Blockchain & Cryptos – The Hype, Possibilities & Realities

Blockchain & Cryptos – The Hype, Possibilities & Realities

J. Walubengo
Member National Taskforce on Blockchain & AI
Jwalubengo@mmu.ac.ke. Walu.John@gmail.com
ICPAK, Oct 2020

Summary

- The Initial Problem & The Solution- Bitcoin
- Blockchain vs Bitcoin – how it works
- What exactly is Blockchain?
- Characteristics & Types of Blockchains
- Taxonomy of Digital Assets
- Digital Token Economy & Opportunities
- Digital Token Risks & Realities
- Regulatory Frameworks
- State of Play in KE

The Initial Problem

- **The Question:** How Can we Send Money (Value) over the Internet without the need for Central Intermediaries (e.g Banks, Western Money Union, etc)
- The **Double Spend Problem:** The double spending problem is about a user being able to simultaneously spend or transfer the same money(digital token) to two or more different accounts.
- In a **centralized system**, a trusted third party/ authority sorts out this issue (Banks, Credit Card Providers etc).
- The central authority (3rd Party) has a global view of all transactions happening between the two parties and can therefore prevent a user from spending the same money to multiple accounts.

The Solution - Bitcoin

- In **a decentralized system**, this problem is much harder to solve

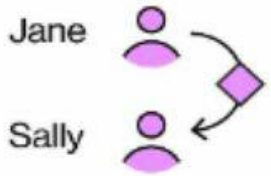
- Satoshi (Bitcoin) creator, created a technical system that simulates and replaces Trusted 3rd Parties – Blockchain

- Blockchain is the underlying technology supporting the (bitcoin) crypto-currency:
  - It is a distributed database that is practically immutable and is maintained by a decentralized Peer to Peer network
  - It uses a consensus mechanism, cryptography and back-referencing blocks to order and validate transactions

How Blockchain Works for Bitcoin

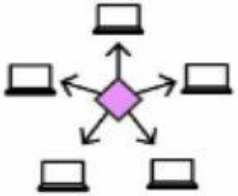
When payment is made with a physical coin, the person who handed it over can't spend it again. Preventing "double spending" in a digital currency is more complicated.

Transaction



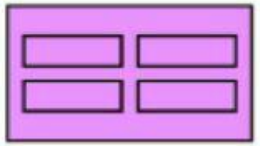
Jane uses bitcoin to buy a cup of coffee at Sally's internet café, using her private key to transfer ownership of the currency.

Mining network



Word of the transaction is sent through the bitcoin network to "miners" with powerful computers.

Block

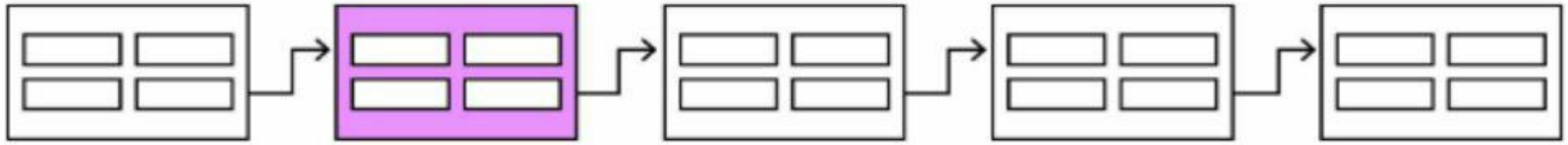


Miners use trial-and-error computations to solve a puzzle created by combining data about recent transactions. The first to find the unique number that unlocks the puzzle earns the right to bundle the transactions into a confirmed batch known as a block.

Verification

The winning miner is rewarded with newly minted bitcoin — but only after other miners confirm that the block's transactions don't contain any attempts to spend the same funds twice.

The Chain



Blockchain acts as a public ledger showing all transactions, though the identities of participants are obscured. Each block has a cryptographic link to the previous one. Every addition of a new, linked block to the chain makes it harder for a rogue miner to steal Sally's bitcoin by rewriting the sequence of transactions.

Data: Bloomberg; graphic by Bloomberg QuickTake

Blockchain vs Bitcoin

- Bitcoin is a crypto-currency and is the first successful application that ran on an underlying Blockchain Technology.
- Blockchain powers the record-keeping system for crypto-currency being exchanged between users without the need for a central authority (banks)
- The reliability and efficiency of this model can be exported to other industries/use cases.

What exactly is Blockchain?

- Blockchain and DLT systems are new accounting tools that enable shared distributed recordkeeping
  -without the need to rely on a single controlling party
- Records are added into database (ledger) using consensus mechanisms or protocols.
- Video
- https://www.cigionline.org/multimedia/what-blockchain

Characteristics of a Blockchain

- The main thing distinguishing a blockchain from a normal database is that there are specific rules about how to put data into the database.
- That is, it cannot conflict with some other data that's already in the database (consistent),
- it's append-only (immutable), and the data itself is locked to an owner (ownable),
- it's replicable, distributed and highly available.
- Finally, each node agrees on what the state of the things in the database are) without a central party (decentralized)

Types of Blockchains

- **Public Blockchains**
- Public blockchains allow all/any nodes to read blockchain data and propose new transactions.

- **Private Blockchains**
- Private Blockchains allow only nodes that are preregistered by a central authority to read blockchain data and submit new transactions

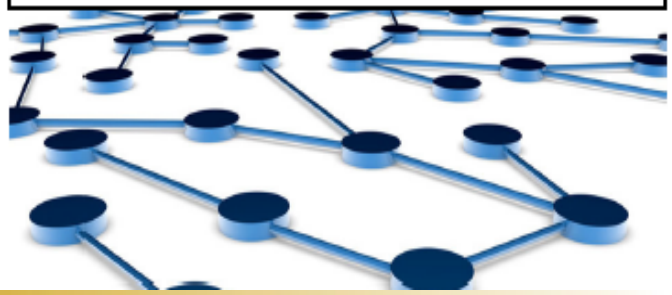
Types of Blockchain

Validation

Access	Permissionless	Permissioned
Public	Bitcoin IOTA Ethereum	Sovrin
Private	Hyperledger Sawtooth	Hyperledger Fabric R3 Corda Quorum

Blockchain Ecosystem

Use Case (Based on Token Type)		
Money Cryptocurrency -Token	Property Securities-Token	Voting Utility-Token
Smart Contracts (Programmable Layer/Token Layer)		
Blockchain (Distributed, Cryptographic Database)		
Public (Who Validates Transaction: AnyNode)	Private (Who Validates Transaction: Select Nodes)	
Internet Layer		

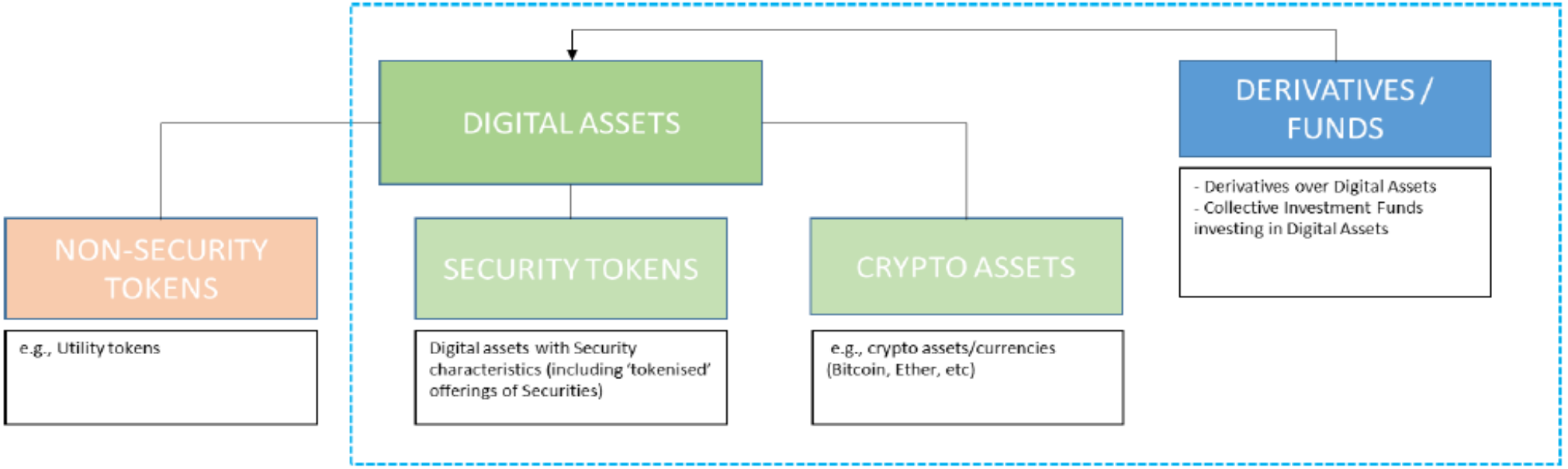


Traditional Currency

- “Fiat Currency” means government issued currency that is designated as legal tender in its country of issuance through government decree, regulation or law.

- “E-money” means a digital representation of Fiat Currency used to electronically transfer value denominated in Fiat Currency.

Taxonomy of Digital Assets



Crypto-Asset/Currency/Token*

- *"Crypto Asset/Currency/ Token" means a digital representation of value that can be digitally traded and functions as*
  - *(1) a medium of exchange; and/or*
  - *(2) a unit of account; and/or*
  - *(3) a store of value, but does not have legal tender status in any jurisdiction.*
- *A Crypto Asset/Token is -*
- *(a) neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Crypto Asset; and (b) distinguished from Fiat Currency and E-money."*

- *Defn: from Abu Dhabi Global Market (ADGM)*

Crypto-Token /currency

- Within the Bitcoin blockchain network, bitcoins are spent to pay for monetary transmission and pay miners or block creators for maintaining the network
- Within the Ethereum blockchain network, Ether (ETH) pays for decentralized computing power and pay miners/block creators for maintaining the network.
- One needs Crypto-exchanges & Crytpo Wallets to ‘cash’ crypto assets (convert to fiat)
- There are over 1000 crypto-currencies available and the list keeps growing

Securitized Tokens

- “Securitized Tokens” are Virtual tokens that have the features and characteristics of *a Security* under the traditional capital market regulations).
- They are a digital representation of a traditional asset (Land title, Shares, Stock, Units in a Collective Investment Fund, etc)
- They are also known as Asset-backed Tokens and are cryptocurrency versions of a traditional asset.

Non-Securitized Tokens

- Also Known as “Utility Tokens” or “Non-Security Tokens”
- These are Virtual tokens that do not exhibit the features and characteristics of a regulated investment (traditional assets).
- Could be comparable to Bonga-points, Supermarket Loyalty Points, Hotel Lunch Voucher or Frequent Flyer Miles.
- They give user access to specific benefits within a particular business network.

The Token economy

ROLE	PURPOSE	FEATURES
RIGHT	Bootstrapping engagement	Product usage, Voting, Governance, Product Access, Contribution, Ownership
VALUE EXCHANGE	Economy creation	Work rewards, Selling something, Buying, Active/Passive work, Spending, Creating a product
TOLL	Skin in the game	Running smart contracts, Security deposit, Usage fees
FUNCTION	Enriching user experience	Joining a network, Connecting with users, Incentive for usage
CURRENCY	Frictionless transactions	Payment unit, Transaction unit
EARNINGS	Distributing benefits	Profit sharing, Benefits sharing, Inflation benefits

Token Opportunities

- Internet of Value: New Models for local and international payments and remittances.
- Mining: Earning rewards for maintaining Blockchain networks
- Banks: Using Blockchain based Funds Transfers (Cryptos pegged on Fiat Currency eg. Ripple Blockchain and/or Stable Coins)
- Central Banks: Exploring CBDC-Central Bank Digital Currencies

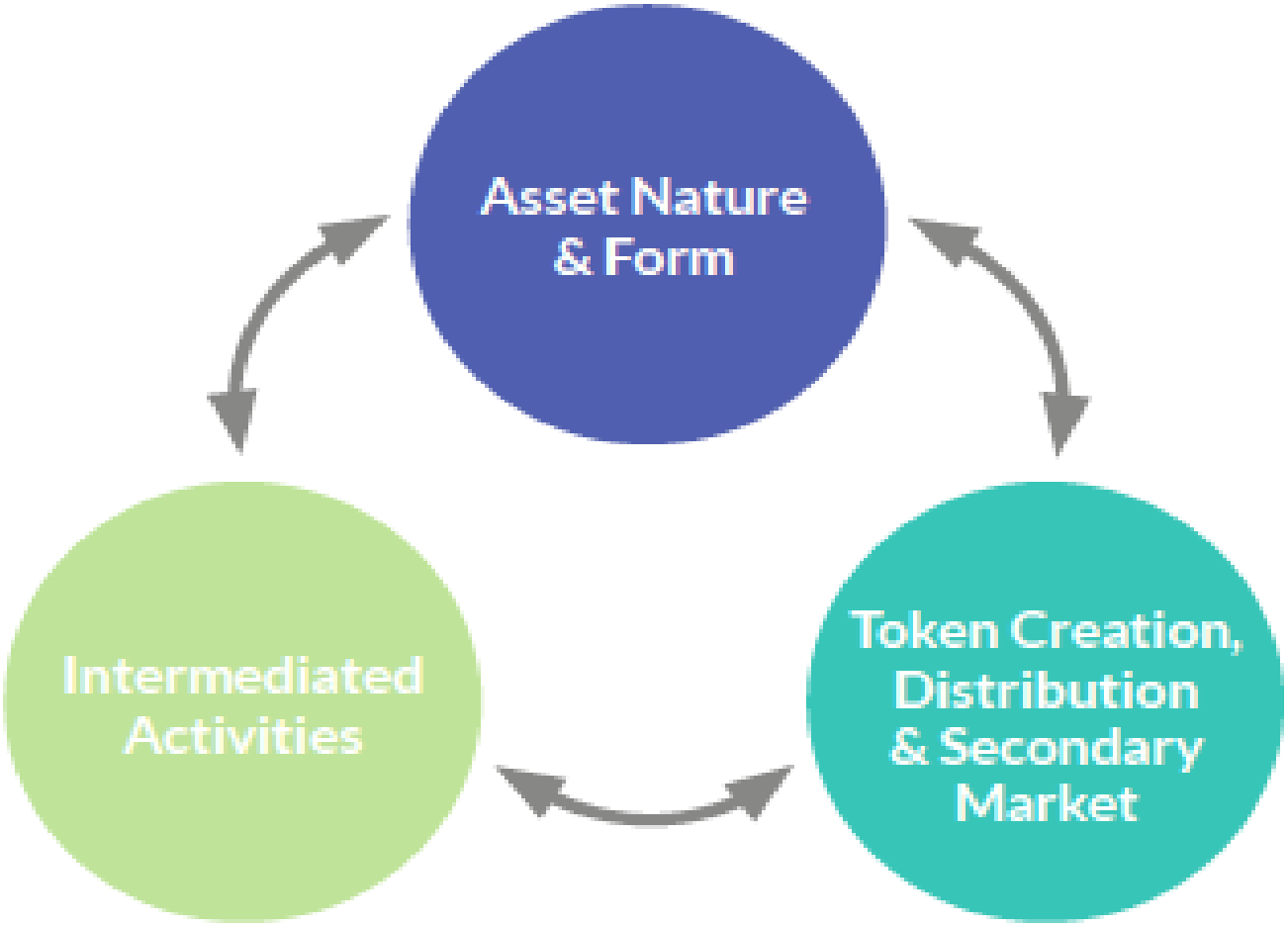
Token Opportunities

- Token-economy: Using tokens to incentivize behavior e.g instead of sending cash to senior citizens, send redeemable tokens to service providers (food, health, etc)
- ICOs- Initial Coin Offerings: new model for raising funds for projects
- STO – Securities Token Offerings: new model for securing digital securities/assets
- Smart Contracts:-new models for executing legal contracts and settling payments without third parties

The Risks/Realities

- Money Laundering/Terrorists can and do use the anonymity attributes.
- Fake Crypto Assets/Currencies, Cyrpto-Exchanges & Cyrpto Projects/ICOs created and gullible citizens conned
- Blockchain Projects demand a huge paradigm shift (centralized vis decentralized) and governance frameworks
- Blockchain based solution requires and puts more responsibility on Users for the safety of

Regulatory Frameworks



Conclusions

- Tokens/Crypto currencies are here to stay
- Progressive Governments are engaging positively to understand the ecosystem
- Best approach is to have ‘Sandbox’ Regulation to host emerging technologies in a controlled environment
- A delicate balance between embracing new technologies and their benefits while safeguarding or protecting consumer interests is required.

State of Play in KE

- Download The KE Blockchain report 2019
- In General
  - Very little activity on using Blockchain as a reliable database to be used for secure record keeping in public sector
  - A lot of activitiy on using Blockchain for crypto currency (payments, remittance, exchange, ICO, etc)

References

- Abu Dhabi Global Markets
- https://www.adgm.com/media/304700/guidance-icos-and-crypto-assets_20180625_v11.pdf
- Satoshi Original White Paper – Peer to Peer electronic cash System
- https://nakamotoinstitute.org/bitcoin/
- Token Economics
- https://medium.com/@wmougayar/tokenomics-a-business-guide-to-token-usage-utility-and-value-b19242053416
- Regulation
- https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf

Ends

- Q&A