BlockChain, Crypto, IS Audit aspects
(Module - 5 : DISSA Course)

Arijit Chakraborty
March 26, 2022

Guidance on executing IS Audit

1. Defining understanding of business process & IT environment
2. - Refining IS Audit scope & identifying internal controls
3. - Testing Control Design
4. - Testing outcome of control objectives
5. - Collecting audit evidence
6. - Documenting test results
7. - Concluding tests performed
8. - Considering use of audit accelerators- CAAT s, GAS, EWP
9. Considering work of other IS Auditors, Experts
10. Considering review of service providers (SOC)

Overview

- *Blockchain* = shared, immutable ledger that facilitates process of recording transactions & tracking assets in a business network.
- A*sset* = tangible (car, cash, land) or intangible (IPR, patents, copyrights, branding)
- BC network can track orders, payments, accounts, production.
- Members share single view = users see all details of a transaction end-to-end,
- **Features**

✓ *Decentralized*

✓ *Consensus*

✓ *Immutability*

✓ *Hash-Identifier*

✓ *Distributed Ledger*

- **Consensus algorithm**
- No one node or server is responsible for approving transactions, leading to genuinely distributed transaction processing
- Each entry is validated & recorded on all ledgers across network

Blockchain

- Distributed database/ ledger = maintains continuously growing list of data records (public & private) put together in encrypted blocks.
- Distributed Ledger Technology (DLT)
- **Technology creates** = concrete transaction record & transaction integrity.
- distributed transactional database, GL - transactions & details *(date, place, amount, anonymized participants & their encrypted signatures)* recorded & verified through **consensus algorithms**
- Blockchain features—autonomy, decentralization, security and transparency

BC = storage of data

- Usually contains financial transactions;
- Is replicated across several systems in almost real-time;
- Usually exists over a peer-to-peer network;
- Uses cryptography & digital signatures to prove identity, authenticity & enforce read/write access rights;
- Can be **written b**y certain participants;
- Can be **read by** certain participants, or a wider audience;
- Have mechanisms to make it hard to change historical records,
- Make it easy to detect when someone is trying to do so.
- BC technology = backbone of cryptocurrency network Bitcoin
- **Consensus Algorithm= Mechanism**
- When 1 participant wants to send value to another, all other nodes in network communicate with each other using pre-determined mechanism to check that new transaction is valid.

Participants & their roles

- ! **Blockchain user:** Participant (business user) with permissions to join the Blockchain network, conducts transactions with other network participants.
- ! **Regulator:** Blockchain user with special permissions to oversee transactions happening in network. Regulators may be prohibited from conducting transactions.
- ! **Blockchain developer:** Programmers who create applications & smart contracts -enable Blockchain users to conduct transactions on BC network.
- ! **Blockchain network operator:** Individuals - special permissions & authority to define, create, manage, monitor Blockchain network.
- ! **Certificate authority:** Individual who issues & manages different types of certificates required to run a permissioned Blockchain
- **Consensus Algorithm= Mechanism**
- When 1 participant wants to send value to another, all other nodes in network communicate with each other using a pre-determined mechanism to check that new transaction is valid.

Smart Contracts

- Smarts contracts = automated contracts = embedded in the block chain
- self-executing contracts with terms of agreement between buyer & seller directly written into lines of code.
- Code & agreements exist across distributed, decentralized BC network.
- Code controls the execution, transactions are trackable & irreversible.
- Help exchange money, property, shares, Avoids a middle man
- Transactions can be sent with rules attached
- **Benefits**
- Immutable
- Distributed ledger
- Efficient & Reliable
- Lacks single point of failure
- **Consensus Algorithm levels**

BC - types

- **Permissionless Blockchain**
- open to any potential user. Ex- Bitcoin blockchain - public or permissionless blockchain; anyone can participate as a node in the chain by agreeing to relay and validate transactions on the network thereby offering their computer processor as a node.
- Joining blockchain = simple as downloading software & bitcoin ledger from Internet.
- Blockchain maintains list of every transaction performed, reflects full transaction history & account balances of all parties
- **Permissioned Blockchain**
- Participation in BC network to participants who have already been given permission by agreed-upon administrators.
- Example - supply chain network may use blockchain to track movement of goods.

BC – Major Risks

- Misconfigured access permissions, consensus & proof of stake mechanisms leading to transaction trust issues
- Lack of governance mechanisms leading to non compliance of transactions & regulatory penalties
- Concerns = unencrypted personal & confidential information contained in global transactions leading to regulatory concerns
- Challenges in interconnecting different blockchain protocols & data formats creating solution implementation roadblocks
- Challenges in securely maintaining cryptographic keys or weak encryption leading to permanent loss of whole data

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” located in device connected to Internet (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

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

Cryptocurrency Audit

- Provides independent, substantive audit evidence of private key & public address “pairing” = element needed to establish ownership of crypto assets.
- Securely interrogates BC to independently & reliably gather corroborating information about BC transactions & balances

Potential Professional Opportunities

- Blockchain Auditor
- Cryptocurrency Auditor
- Cryptocurrency Project Manager
- Cryptocurrency Consultant
- Blockchain & Cryptocurrency Forensic Examiner
- **Domains for Cryptocurrency Auditors**

✓ Retail, E-commerce

✓ Banks

✓ Telecom

✓ FMCG, Manufacturing

✓ Cross-border payments

✓ Personal identity security

✓ Finance and Insurance

✓ Cryptocurrency exchanges & other Domains

Crypto Audit qualification

- **Certified Cryptocurrency Auditor™ (CCA)**
- **Certified Cryptocurrency Auditor™** = *exclusively developed certification focusing on core concepts of auditing Blockchain-based Cryptocurrencies.*
- Exam-based certification
- Successful completion of certification will enable to perform Blockchain forensics & track exchange-of-hands of Cryptocurrencies.
- Complete understanding of Cryptocurrencies
- In-depth knowledge of Blockchain technology
- Insights on various scams and frauds targeting Cryptocurrencies
- Ability to audit Cryptocurrencies
- Ability to perform Blockchain forensics ,