Business Application – Acquisition, Development & Implementation
(Chapter - 5 : DISSA Course) - Blockchain Part 2

Arijit Chakraborty
July 24 , 2021

Coverage- Chapter 5 : Blockchain – Part 2

- Updates & recent trends- IT
- BC recap
- IS Risks in BC
- **Case studies –**
- 1. Land Records BC
- 2. Certificate verification BC
- Potential professional opportunities & CCA Designation

RBI- Move towards CBDC

- Moving towards : **Central Bank Digital Currency (CBDC)**
- pilot test in process , Deployment phase-wise : Dy Governor, RBI
- CBDC being introduced **in lieu of** private digital assets
  = cryptocurrency
- CBDC ends up on RBI's balance sheet as a currency in circulation.
- RBI : plan to launch the digital asset for general purposes on mass population scale.
- **Proposed changes in legal frameworks:**
- sections 24, 25 and 26 of RBI Act
- Coinage Act of 2011,
- FEMA 1999
- IT Act 2008

RBI Focus

1. Scope = retail or wholesale
2. Technology = DLT or CLT
3. Validation base = token or account based system
4. Distribution = issued by RBI or by banks
5. Enabling legal framework & amendments = RBI Act, FEMA, Coinage Act, IT Act

- **CBDC Benefits**

✓ Reduced dependence on cash

✓ Savings – cost of currency printing

✓ More robust settlement mechanism

✓ Elimination of time zone difference in forex transaction

- **1. Crypto bourses to share trade information with IT Dept**
- IT Notices sent to 3 exchanges- to share ledger entries w.r.t. no of coins, price, time
- Crypto exchange – no trader / broker/ intermediary required
- IT : as Crypto is not security, profits taxed at over 30 %

- **2. ED asks WazirX** to explain why ‘withdrawals’ from crypto-wallets is not FEMA violation
- Crypto – stored in single/ multiple wallets
- Wallets – private or kept with exchanges
- ED = track : inflow & outflow from exchange wallets to other wallets
- Transfers = Rs 2790.74 crores in WazirX ,
- ED= WazirX allowed transfer without documentation, possible money laundering

Pegasus : impact on corporate Cyber Risk management

- Corporate rope IS Auditors & Cyber Forensic
- professionals to create Firewalls , data protection protocol
- **BoD** = concerned if financial data / FS information , PII, Information assets may get leaked , CEO, CFO, CXO = laptops secure ?
- **Case :**
- Indian company handed over 150 special phones to key executives
- Phones = cannot download apps / cannot surf internet
- Call / sms routed through protected server
- **Services in demand**

✓ VAPT, dark web monitoring

✓ Centralised servers

✓ VPN

✓ Diagnostic Reviews of IS Security

✓ Training for employees, presentations to management

Whatsapp CEO – Comment (Pegasus Case)

- *‘’The mobile phone is the primary computer for billions of people More companies and, critically, governments, need to take steps to hold the Israeli surveillance firm NSO Group accountable….*
- *“To those who have proposed weakening end-to-end encryption: deliberately weakening security will have terrifying consequences for us all...This is a wake-up call for security on the internet,”*
- - **Will Cathcart**, Head - WhatsApp

Recap : 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**
- Blocks in chain validated by nodes to maintain single version of truth
- **ISACA-AICPA & CIMA Joint Blockchain Working Group**
- **Key Risks to be identified by IS Auditors**

Blockchain – Risks

- **1. Governance/design risk:**
- Lack of protocols for unconfirmed transactions can allow processing of fraudulent transactions that were previously rejected= network threat
- **2. Infrastructure/protocol management risk:**
- Conditional instructions in protocol or smart contract code can allow infinite loops putting ongoing operation & integrity of network at risk.
- **3. Key ownership & management:**
- Keys for storing & transacting in crypto assets at risk. Keys can be brute forced or guessed= loss of assets.
- **4. Interoperability & integration risk**
- **5. Hetero Regulatory compliance Risk**
- **6. Access risk**
- **7.Application management risk**
- **8. Network & Nodes governance risk**

Approach for IS Auditors

- monitor developments in BC technology because it will impact their clients‘ IT systems.
- should be conversant with basics of BC technology , understanding technical programming language & functions of blockchain.
- work with experts to audit complex technical risks associated with Blockchains.
- be aware of opportunities to leverage their clients' adoption of BC technology to improve data gathering during audit.
- **Auditor of Smart Contracts and Oracles**
- **Smart contracts =** embedded in BC to automate business processes. Contracting parties may want to engage assurance provider to verify:
- smart contracts are implemented with correct business logic

Service Auditor of Consortium Blockchains

- Prior to launching new application on existing BC or leveraging or subscribing to existing BC product, users of system may desire independent
- assurance = stability & robustness of architecture.
- Better than each participant performing their own due diligence
- IS Auditor review = cryptographic key management , ITGCs = protection for sensitive information, processing controls = CIA
- **Arbitration Function**
- For permissioned blockchain, arbitration function needed to settle disputes among consortium-BC participants.
- Participants on BC may require Arbitration = to enforce contract terms where spirit of smart contract departs from a legal document, contractual agreement or letter
- Certifications : BC Council
- **Certified Blockchain Expert / Developed / Architect (CBE, CBD, CBA)**

BC,CC & IoT

IIT Madras

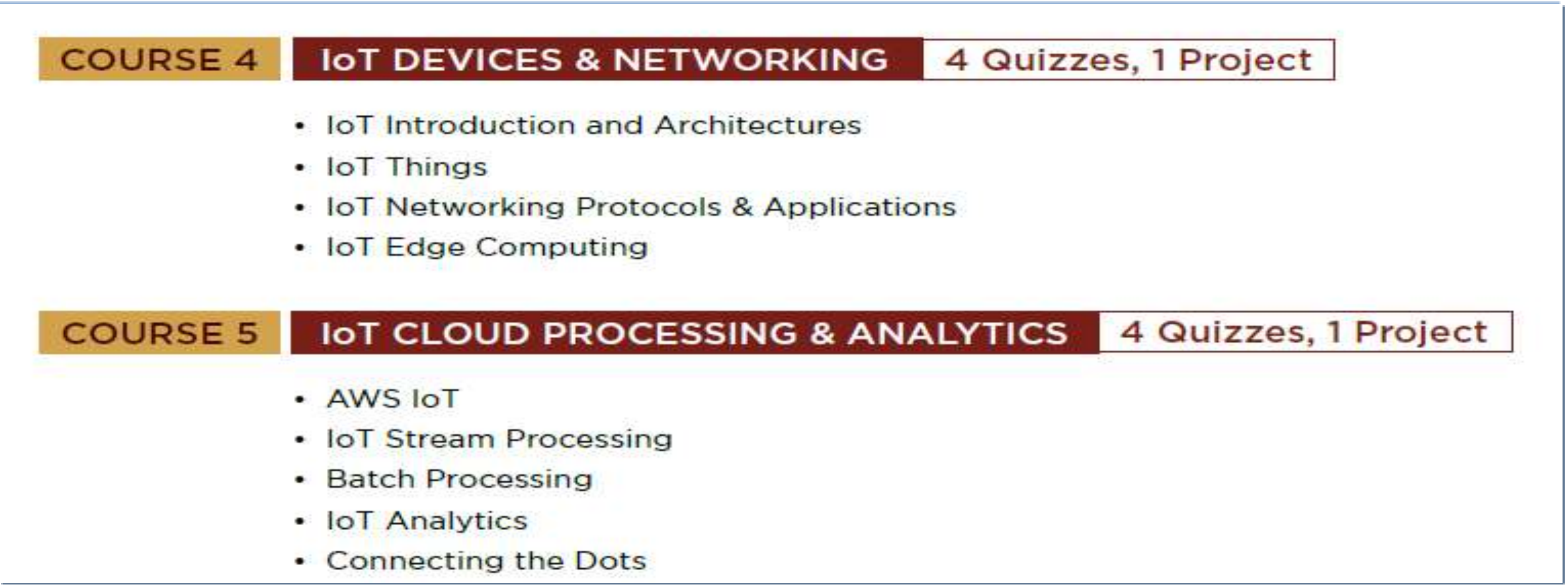
10 Months | Online

ADVANCED CERTIFICATION IN

SOFTWARE ENGINEERING FOR CLOUD, BLOCKCHAIN & IOT

Target participants- IIT Madras

- ***Technology professionals*** *looking to upgrade their skills in cutting-edge technologies*
- ***Mid-career professionals and functional managers*** *handling technology implementation of projects in Cloud Computing, Blockchain and Internet of Things (IoT)*
- ***Recent Computer Science graduates*** *who want to continue learning in the field of technology and prepare themselves for their aspirational roles in technology companies*

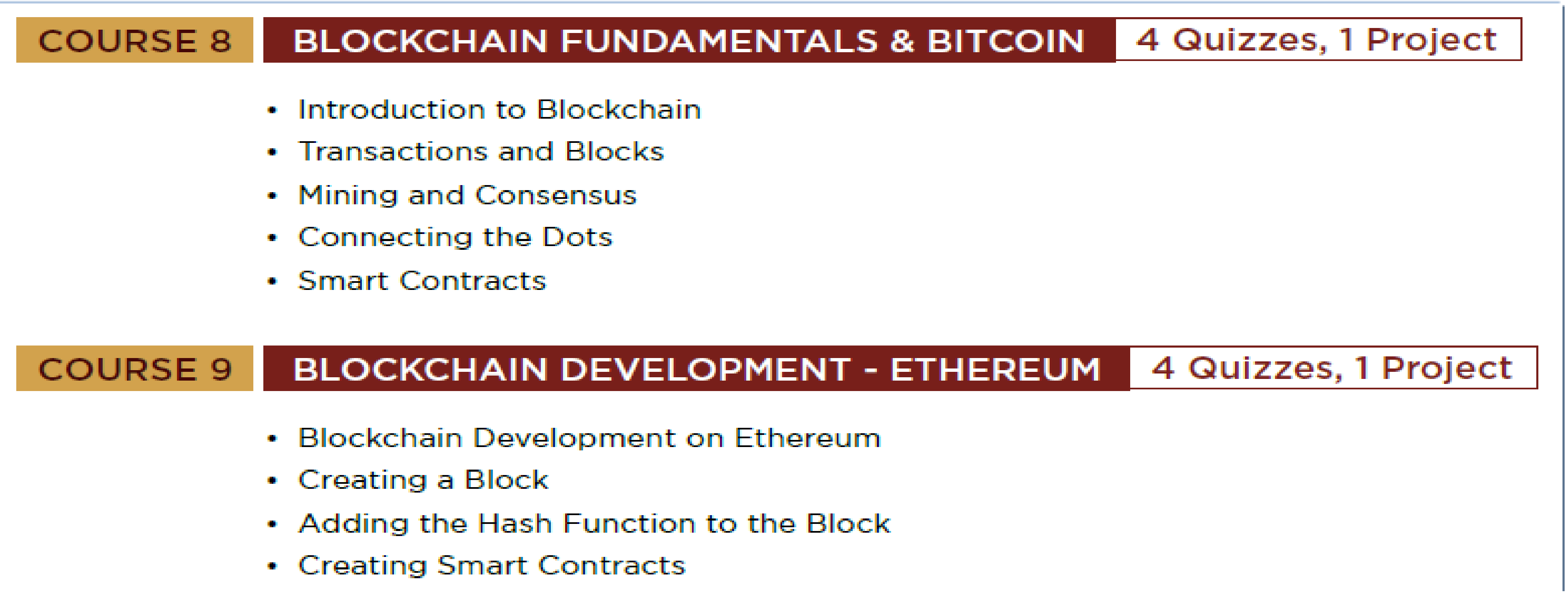


COURSE 4 IoT DEVICES & NETWORKING 4 Quizzes, 1 Project

- IoT Introduction and Architectures
- IoT Things
- IoT Networking Protocols & Applications
- IoT Edge Computing

COURSE 5 IoT CLOUD PROCESSING & ANALYTICS 4 Quizzes, 1 Project

- AWS IoT
- IoT Stream Processing
- Batch Processing
- IoT Analytics
- Connecting the Dots



COURSE 8 BLOCKCHAIN FUNDAMENTALS & BITCOIN 4 Quizzes, 1 Project

- Introduction to Blockchain
- Transactions and Blocks
- Mining and Consensus
- Connecting the Dots
- Smart Contracts

COURSE 9 BLOCKCHAIN DEVELOPMENT - ETHEREUM 4 Quizzes, 1 Project

- Blockchain Development on Ethereum
- Creating a Block
- Adding the Hash Function to the Block
- Creating Smart Contracts

BC –Property ownership

- Move property title records in BC Networks
- Title records – safe & verifiable in BC
- Simple to establish clear chain of legal ownership
- Players = individual transferring title
- Bank managing home-loan process
- **Benefits**
- Cut legal cost= ex: search costs
- Better mortgage management
- End to end transparency

BC – application : Case 1 : Land Records

- Registration = recognized as agreement between 2 parties for transfer of property.
- Constraint = any one of intermediate transactions liable to be challenged as office of sub-registrar(SRO) is only undertaking deed registration under central registration act 1908 & does not verify ownership of land.
- Property fraud = rampant in many forms in our country.
- Land records is under the jurisdiction of state laws.
- Land records system deployed in states facilitate mutation of land.
- **Stored & maintained** = change in ownership of land, cultivators, crop grown, source of irrigation, rights & liabilities
- **Record of Rights (RoR)** = document required for farmers to obtain benefit from Government in the form of subsidy for seeds, fertilizers & other purposes like securing loan, for sale etc.

Process followed

- Registration departments use a software independent of land records system.
- Complete document pertaining to the property to be registered is uploaded along with meta data by citizen.
- It undergoes approval process & at final stage, biometrics of parties is taken.
- Then sale deed document is printed, signature obtained from purchaser & seller
- Uploaded again into system for future issuance of certified copy.

Challenges in current system

1. increase in the number of Land related litigations ,
2. difficulty to track double selling of the same land or landed property ,
3. non-existence of unique record or golden record of ownership,
4. lack of system to facilitate citizens to verify land records,
5. lot of paper work for obtaining loan from banks using land as collateral security,
6. financial institutions do not get factual picture of the piece of land for providing loan as they rely heavily on property for collateral security,
7. delay in obtaining documents from revenue and financial institutions etc.

- Farmer has to spend time and money to collect : : RoR, mutation extract, crop certificate etc necessary for securing loan , subsidy & benefit from Government.
- **Need to ensure** = data in land records system, registration system etc. not susceptible to alteration as **these departments rely totally on integrity of other.**
- **Need for trust** : to use a common source of data to perform approvals for different activities so as to avoid the problem.
- **History shows** : duplicate registration documents generated by tampering original documents & properties sold on basis of tampered documents.

Proposed System

- Land records data need to be accurately stored in BC.
- Existing history of transactions on a piece of land first inserted in BC after approval by Revenue functionaries in the State.
- Approved data will be digitally signed & stored. = starting point for mutation.
- Certificates issued by Revenue Department will be stored in BC & used by other agencies – ex .bank for any of the verification process during a transaction on land parcel / farmer.
- Transactions related to change of ownership through sale, loan, mortgage, release of mortgage, crop updation is initiated by other departments.
- Initiation of such transactions = verification of details using BC data.

- After approval of transaction in respective database : completion of deed registration / approval of loan by bank, transaction details to be stored in BC .
- Registration department will fetch details w.r.t a survey number from BC & ensure ownership of land parcel **indeed rests with the prospective seller** before initiating a sale.
- After obtaining signature of purchaser & seller in sale deed, scanned document should be moved in to BC Network to create a block.
- Once block created it cannot be edited or tampered.
- Chain of block is created every time the property title is changed from one person to another.
- By implementing smart contracts, events - registration of land can automatically initiate mutation request in the land record,
- approval of loan by bank can update rights & liabilities,
- crop details updation can trigger updation of cultivators
- **Smart contracts** = facilitate payment of subsidy to farmers on failure of crops.

Benefits

1. No need for trusted authority - notaries to provide attested copies of docs.
2. Farmers will be assured - land ownership cannot be changed by spurious persons.
3. The farmers can obtain loans quickly
4. Facilities provided to farmer from agriculture / Horticulture / Animal Husbandry department when recorded in BC will facilitate these departments to ensure that same benefit / multiple benefits do not reach the same farmer multiple times or might not receive multiple benefits as per the terms & conditions laid down.
5. BC data of the property registration will be made available in work flow system of the Registration software as well as the public for verification.
6. Will provide complete details of the property chain right from the first purchaser to latest one.
7. Purchaser need not depend on any non-reliable personnel/agency to verify authenticity of document provided by seller.

Certificate verification Current system challenges

- Existing solutions of educational certificates verification have challenges:
- **i. Centralised** i.e. completely dependent on certificate issuing authority
- **ii. Manual** i.e. verification is usually done through emails, phone calls or web forms
- **iii. Time consuming** – could take weeks or months
- **iv. Easy to breach** & tamper
- Hence : **need for decentralised trust** system = verifiable & tamper-proof, is automatic, real-time & fraud-proof.

‘’SuperCert” solution

- permissioned blockchain architecture = decentralization, intelligent identity encryption & identity interlinking for issuance of educational certificates
- i. Creation of student identity – Superidentity. A unique BC representation of the identity is provided, along with a set of public & private keys.
- ii. Issuance of certificate by university, together with Superidentity of student.
- iii. SuperCert i.e. creation of a block of student certificate – hashed version of the certificate on blockchain
- iv. Verification of the certificate using public key of student & public key of university.
- The solutions have features for both online and offline verification
- BC = immutability feature - ensures : tampering of certificate is not feasible – both content of certificate & identity of certificate holder.
- Tamper & fraud resistant
- Scalable to national and global level
- Real-time, automated verification from anywhere in the world.

Steps towards BC Ecosystem

- *1. Regulatory & policy considerations for evolving a vibrant blockchain ecosystem*
- *2. IndiaChain: creation of a national infrastructure for deployment of blockchain solutions with inbuilt fabric, identity platform & incentive platform.*
- *3. India as blockchain hub: promotion of research and development in blockchain,*
- *4. Need to focus on skilling of workforce and students*
- *4. Procurement process for government agencies to adopt blockchain solutions*
- *5. Need for re-evaluating cryptocurrencies.*
- *6. Crypto currencies for India: Does India need a cryptocurrency / ICO / ITO market? (coin, token)*

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

Blockchain Council™

- **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 ,
- **Details** : https://www.blockchain-council.org/certifications/certified-cryptocurrency-auditor/

CCA – Subjects

1. Introduction to Certified Cryptocurrency Auditor™
2. Introduction to the Cryptocurrency
3. Cryptocurrency Trail
4. The Dark Web
5. Cryptocurrency and the Criminal Elements
6. Blockchain Forensics