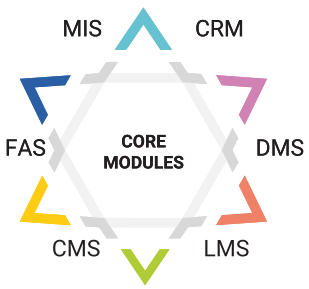
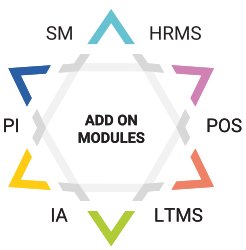
FiNSTA

Best selling FINTECH software for

NBFC (Non Banking Finance), Nidhi, Producer & Mac societies



- Customer Relationship Management
- Document Management System
- Loan Management System
- Collection Management System
- Financial Accounting
- MIS and Analyticals



- Human Resource System
- Point of Sale
- Lead Tracking Management System
- Share Holder
- Internal audit
- Portal Integration

Crafted with 38 years of experience in residuary non banking financial institutions

Unique Features of **FiNSTA**

- ✓ E-KYC
- ✓ Decision / Approval Matrix
- ✓ Risk Analysis, NPA Classification
- ✓ Documentation
- ✓ Collection from Omni channel
- ✓ CIC, CERSAI & Cosmos Reports

FiNSTA software can solve major challenges of lending business

NBFC'S	Nidhi Companies	Producer Companies	MAC Societies
- Vehicle Loans	- Share holder Management	- Member Management	- Member Management
- Gold Loans	- Deposits	- Producer Accounting	- Savings, FD, RD etc.,
- Consumer Loans	- Loans		- Loans
- Term Loans			

Empower and Grow

Flexibility to cater to growing business needs

- Enterprise Intelligence
- Audit and Controls
- Business Process Management
- Data Security and Compliances
- Enlarge Profits
- Intuitive Interface
- Accounts

Why FiNSTA?

Offering a simpler, more effective way to manage every stage of your subscriber

Mobility · Agility · Scalability · Simplicity

Powered by :

techkapil
navigate challenges
www.techkapil.com

Kapil IT Solutions Pvt. Ltd.
Kapil Towers, Financial District, Nanakramguda, Gachibowli, Hyderabad - 32

Talk to us :
9555 763 763
e-mail : sales@techkapil.com

CMMI LEVEL 3

a member of NASSCOM

Blockchain – Concepts and Impact on CA Profession

Technological advances have played a significant role in the world of accounting and auditing. Most CAs will appreciate how this evolution has taken place with the phenomenal impact of computers and its amazing benefits. Today we see that many emerging technologies like Blockchain are going to change the way we do accounting, auditing & assurance, and in this context it is important that our CA profession is well equipped to navigate the future. This article will endeavor to explain the evolution of Blockchain, the basic concepts, distributed ledgers, smart contracts, the technological framework and the impact on accounting, auditing & assurance. Read on…

CA. Babu Jayendran

(The author is a member of the Institute. He can be reached at babujay@gmail.com)

Evolution of Blockchain

In 2008, Satoshi Nakamoto, whose true identity is still unknown, released the whitepaper "*Bitcoin: A Peer to Peer Electronic Cash System*". Blockchain is the underlying technology that runs Bitcoin and has the potential to impact every industry. Therefore, it should be noted that Blockchain to Bitcoin is like Internet to Email.

YEAR	EVENT
1999	The first peer to peer network for sharing music and files was created
2008	Satoshi Nakamoto, whose true identity is still unknown, released the whitepaper Bitcoin: A Peer to Peer Electronic Cash System
2010	First Bitcoin transaction – Purchase of a Pizza
2013	Ethereum was proposed to provide a platform for decentralized applications on Blockchain Technology
2015	Evolution of Smart Contracts
2016	The founding members of the Hyperledger project were announced
2017	Early adoption of Blockchain Technology
2018	Growth, more adoption and gaining maturity

Basic Concepts of Blockchain

There are fundamentally four pillars to understand the Blockchain technology namely, Distributed Ledger, Cryptography, Consensus & Smart Contracts. I will attempt to explain these concepts from a CA's perspective.

Distributed Ledger

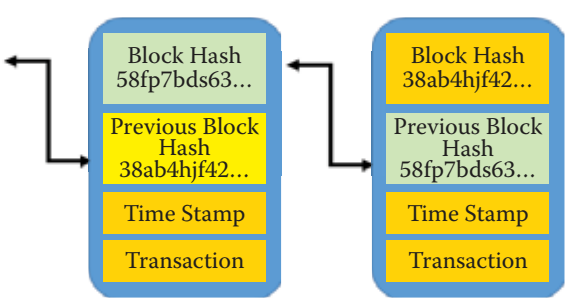
Today organisations account their transactions in ledgers which are maintained by an ERP system or some accounting software, within the centralized premises or on the cloud. It is centralized and not distributed across many nodes.

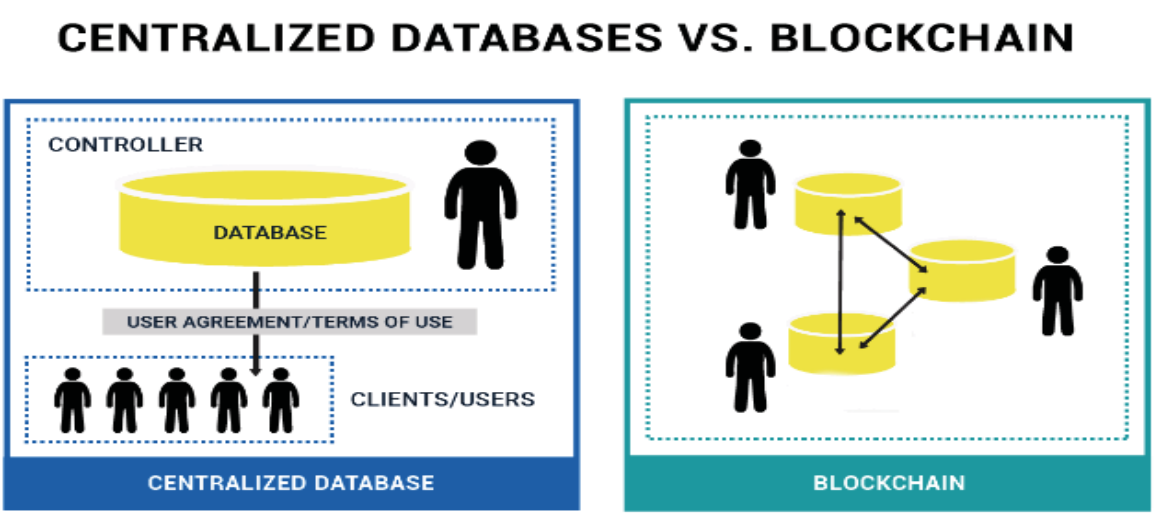
A distributed ledger can be described as a ledger of any transactions or contracts maintained in a decentralized form across different locations and people, eliminating the need of a central authority to keep a check against manipulation. Every participant in the network has simultaneous access to a view of the information.

Centralised vs Blockchain

Cryptography

Integrity and security of the information on the Blockchain are ensured with cryptographic functions. Each block contains a validated pointer to the previous block. This 'chains' each block to the previous one. This ensures that the transaction, once validated, and written to a block is immutable. If any attempt is made to change a transaction it will not be accepted because there will a mismatch of the block hash with the previous block hash.





Consensus

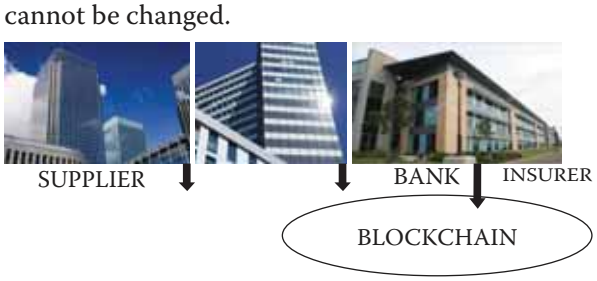
For a transaction to be accepted and validated in the Blockchain there must be consensus amongst the participants of the Blockchain. A simple analogy would be a card game with 4 participants (A, B, C & D) wherein, we have 2 options for keeping score, one person (A) will keep the score or each of the participants will maintain the score. In the first case if A modifies the score in his favour it may go unnoticed by other participants. In the second case, if A modifies the score it will not be in agreement with the score maintained by B, C & D and therefore the erroneous or fraudulent act will be exposed. There are a few consensus mechanisms like Proof of Work, Proof of Stake etc. but we will not go into the technical details in this article.

Smart Contract

This is a business logic that can be assigned to transactions. A contract between parties is written as code in the Blockchain and based on a triggering event, the contract executes itself according to coded terms. For example, we could have a situation wherein a supplier invoice pays for itself provided the goods have been received in good condition, quantity and price is as per the Purchase Order and there is sufficient bank balance.

Benefits of Blockchain

In today's world, each entity maintains its own books of accounts and thereby its own "version of truth". This leads to an un-ending task of reconciliations of inter or intra company accounts. As accountants we all know what a painful task this is! Also persons with fraudulent intent can, by hacking, change transactions posted in a database. This is an inefficient, expensive and a vulnerable way to perform accounting tasks. With Blockchain all shared business processes are written to a distributed ledger and the data, once written, cannot be changed.



There is only a "single version of truth" since all participants of shared processes see the same information. The benefit is that the painful task of reconciliations does not arise. A good example to highlight this point, is the current GST Network in India. Although, it is not created on the Blockchain technology, the concept of a "single version of truth" is applicable since the sales figures once uploaded to GSTN is automatically downloaded to the buyer to confirm its correctness. From an accounting perspective, we started with single entry accounting, moved to double entry and will now enter the era of triple entry accounting! The benefits of Blockchain can be summarized as follows:

Commissioned : View information on a "Need to Know" basis

Consensus : People involved in the transaction should be able to approve it

Provenance : Knowing the history of the asset – Where it came from & went

Immutability : Once transaction is recorded it cannot be changed

Finality : To ensure that transaction occurred and has not changed

Trust : Single version of truth

The Technological Frameworks

The following major platforms/frameworks are available today for implementing Blockchain solutions:

Hyperledger	Supported by Linux Foundation, IBM, Intel, Cisco, JP Morgan, Wells Fargo, SAP, Accenture.... etc.
Ethereum	Open source public distributed platform featuring smart contract functionality
R3 Corda	Specifically designed for the BFSI sector with over 80 participating banks

Multichain	A software tool for web asset and legal contracts on Blockchain, allows its customers to control whether the chain is private or public, how big the block is, and who can connect to the network.

When evaluating which platform should be used it is important to consider the following:

- Consensus — Algorithms are parameterised and can be customized
- Smart Contract — The functionality to create smart contracts is available
- Security — The data and transactions are well protected
- Scalability — Can handle large volumes of transactions without degradation
- Support — Technical support is easily available
- Documentation — Detailed documentation is available with tutorials
- Accessibility — Access through GUI is available
- Open Source — Should not be dependent on a specific vendor
- Language — Programming language should not be specific to a platform
- Deployment — Should be easy to install and use

Blockchain Components

Assets	Anything of value that can be transacted tangible (cars, house etc.) or intangible (intellectual property)
Participants	Actors in the business network who need to share transaction information
Transactions	Describe what can be done to the assets as they move around the business network (buy, sell…etc.)
Node Application	Each Internet-connected computer needs to install and run a computer application specific to the ecosystem they wish to participate in. E.g. For Bitcoin, each computer must be running the Bitcoin wallet application
Distributed Ledger	A data structure managed inside the node application. Once you have the node application running, you can view the respective ledger (or blockchain) contents for that ecosystem.
Consensus	The algorithm implemented as part of the node application, providing the 'rules of the game' for transaction validation

Impact on Accounting, Auditing & Assurance

In order to understand the impact on Accounting, Auditing & Assurance, I give below a "Proof of Concept" in the area of Mortgages. Let us look at this simple scenario.

PROCESS	ACTIVITIES
Mortgage Request	• Property is listed on blockchain by seller • Buyer and seller are verified by the lender and invited to participate
Offer Negotiation	• Buyer makes an offer for the property • Buyer & Seller negotiate and agree on final price • Valuation check • Lender offers mortgage terms to buyer
Due Diligence	• Lender verifies title, valuation, buyer credit ratings • Seller's time line for handover • Lender makes payment to Seller's bank
Title Transfer	• Title registration storage • Title hypothecation with bank if required • EMI payments from buyer to lender

In this case, the participants are Buyer, Seller, Lender, Bank, Valuer, Property Registry.

Sample Audit steps

Based on this simple Mortgage Management Blockchain implementation scenario, let us now look at a few risks and establish some of the audit steps required for assurance.

- **Valid Participants**
  - Participants within a Blockchain implementation, need to accurately represent the various actors within the business network who share business processes.
  - e.g. Lender, Bank, Buyer, Seller, Valuer etc.
- **Valid Assets**
  - Assets need to accurately represent entities within the business network
  - e.g. Title, Property, Loan Contract, Sale Offer, Sale Contract, etc.
- **Valid Transactions**
  - Transactions within the implementation, need to replicate transactions that actually happen within the business network
  - For the purposes of data integrity Assets should ideally never be edited or deleted; Assets should only be created or transferred through another transaction
  - e.g. List Property, Make Loan Offer, Transfer Title, Purchase, Sale etc.
  - Within a smart contract, ideally all transactions should never edit existing assets; they should either create or transfer ownership. If a transaction edits an asset or a participant, it needs to be clearly documented, so that the scenario can be validated. Also, an edit transaction should ideally ensure that all people related to that asset/participant are clearly notified of the change, and approve of the same. Change to an asset or participant, without the related parties' prior approval can lead to dangerous consequences.
- **Valid Smart Contract Code**
  - The actual enforcement of rules within the related Smart Contract code need to be carefully audited and inspected to ensure there are no backdoors or loopholes that can possibly be exploited in the future by a bad actor, familiar with those backdoors.
  - The logic/code within the Smart Contracts needs to accurately represent the identified assets, participants and transactions for the application platform and the selected business network. It is best to walk through the entire smart contract code, with the developer, after a thorough solo independent review.
- **Malicious Conditional Checks:**
  - Transfer Money (while balance > 0)
    - The money transfer transaction should not be based only on the event that a bank balance is available. For example, let's assume that if there's a money transfer transaction that has to happen within a coded smart contract once certain items have been received in good condition and the price is right. If this money transfer transaction was coded to get triggered on that same event, but instead of executing and transferring the invoice amount of the goods to the vendor, the transaction is maliciously coded, to keep transferring money to a disgruntled employee's bank account, as long as the smart contract bank account balance is greater than 0. A dangerously coded transaction such as this, if not caught in an audit, prior to deployment, could potentially empty the bank account attached to the smart contract, while making the disgruntled employee very rich, overnight.
  - Auto Accept Any Loan Offer
    - This ideally should not happen. Acceptance of any offer or agreement, should happen after some level of review, and should only be done by the concerned participant; e.g. The Banker should not be allowed to accept a loan offer on behalf of the buyer.
- **Hard-coded Value:**
  - Variable "Money Receipient Bank Account" = <fixed_bank_account_number>
    - Bank account numbers should be dynamic and not fixed within smart contract code; hard-coded values are bad developer practices, and are also easy ways to introduce malicious backdoors into smart contracts.
    - A disgruntled developer can hard-code his bank account number into the smart contract code, so that a fraction of every money transfer transaction that occurs gets transferred into his account as well. The difference in money amounts would be negligible, but would definitely add up to a large sum over time, especially if there are thousands of transactions happening within a busy system.

- **Undocumented Methods/Transactions:**
  - Every single transaction/method within the code of a smart contract needs to be thoroughly documented, so as to not miss a malicious transaction buried within the code, with no trace within the official documentation, possibly performing malicious actions in the background, without anyone's knowledge.
- **Use of Version Control systems to manage code effectively:**
  - Every single change made to Smart Contract code needs to pass through layers of peer/leadership review, prior to being deployed in production, so that no malicious code can be deployed without anyone's prior approval, and code changes can be easily traced back to developers.

Conclusion

Blockchain is a technology designed to focus on capturing transactions of participants, across shared processes of a business network thereby providing a "single version of truth". Due to the fact that it uses Distributed Ledger Technology (DLT) to record transactions across many computers, the transactions cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. As a consequence of this, it provides a good audit trail for both the participants and the auditors. Peer-to-Peer networking coupled with a distributed time-stamping server, is the core to its architecture. Transactions are authenticated through a consensus from all participants, who have vested interests in the business network. The immutability of data/transactions gives a higher level of comfort to the participants and auditors, provided the edit functionality is properly audited.

For Chartered Accountants, it brings a number of opportunities. CAs have the expert knowledge of business processes which can be used to identify the shared processes, in business networks, which can be architected into a Blockchain solution, with the help of technologists. At the outset, modeling of the solution should be done in order to identify the Assets, Participants, Transactions, and Events etc. CAs should review the model to ensure that the business network is properly defined and the information is accessed on a "Need to Know" basis. The potential for Blockchain solutions can be extended to Banks, Manufacturing, Insurance, Retail, Ecommerce, Real Estate, Healthcare and many other industries. If solutions can be created to avoid reconciliations, a lot of time of accountants can be utilised for more productive work. A "single version of truth" should prevail in a business network. However, it must be noted that to leverage the domain knowledge, CAs must take the plunge into Blockchain technology, reskill themselves and above all "think out of the box". Accounting, Audit & Assurance services are drastically going to change in the years to come and if CAs want continued bright future, they must learn to navigate the future world of technology. ■

O peace! how many wars were waged in thy name. - *Alexander Pope*