support if something goes wrong

Correct answers: A, B, D



Quiz 4: Checking Platforms

Which actions help you know if a platform is safe?

(Choose all that apply)

- A. Checking if it is licensed or authorised
- B. Using apps shared by strangers
- C. Asking a trusted agent or person
- D. Looking for precise contact details

Correct answers: A, C, D

Quiz 5: Consumer Protection and Reporting

What should you do if you face fraud or suspicious activity?

(Choose all that apply)

- A. Report to the service provider
- B. Ignore the problem and move on
- C. Keep proof like messages or transaction numbers
- D. Report severe cases to authorities or hotlines

Correct answers: A, C, D

Quiz 6: Staying Safe and Informed

Which actions help people stay safe when using virtual assets?

(Choose all that apply)

- A. Checking information before acting
- B. Rushing into offers that promise quick gains
- C. Listening to advice from trusted sources
- D. Staying alert and careful

Correct answers: A, C, D



Quiz 7: Identifying Risky Offers

Which of the following are warning signs of risky offers?

(Choose all that apply)

- A. Messages promising quick or free money
- B. Pressure to act immediately
- C. Clear information from trusted authorities
- D. Offers that sound too good to be true

Correct answers: A, B, D

PUBLIC



References

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

Singh, D. (2025), *What are utility tokens and how do they work?* Debut Infotech.

The Investopedia Team. (2025), *Types and characteristics of digital currencies: Pros, cons, future applications*. Investopedia.

PUBLIC



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.

PUBLIC





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: 978-9988-41-656-0

