



REPUBLIC OF KENYA

VIRTUAL ASSETS

A Beginner's Guide for Legal Professionals

Understanding Cryptocurrency, Blockchain, and Digital Asset Law

Prepared for: Kenya Legal Professionals Training Programme

Audience: Lawyers, Advocates & Legal Practitioners

Date: 2026

About These Training Notes

These notes are designed specifically for legal professionals in Kenya who are new to the world of virtual assets and digital currencies. The language is intentionally straightforward — we have avoided unnecessary technical jargon where possible, and where technical terms are used, they are clearly explained.

By the end of these notes, you should be able to:

- Explain what virtual assets are and how they work in simple terms
- Identify the major types of virtual assets
- Understand the legal and regulatory landscape in Kenya and globally
- Recognise the key legal risks and issues that arise in virtual asset transactions
- Advise clients on basic compliance requirements

How to Use These Notes

Work through each section in order. Key terms are highlighted and collected in the Glossary at the end. Practical examples drawn from Kenyan contexts are included throughout. Boxes like this one highlight important points.

Module 1: What Are Virtual Assets?

1.1 A Simple Starting Point

Imagine you and a friend agree that a certain token (like a poker chip) has value — say, it can be exchanged for goods or services. Nobody issued it officially; you both just agreed it has worth. Virtual assets work on a similar principle, but on a global digital scale, and without a central authority like a bank or government controlling them.

A virtual asset is a digital representation of value that can be traded, transferred, or used as a means of exchange or investment — but it exists only in digital form, with no physical coin or note.

FATF Definition (International Standard)

The Financial Action Task Force (FATF) — the global standard-setter for anti-money laundering — defines a virtual asset as: "a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes." Kenya's emerging framework draws on this definition.

1.2 Virtual Assets vs. Related Concepts

It helps to distinguish virtual assets from related but distinct concepts:

Term	Definition / Explanation
Virtual Asset (VA)	Broad category — any digital representation of value tradeable or transferable electronically. Includes cryptocurrencies, tokens, and more.
Cryptocurrency	A type of virtual asset that uses cryptography (complex mathematical codes) to secure transactions. Examples: Bitcoin (BTC), Ether (ETH).
Digital Currency	Can include government-issued digital money (like a Central Bank Digital Currency — CBDC) and private virtual assets.
E-Money	Electronic version of fiat (government) money, e.g., M-Pesa balance. Regulated differently from virtual assets.
Stablecoin	A virtual asset designed to maintain a stable value, often pegged to a currency like the US Dollar. Example: USDT (Tether).
NFT (Non-Fungible Token)	A unique digital token representing ownership of a specific item (art, music, etc.). Unlike Bitcoin, each NFT is one-of-a-kind.
CBDC	Central Bank Digital Currency — a digital version of a national currency issued by a government. Kenya's Central Bank has explored this concept.

1.3 Why Should Lawyers Care?

Virtual assets are no longer a niche technology topic. They are increasingly relevant to legal practice in multiple areas:

- **Criminal Law:** Virtual assets are used in money laundering, fraud, and ransomware attacks.
- **Family Law:** Spouses may hold cryptocurrency as hidden assets during divorce proceedings.

- **Commercial Law:** Contracts may involve payment in cryptocurrency or token-based instruments.
- **Tax Law:** The Kenya Revenue Authority (KRA) has signalled interest in taxing virtual asset gains.
- **Banking & Finance:** Clients may seek advice on virtual asset investments or fundraising (token sales).
- **Property Law:** NFTs raise questions about digital ownership and intellectual property rights.
- **Employment Law:** Some employers (including global firms) pay salaries partially in cryptocurrency.

Module 2: How Blockchain Technology Works

2.1 The Basics — No Technical Background Needed

To understand virtual assets, you need a basic grasp of blockchain — the underlying technology. Think of a blockchain as a public notebook that records every transaction ever made. The key features that make it different from a normal bank ledger are:

2.1.1 Decentralisation

Instead of one bank holding a master record, thousands of computers around the world each hold an identical copy of the notebook. There is no single owner or controller. This is why Bitcoin, for example, has no headquarters or CEO.

2.1.2 Immutability

Once a transaction is written into the blockchain, it cannot be changed or deleted. Each new "block" of transactions is mathematically linked to the one before it — like a sealed chain. Altering one block would break the chain, and the network would reject it.

Legal Significance of Immutability

Because blockchain records cannot be altered, they can serve as strong evidence in litigation — for example, proving that a payment was made at a specific time, or that a smart contract was executed. However, they also mean that errors (such as sending funds to the wrong address) are very difficult or impossible to reverse.

2.1.3 Transparency

On public blockchains (like Bitcoin), anyone can view every transaction ever recorded. However, identities are pseudonymous — meaning accounts are identified by a long code (a "wallet address"), not a name.

2.1.4 Smart Contracts

A smart contract is a self-executing programme stored on the blockchain. It automatically performs agreed actions when pre-set conditions are met — similar to a vending machine that gives you a product when you insert the right amount of money.

Example: A smart contract for an escrow arrangement could automatically release payment to a supplier once a delivery confirmation is recorded on the blockchain — without any bank or lawyer needed to release funds.

Legal Question for Practitioners

If a smart contract automatically executes and causes harm (e.g., releases funds incorrectly due to a bug), who bears liability — the developer, the deployer, or the parties who agreed to use it? This is an unresolved area of law in Kenya and globally.

2.2 Public vs. Private Blockchains

Not all blockchains are the same. The distinction matters legally:

Public Blockchain	Private / Permissioned Blockchain
Open to anyone to participate	Restricted to approved participants only
Bitcoin, Ethereum (global, permissionless)	Banks' internal settlement systems, trade finance platforms
No central authority	Controlled by an organisation
Higher privacy concerns for regulators	Easier to regulate and audit

Module 3: Types of Virtual Assets

3.1 Major Categories

3.1.1 Payment Cryptocurrencies

These are designed primarily to function as a medium of exchange — digital money. The most prominent example is Bitcoin (BTC), created in 2009. Ether (ETH) is another, though it also powers the Ethereum blockchain's broader functions.

3.1.2 Utility Tokens

These tokens give holders access to a specific product or service on a platform. They are not necessarily investments — they are more like prepaid vouchers. Example: A gaming platform may issue tokens that let users purchase in-game items.

3.1.3 Security Tokens

These represent ownership or equity in an asset — similar to shares or bonds, but in digital form. This is legally significant because they may trigger securities law requirements. In Kenya, this would fall under the purview of the Capital Markets Authority (CMA).

3.1.4 Stablecoins

Designed to maintain a stable value, typically pegged 1:1 to a fiat currency like the US Dollar. Examples include USDT (Tether) and USDC (USD Coin). They are widely used in international remittances and cross-border payments — highly relevant in Kenya's context given the importance of the diaspora remittance corridor.

3.1.5 Non-Fungible Tokens (NFTs)

Each NFT is unique and cannot be exchanged one-for-one with another (unlike Bitcoin, where one Bitcoin always equals another Bitcoin). NFTs represent ownership of specific digital items: art, music, videos, real estate deeds, or even legal documents. Questions of intellectual property and asset ownership are central here.

3.1.6 Central Bank Digital Currencies (CBDCs)

These are digital currencies issued and controlled by a country's central bank — the digital equivalent of the Kenya Shilling note. They carry government backing, making them legally and financially distinct from private virtual assets. The Central Bank of Kenya (CBK) has studied but not yet issued a CBDC.

Module 4: The Legal and Regulatory Landscape in Kenya

4.1 Kenya's Current Position

As of 2026, Kenya does not have a single, comprehensive Virtual Asset law. Regulation is evolving and spread across several existing frameworks and regulatory bodies:

Term	Definition / Explanation
Central Bank of Kenya (CBK)	Has warned the public against using cryptocurrency as legal tender. Legal tender in Kenya remains the Kenya Shilling. However, the CBK has not banned all virtual asset activity outright.
Capital Markets Authority (CMA)	Has powers under the Capital Markets Act to regulate securities. Tokens that qualify as securities may fall within CMA jurisdiction. The CMA has issued guidance on digital asset exchanges.
Kenya Revenue Authority (KRA)	Treats gains from virtual asset trading as taxable income. There is no specific cryptocurrency tax law, but general income tax principles apply.
Financial Reporting Centre (FRC)	Kenya's anti-money laundering (AML) authority. Virtual asset businesses may need to register and comply with AML/CFT obligations under the Proceeds of Crime and Anti-Money Laundering Act (POCAMLA).
Communications Authority	Has a peripheral role regarding digital platforms and cybercrime related to virtual assets.

Key Point: No Ban, But No Formal Legal Tender Status

Cryptocurrency is not illegal in Kenya, but it is not recognised as legal tender. This creates a legal grey area: private parties may agree to transact in cryptocurrency, but it cannot be forced on a creditor as payment of a debt in the way that Kenya Shillings can.

4.2 Relevant Kenyan Legislation

- Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), 2009 — primary AML framework; applies to virtual asset businesses.
- Prevention of Terrorism Act, 2012 — covers financing of terrorism through any means, including virtual assets.
- Computer Misuse and Cybercrimes Act, 2018 — addresses online fraud, hacking, and related offences relevant to virtual asset crime.
- Capital Markets Act (Cap. 485A) — may apply to token offerings that constitute securities.
- Income Tax Act (Cap. 470) — capital gains and income tax principles apply to virtual asset profits.
- National Payment System Act, 2011 — may apply to virtual asset payment services.

4.3 The FATF Framework — Why It Matters in Kenya

Kenya is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), which is affiliated with FATF. FATF's Recommendation 15 requires countries to regulate Virtual Asset Service Providers (VASPs) for AML/CFT purposes. Kenya has been under

pressure to improve its compliance, meaning we can expect more formal virtual asset regulation in coming years.

Who is a VASP?

A Virtual Asset Service Provider (VASP) is any business that offers services including:

- Exchange between virtual assets and fiat currencies (e.g., converting Bitcoin to Kenya Shillings)
- Exchange between different virtual assets
- Transfer of virtual assets
- Safekeeping/administration of virtual assets (custodial wallets)
- Participation in or provision of financial services related to an issuer's offer or sale of a virtual asset

Practical Implication

If your client operates a cryptocurrency exchange, a wallet service, or facilitates token sales, they may already be operating as a VASP and have AML compliance obligations under POCAMLA – even without specific cryptocurrency legislation.

4.4 Comparative Snapshot: What Are Other African Countries Doing?

Country	Status
South Africa	First to formally licence crypto exchanges (FSCA); comprehensive framework in place.
Nigeria	Has licenced VASPs through the SEC; digital asset regulation is active.
Ghana	Bank of Ghana exploring CBDC; virtual asset rules developing.
Rwanda	Progressive approach; seeking to become a fintech hub.
Tanzania	Has been more restrictive; has previously issued bans on some cryptocurrency activity.

Module 5: Key Legal Issues in Virtual Asset Practice

5.1 Contract Law and Virtual Assets

When parties contract using virtual assets, standard contract law principles apply — offer, acceptance, consideration, capacity, legality. However, unique questions arise:

- **Denomination Risk:** If a contract specifies payment in Bitcoin, and Bitcoin's value drops 50% before payment, who bears the loss? Contracts must clearly address exchange rate risk.
- **Irreversibility:** Unlike a bank transfer which can sometimes be reversed, a blockchain transaction is generally final. Escrow and conditional payment mechanisms need to be carefully structured.
- **Smart Contracts:** Are they legally binding contracts? Most legal scholars say yes — provided the elements of a valid contract are met. The issue is enforcement and identifying parties.

5.2 Property Law

Can virtual assets be owned, inherited, seized, or attached? These questions are only beginning to be addressed by courts globally. Key issues include:

- **Classification:** Is cryptocurrency personal property? In England, the courts have held that it is a form of property. Kenya has not definitively ruled on this.
- **Seizure by Law Enforcement:** Police can obtain private keys (the "password" to a cryptocurrency wallet) through court order. Kenya's DCI has experience with this in fraud cases.
- **Matrimonial Property:** Spouses may hold cryptocurrency secretly. Practitioners need to know to ask about virtual asset holdings in divorce proceedings.
- **Succession:** Cryptocurrency held only in a deceased person's memory (with no key backup) may be permanently inaccessible — a novel problem for estate lawyers.

5.3 Anti-Money Laundering (AML) Compliance

This is currently the most active area of virtual asset law practice. The key obligations for VASPs under Kenya's AML framework include:

- **Customer Due Diligence (CDD):** Know Your Customer (KYC) — verify the identity of customers using government-issued ID.
- **Enhanced Due Diligence (EDD):** For high-risk customers, politically exposed persons (PEPs), or large transactions.
- **Transaction Monitoring:** Flag and report suspicious transactions to the Financial Reporting Centre.
- **Record Keeping:** Maintain transaction records for at least 7 years.
- **Travel Rule:** For international transfers above a threshold, transmit sender and recipient information — a FATF requirement increasingly enforced globally.

AML Red Flags in Virtual Asset Transactions

Watch for: structuring transactions to avoid reporting thresholds ("smurfing"); use of mixers or tumblers (tools designed to obscure transaction trails); transactions from high-risk jurisdictions; customers unwilling to provide identification; rapid movement of large sums across multiple wallets.

5.4 Taxation of Virtual Assets

The KRA's position is that virtual asset income is taxable. Lawyers advising clients on virtual assets should consider:

- **Trading Gains:** Profits from buying and selling cryptocurrency are likely taxable as income or capital gains.
- **Mining Income:** Income from cryptocurrency mining is taxable.
- **Payment in Cryptocurrency:** If an employee is paid in cryptocurrency, the employer may have PAYE obligations; the value at the time of receipt would need to be determined.
- **VAT:** Whether virtual asset transactions attract VAT is unsettled in Kenya; advise clients to take professional tax advice.

5.5 Fraud and Criminal Law

Virtual assets feature prominently in financial crime. Common schemes include:

- **Investment Fraud / Ponzi Schemes:** Fraudsters promise high returns on cryptocurrency investments. Several Kenyan victims have lost funds to schemes promising Bitcoin returns.
- **Ransomware:** Cybercriminals encrypt victims' data and demand payment in cryptocurrency (because it is harder to trace).
- **Phishing:** Attackers trick victims into revealing wallet private keys or login credentials.
- **Romance Scams:** Fraudsters build fake relationships online and convince victims to invest in fake cryptocurrency platforms.
- **Rug Pulls:** Token creators launch a cryptocurrency, attract investors, then disappear with the funds.

For Criminal Defence Practitioners

Blockchain analytics firms (such as Chainalysis and Elliptic) can trace cryptocurrency transactions across the blockchain. Prosecutors are increasingly using this evidence. Defence teams need to understand how blockchain evidence is obtained and its limitations.

Module 6: Advising Clients — Practical Scenarios

6.1 Scenario 1: Client Wants to Set Up a Cryptocurrency Exchange

Your client, a tech entrepreneur, wants to launch a platform where Kenyans can buy and sell Bitcoin and other cryptocurrencies using M-Pesa. Key advice points:

- The client will almost certainly qualify as a VASP and must comply with POCAMLA — including registering with the FRC and implementing a full AML/CFT programme.
- Engage the CBK early — payment services linking to M-Pesa may require approval under the National Payment System Act.
- Consider CMA engagement if the platform will deal in any tokens that could be classified as securities.
- Draft clear Terms of Service addressing dispute resolution, liability for failed transactions, and KYC requirements.
- Implement data protection compliance under the Data Protection Act, 2019 — customer data will be held.

6.2 Scenario 2: Divorce — Spouse Suspected of Hiding Cryptocurrency

In matrimonial proceedings, your client suspects their spouse is hiding wealth in cryptocurrency. Key advice points:

- Apply for disclosure orders — courts can compel disclosure of digital assets just as with bank accounts.
- Look for evidence of cryptocurrency holdings: exchange account emails, hardware wallets (physical devices), transaction receipts, or references in financial records.
- Blockchain forensic experts can trace transactions if a wallet address is known.
- Note that without the private key, even if an account is identified, accessing funds may require specialist technical assistance.

6.3 Scenario 3: Client is a Victim of Cryptocurrency Fraud

Your client invested KES 500,000 on a platform promising 30% monthly Bitcoin returns. The platform has disappeared. Key advice points:

- Report to the Directorate of Criminal Investigations (DCI) — Kenya has experience investigating cryptocurrency fraud.
- Report to the Communications Authority if the fraud was conducted through a digital platform.
- Blockchain analytics may help trace where funds went, but recovery is not guaranteed.
- Consider civil remedies against any identifiable individuals or entities involved.
- Advise client honestly: recovery of cryptocurrency from sophisticated fraudsters is extremely difficult and often not possible.

Module 7: Glossary of Key Terms

The following terms are used throughout these notes and in virtual asset law and practice generally:

Term	Definition / Explanation
Blockchain	A distributed digital ledger recording transactions in chronological, tamper-resistant blocks linked in a chain.
Cryptocurrency	A virtual asset that uses cryptographic techniques to secure transactions and control the creation of new units.
Bitcoin (BTC)	The first and most widely known cryptocurrency, created in 2009 by an anonymous person or group known as Satoshi Nakamoto.
Ethereum (ETH)	A blockchain platform that supports smart contracts and decentralised applications; its native currency is Ether.
Wallet	A software or hardware tool that stores the cryptographic keys allowing a user to access and transact with their virtual assets.
Private Key	A secret code (like a PIN) that proves ownership of virtual assets. Losing it means losing access to the assets permanently.
Public Key / Wallet Address	A shareable address (like a bank account number) to which others can send virtual assets.
Smart Contract	A self-executing programme on the blockchain that automatically performs actions when specified conditions are met.
DeFi (Decentralised Finance)	Financial services (lending, trading, savings) provided through smart contracts on a blockchain, without banks.
NFT	Non-Fungible Token – a unique digital token representing ownership of a specific item or piece of content.
Stablecoin	A virtual asset pegged to a stable value, usually a fiat currency like the US Dollar.
CBDC	Central Bank Digital Currency – a government-issued digital currency.
VASP	Virtual Asset Service Provider – any business providing exchange, transfer, or custody services for virtual assets.
FATF	Financial Action Task Force – the global body that sets anti-money laundering and counter-terrorism financing standards.
KYC	Know Your Customer – the process of verifying a customer's identity to prevent financial crime.
AML/CFT	Anti-Money Laundering / Counter-Financing of Terrorism – regulations to prevent the use of financial systems for crime.
Mining	The process by which new cryptocurrency transactions are verified and added to the blockchain, typically rewarded with new coins.
Exchange	A platform where virtual assets can be bought, sold, or traded – either for fiat currency or other virtual assets.
Hash / Hash Function	A mathematical function that converts data into a fixed-length code; used to secure blockchain transactions.

Term	Definition / Explanation
Fork	A change to a blockchain's protocol — a "hard fork" creates a permanent divergence, potentially creating a new cryptocurrency.
ICO / ITO	Initial Coin Offering / Initial Token Offering — a fundraising method where a project sells tokens to early investors.
Rug Pull	A type of fraud where developers of a cryptocurrency project abandon it and abscond with investor funds.
Tumbler / Mixer	A service that obscures the trail of cryptocurrency transactions by mixing funds with those of other users — a red flag for AML.
Travel Rule	FATF rule requiring VASPs to share sender and recipient information for transfers above a threshold amount.
POCAMLA	Proceeds of Crime and Anti-Money Laundering Act, 2009 — Kenya's primary AML legislation.
FRC	Financial Reporting Centre — Kenya's financial intelligence unit responsible for AML oversight.

Module 8: Quick Reference — Key Contacts and Resources

Term	Definition / Explanation
Central Bank of Kenya (CBK)	www.centralbank.go.ke — Monetary policy, payment systems, CBDC developments.
Capital Markets Authority (CMA)	www.cma.or.ke — Securities regulation; digital asset guidance.
Financial Reporting Centre (FRC)	www.frc.go.ke — AML/CFT compliance, suspicious transaction reports.
Kenya Revenue Authority (KRA)	www.kra.go.ke — Tax obligations on virtual asset income.
Communications Authority	www.ca.go.ke — Digital platform and cybercrime matters.
Directorate of Criminal Investigations (DCI)	www.dci.go.ke — Report cryptocurrency fraud and financial crime.
FATF	www.fatf-gafi.org — International AML standards and guidance on virtual assets.
ESAAMLG	www.esaamlg.org — Regional AML body; Kenya's FATF-style regional body.
Blockchain Simulator	Interactive learning tool — explore how blockchain transactions, blocks, and chains work in practice. Recommended for participants wanting a hands-on introduction: blockchainsim.blockchainsimulations.com

Module 9: Key Stakeholders in the Virtual Asset Ecosystem

Understanding who the major players are in the global virtual asset ecosystem helps legal professionals identify counterparties, assess risk, and advise clients more effectively. The stakeholders below represent the most prominent exchanges, service providers, analytics firms, and stablecoin issuers currently operating internationally. Participants are encouraged to explore their websites and published compliance policies.

9.1 Major Cryptocurrency Exchanges

Stakeholder	Description / Relevance to Legal Practitioners
Binance	The world's largest cryptocurrency exchange by trading volume. Widely used across Africa, including Kenya. Subject to enforcement actions in multiple jurisdictions over AML compliance. Relevant in cases involving large-volume cryptocurrency transactions. Website: www.binance.com
Coinbase	A publicly listed US-based exchange (NASDAQ: COIN) known for its strong regulatory compliance posture. Often cited as a model for compliant VASP operations. Publishes detailed legal and compliance documentation. Website: www.coinbase.com
Kraken	A well-established US-based exchange with a reputation for security and transparency. Has faced regulatory scrutiny in the United States over securities law. Useful reference for understanding exchange terms of service and dispute resolution practices. Website: www.kraken.com
Yellow Card	Africa-focused cryptocurrency exchange operating in over 20 African countries including Kenya. Facilitates local currency on-ramps and off-ramps. Highly relevant to East African virtual asset cases. Website: www.yellowcard.io
Paxful	Peer-to-peer Bitcoin marketplace popular in Africa. Allows trades using M-Pesa and other local payment methods. Commonly referenced in Kenyan fraud investigations. Website: www.paxful.com

9.2 Stablecoin Issuers

Issuer	Description / Relevance
Tether (USDT)	Largest stablecoin by market capitalisation, pegged to the US Dollar. Issued by Tether Limited. Widely used in cross-border remittances and frequently appears in AML investigations. Website: tether.to
Circle (USDC)	Issuer of USD Coin (USDC), a fully reserved and regulated stablecoin. Circle maintains high transparency standards and publishes regular reserve attestations. Considered a more regulation-friendly stablecoin. Website: www.circle.com

9.3 Blockchain Analytics and Compliance Firms

Firm	Description / Relevance
Chainalysis	Leading blockchain analytics company used by law enforcement, regulators, and VASPs globally to trace cryptocurrency flows and identify illicit activity. Their tools are used in criminal prosecutions. Publishes annual Crypto Crime Report — a valuable resource. Website: www.chainalysis.com

Firm	Description / Relevance
Elliptic	A blockchain analytics and AML compliance firm used by financial institutions and governments. Provides risk-scoring of cryptocurrency transactions. Referenced alongside Chainalysis in major cross-border investigations. Website: www.elliptic.co

Closing Note for Participants

Virtual assets represent one of the most rapidly evolving areas of law globally. What is written here reflects the position as of 2026, but the landscape — including Kenyan legislation, regulatory guidance, and court decisions — is changing quickly.

As legal professionals, your role is not to become blockchain engineers, but to:

- Ask the right questions when clients present virtual asset issues
- Recognise which regulatory bodies are relevant
- Understand the core legal risks (AML, fraud, contract, property, tax)
- Know when to bring in specialist technical or forensic expertise

A Final Thought

The law always follows technology. Our task as lawyers is to apply enduring legal principles — property, contract, evidence, liability — to new forms. Virtual assets are new instruments; the legal questions they raise are largely familiar ones in unfamiliar dress.

END OF TRAINING NOTES

These notes are for educational purposes only and do not constitute legal advice.