Business Application – Acquisition, Development & Implementation
(Chapter - 5 : DISSA Course) **- Cryptocurrency**

Arijit Chakraborty

July 25 , 2021

Coverage- Chapter 5 : Cryptocurrency & IS Audit report

- Crypto-currency
- CC / BTC Exchange – operation
- Purchase / sell transactions
- Crypto -exchange : risks
- International Guidelines / best practices = Audit aspects
- IS Audit – significant observations
- Sample = Complete IS Audit Report
- End of Chapter 5

What Is Cryptocurrency?

- Cryptocurrencies **-** speculation & not real investments.
- No underlying & do not generate any cash flow
- Cryptocurrency **takes the form of digital assets**
- Buyers **use money to buy assets** (or a part of an asset)
- Buyers than **exchange the assets online for goods or services**
- **Ex : a chip at a casino.**
- In a casino, exchange money for chips. Buyer can then use chips to play games.
- **Here :** casino chips = assets,
- games = goods buyer is purchasing.
- **How Does It Work?**
- **Transactions verified using Blockchain- DLT**
- Cryptocurrency miners verify legitimacy of BC transactions by solving complex puzzles.
- First miner to complete a "block" (a.k.a. solve puzzle) verifies transaction & receives a small cryptocurrency reward for their work.

Background

- A 2008 paper by a person or people calling themselves Satoshi Nakamoto first described both blockchain & Bitcoin
- Both terms were used in synonymous manner
- **Bitcoin = software**
- Other participants in BTC market can buy or sell tokens through cryptocurrency exchanges or peer-to-peer.
- BTC has no physical presence,
- Decentralized cryptocurrency produced by entire cryptocurrency system collectively, at a rate defined when system is created & publicly known.
- **Initial coin offerings**
- ICO = controversial means of raising funds for new cryptocurrency venture.
- ICO may be used by startups with intention of avoiding regulation

Cryptocurrencies by market capitalization

Cryptocurrency	Market Capitalization
Bitcoin	$608.6 billion
Ethereum	$240.4 billion
Tether	$61.8 billion
Binance Coin	$48.6 billion
Cardano	$37.6 billion
XRP	$27.4 billion
USD Coin	$26.9 billion
Dogecoin	$24.9 billion
Polkadot	$12.5 billion
Binance USD	$11.5 billion

Data = July 23, 2021.

Cryptocurrency Value drivers

- Like non-fungible token (NFT), cryptocurrency gets its value based on what buyers willing to pay
- **Ex** : fine art or real estate.
- Value of CC = will go up or down based on how much demand
- Ex 1: Housing prices across U.S. fell by 33% during 2008 recession.
- The price of **dogecoin,** a cryptocurrency, dropped by 35% after Elon Musk called it ‘’a hustle’’
- CC to be future currencies require **stability.**
- Recently BTC crossed value of $ 50,000 & in no time fell by $9,000 on comments by Elon Musk that they are overvalued
- Bitcoin rose to $20,000 in December 2017 & fell to $3,200 in a year & by Feb-2021 was trading at record level.
- value = not defined by any fundamentals.
- Volatile

Disadvantages

1. Lack of regulation thus exposing it to illegal use.
2. Value can erode as fast as they rise and there is no stability.
3. High levels of volatility creating financial instability.
4. Not accepted in most countries.
5. RBI = CC trade - harm financial stability & economy. CBDC route
6. Government = CC used to launder money & also be used for terror-funding

Currency ticker used for bitcoin = either BTC or XBT.

Buying BTC

- 1. Buyer need a wallet = an online app that can hold the currency.
- 2. Buyer create - account on CC exchange & transfer real money to buy CC
- Coinbase = such wallet.
- **Bitcoin Exchange**
- **BTC exchange** = digital marketplace where traders can buy & sell BTC using different fiat currencies or altcoins.
- **BTC exchange** = online platform - acts as intermediary between buyers & sellers of CC . i.e between a "maker" and a "taker.“
- BTC exchange works like brokerage, buyer can deposit money via bank transfer, wire,
- Buyer to pay extra price for this service.
- If trader wants to trade between CC, they pay a currency conversion fee
- Traders can opt to buy & sell BTC by inputting either a market order or a limit order

Bitcoin Exchange Operation

- When **market order selected=** trader is authorizing exchange to trade coins for the best available price in online marketplace.
- **Limit order set =** trader directs the exchange to trade coins for a price below current ask or above current bid, depending on whether they are buying or selling.
- To transact in BTC on exchange, user to register with exchange & go through series of verification processes to authenticate identity.
- Once authentication successful, account opened for user who then has to transfer funds into this account before they can buy coins.
- A trader who **like to withdraw money** from the account could do so using = bank transfer, PayPal transfer, cash delivery, bank wire, or credit card transfer.
- **Example of Market order & Limit order**

Movement in cryptocurrency markets

- Cryptocurrency markets move according to supply & demand.
- **Factors**

1. **Supply**: total number of coins & rate at which they are released, destroyed or lost
2. **Market capitalisation**: the value of all the coins in existence and how users perceive this to be developing
3. **Press**: the way CC is portrayed in media and how much coverage it is getting
4. **Integration**: extent to which CC easily integrates into existing infrastructure such as e-commerce payment systems
5. **Key events**: major events -regulatory updates, security breaches & economic setbacks

Cryptocurrency Purchase process

- **Step 1**: Management determines type of cryptocurrency to be purchased.
- **Step 2** : Cryptocurrency wallet downloaded from service provider. Password or passphrase & security measures used to secure wallet against unauthorized access. (https://www.blockchain.com/)
- **Wallet software** = used to generate entity's cryptographic private key.
- **Step 3:** Public key generated using private key & entity's address for each cryptocurrency purchase generated from entity's public key.
- **Step 4 :** Management establishes A/c with cryptocurrency exchange/ broker.
- **Step 5 :** Desired amount of cryptocurrency purchased using entity's cryptocurrency hot wallet.
- **Step 6 :** Transaction authenticated & irreversibly recorded on BC .
- **Transactions** = viewed using BC or block explorer
- 1 Bitcoin equals
- Indian Rupee 24,66,417.73
- 2 Jul, 2021 : 7:00 am UTC

Bitcoin Wallets

- A digital storage service for bitcoin holders to store their coins securely.
- BTC wallets store private keys which are used to authorize transactions & access BTC address of a user.
- Most bitcoin exchanges provide BTC wallets for their users, but charge fee for this service.
- CC can be bought & sold via exchanges = stored in ‘wallets’ .
- CC exist only as a shared digital record of ownership, stored on BC
- When a user wants to send CC units to another user, they send it to that user’s digital wallet.
- The transaction isn’t considered final until it has been verified & added to BC through a process called mining.

Cryptocurrency
(CC) Wallets

- CC transactions involve = use of software program – **CC wallet.**
- **Wallet used:**
- 1. store entity's private & public encryption keys -CC transactions
- 2. interact with one / more BC to send & receive CC
- 3. show entity's balance in each CC - results from various transactions.
- **Hot Wallet**
- "hot wallet" <u>located in device connected to Internet </u>(hosted or entity-controlled).
- Hot wallet required to send CC to another address (e.g., spend CC) & get updated snapshot - entity's CC transactions & balances.
- **Cold Wallet**
- "cold wallet" ("cold-storage wallet") = not connected to Internet

Key Risks – Cryptocurrency (CC) exchange / transactions : IS Audit plan

- 1. Entity chooses to use cryptocurrency exchange **not having effective controls** over transactions it enters into on behalf of entity or
- Weak IC on balances of cryptocurrency maintained in entity's accounts
- 2. Entity has cryptocurrency wallet not been accounted for.
- 3. Entity loses private key & can no longer access related cryptocurrency
- 4. Fraudulent party obtains access to entity's private key, steals entity's CC
- 5. Entity misrepresents ownership of private key & of related CC
- 6. Entity sends CC to incorrect address & CC cannot be recovered.
- 7. Entity enters into & records CC transaction with related party that cannot be identifed due to **anonymity of parties** to BC transactions.
- 8. **Adverse Events / conditions** = difficult to determine value of cryptocurrency recording for financial reporting purposes. (exchange rate)
- 9. **Ensure** : Backup of entity's cryptographic keys, esp : private key, passwords needed to access wallet, are made & safely stored.
- 10. **Ensure** - CC asset & related transactions to comply with IFRS/ Ind AS

Internal Audit of Cryptocurrency (CC) Exchange & transactions

- **IA = to be satisfied** - members of IA engagement team collectively have appropriate competence & capabilities in IT & CC- ensure compliance : with professional standards
- Entity’s FS may include material CC items.
- **Integrity of client**, business purpose for which entity entered into CC transactions
- Whether transactions do not involve money laundering or other illegal acts)
- Client management’s level of understanding of CC risks & IC over CC transactions
- IS Controls related -infrastructure supporting CC – BC hardware & software used in operating a node
- IS Controls implemented by service organization (CC exchange) & complementary controls designed & implemented by Auditee entity
- **Example** - entity’s CC wallet(s) may be hosted by CC exchange / other Service provider (Carry out TOC , walkthrough , SOC 1 & 2 Review)
- Aspects of income tax expense & liability - how tax laws / regulations apply to CC transactions & balances (Ensure sufficient clarity / guidance available)
- .Check - investments in CC, Initial Coin Offer (ICOs) , Initial Token Offer (ITOs)
- Review of FS of entities that: validate CC transactions on BC (i.e., CC miners)

International Best practices & Guidelines- Cryto-exchange Audit

- **1. Client acceptance considerations**
- thorough “know your client” by audit firms prior to engagement acceptance
- **2. Existence**
- When entity uses BC to support occurrence/existence of crypto-asset transactions/balances recorded in its FS , auditors need to evidence their understanding of how transactions are recorded on applicable BC ledger
- IS auditors not to rely on blockchain ledgers ***without*** first evaluating reliability of BC that are relevant for audit
- **3. Use of Experts**
- IS auditors may have to engage blockchain & cryptography specialists to assist in understanding & evaluating BC that support amounts recorded in an entity’s books & records & there is a risk of material misstatement

- An entity’s FS may include material cryptocurrency items.
- **4. Matters to consider**

✓ integrity of the client,

✓ business purpose for which entity is entering into cryptocurrency transactions (e.g., that transactions do not involve money laundering or other illegal acts)

✓ management’s level of understanding of cryptocurrency risks & internal control over cryptocurrency transactions & balances

✓ Whether engagement partner is satisfed that IS Audit team members have appropriate competence & capabilities in ITGC , BC & CC to perform engagement in accordance with professional standards.

- **5. Obtaining an Understanding of Entity’s Information System for Cryptocurrency Transactions**
- **Use ISA 315**
- **Conduct top-down Risk assessment**
- **9 Major risks**

Risk assessment & documentation

- Auditors to identify & document understanding of relevant *risks relating to the occurrence/existence of crypto-assets on BC :*
- *(i) invalid transactions are recorded on the blockchain,*
- *(ii) validated transactions are not recorded on the blockchain,*
- (iii) validated transactions are subsequently modified.
- (iv) Auditors to identify relevant *attributes of BC*

✓ *cryptography,*

✓ *blockchain validation algorithms &*

✓ *consensus mechanisms that mitigate those risks*

- *Auditors :* **perform tests to determine** *whether they are operating as intended.*

Year end balance confirmation

- In testing occurrence of entity's crypto-asset transactions & existence of crypto-asset balance at year end, auditors will use tools = block explorers to review information recorded on BC ledgers.
- Auditors perform procedures to ensure these tools are designed & operating effectively to extract relevant information from BC
- **Ownership rights**
- **Evaluate** = entity's access to private key & control over the related assets.
- In evaluating entity's ownership assertion, auditors = need to design audit approach to obtain sufficient appropriate audit evidence that the entity owns the crypto-assets associated with a public address
- 1. Auditors may request management to transfer a specified amount of a crypto-asset balance between crypto wallets controlled by entity & inspect BC Record for transaction.
- 2. Auditors may ask management to prove they have access to private key that controls a crypto-asset.

ITGC = Review points for IS auditors

- Risk = risk that an entity could share alphanumeric sequence of a private key with others such that multiple entities or individuals could assert ownership rights over same crypto-asset.
- **Entity executes key ceremonies**.
- **Objective of key ceremony control** –

❑ ensure keys are generated in a cryptographically secure manner,

❑ no one could have made unauthorized copies, &

❑ entity is rightful owner of related crypto-assets.

- **Ensure = 1.** Entity implemented **multi-signature access controls** requiring multiple levels of approval before a transaction is executed.
- • **2.** Entity has implemented ITGCs that apply to digital wallets.
- ***Where private keys are held by a 3rd party custodian***
- Crypto-exchanges execute trades on behalf of their clients by retaining custody of private keys that control assets. They act as brokers & custodians for their clients

Revenue from crypto-asset mining

- Blockchain miners receive rewards for creating blocks of validated transactions & including them in BC
- **Auditor of crypto-asset miner** = need to test each of major assertions relating to revenue recognition : occurrence, accuracy, & completeness.
- When entity earns revenue through mining pool, auditor to understand terms of arrangement with mining pool & risks.
- **Impairment of mining assets (IAS 36)**
- Significant decline in crypto-asset prices over past year should be viewed as = indicator that carrying amounts of mining equipment may be impaired & management should be estimating recoverable amount of these assets.
- **Auditors =** be skeptical if management's estimates include unrealistic expectations about future crypto-asset prices & productivity

Related party transactions

- It will be difficult to obtain sufficient appropriate audit evidence when entity does not have effective internal controls to identify related parties & related party crypto-asset transactions.
- **Auditors** = assess business purpose of crypto-asset transactions &
- transactions were made on terms equivalent to those that prevail in arm's length transactions.
- **Subsequent events**
- Significant risks = existence & ownership of crypto-assets
- **So auditors** = perform procedures & obtain sufficient appropriate audit evidence = assets were not lost or compromised during the period between year-end date & date of auditor's report.

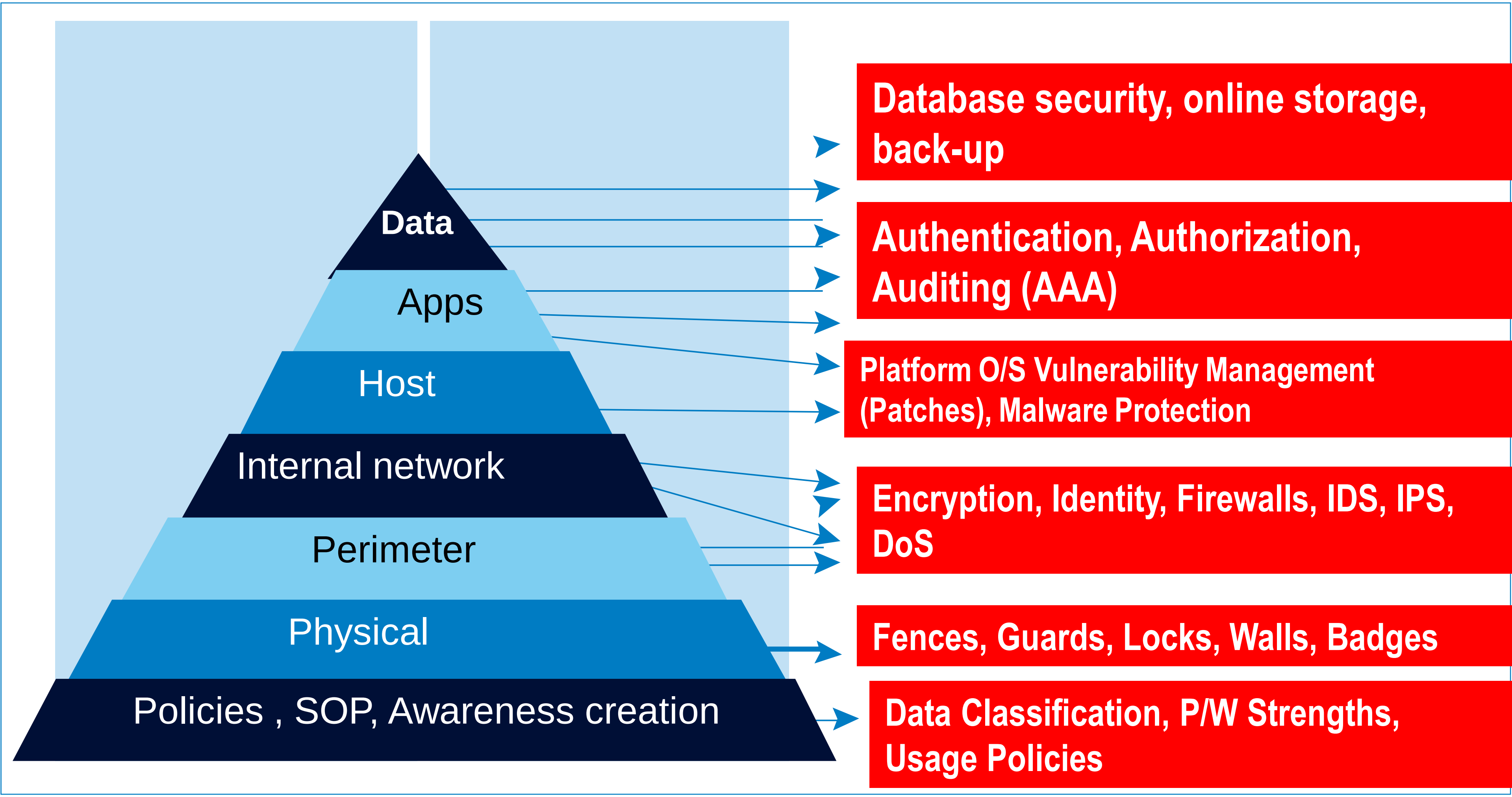
Valuation of crypto-assets- IFRS 13

- For entities that measure crypto-assets at fair value, valuation = assessed as a significant risk by auditors
- In evaluating reasonability of an entity’s crypto-asset valuations, auditors will consider whether an active market exists for crypto-asset (i.e., whether a level 1 valuation can be performed).
- In some cases, several markets for a particular crypto-asset that meet definition of active market, each of those markets might have different prices at the measurement date.
- Here = entity will need to determine principal market (or, in absence of a principal market, most advantageous market) to value asset
- Auditors will need to evaluate whether those prices are reasonable proxies for what an entity will be able to sell crypto-asset in its principal market at measurement date.
- **If no active market** = entity will need to use a valuation technique to value these assets. Auditors may **engage valuation specialists** where crypto-assets do not trade in active markets.

Sch III amendment , FY 21-22

- **Details of Crypto Currency or Virtual Currency**
- Where the Company has traded or invested in Crypto currency or Virtual Currency during the financial year, the following shall be disclosed:-
- a. profit or loss on transactions involving Crypto currency or Virtual Currency
- b. amount of currency held as at the reporting date,
- c. deposits or advances from any person for the purpose of trading or investing in Crypto Currency/ virtual currency.”;
- **NITI Ayog’s PoC of BC – Use Cases**
- 1. ‘Track and trace’ of drugs <u>in pharmaceutical supply chain</u>
- 2. <u>Claim verification & approval in disbursement of fertilizer subsidy</u>
- 3. <u>Verification of university certificates</u>
- 4. Transfer of <u>land records</u>

IT security Model – multi-layered



Database security, online storage, back-up

Authentication, Authorization, Auditing (AAA)

Platform O/S Vulnerability Management (Patches), Malware Protection

Encryption, Identity, Firewalls, IDS, IPS, DoS

Fences, Guards, Locks, Walls, Badges

Data Classification, P/W Strengths, Usage Policies

End of Chapter 5

THANK YOU
EVERYONE