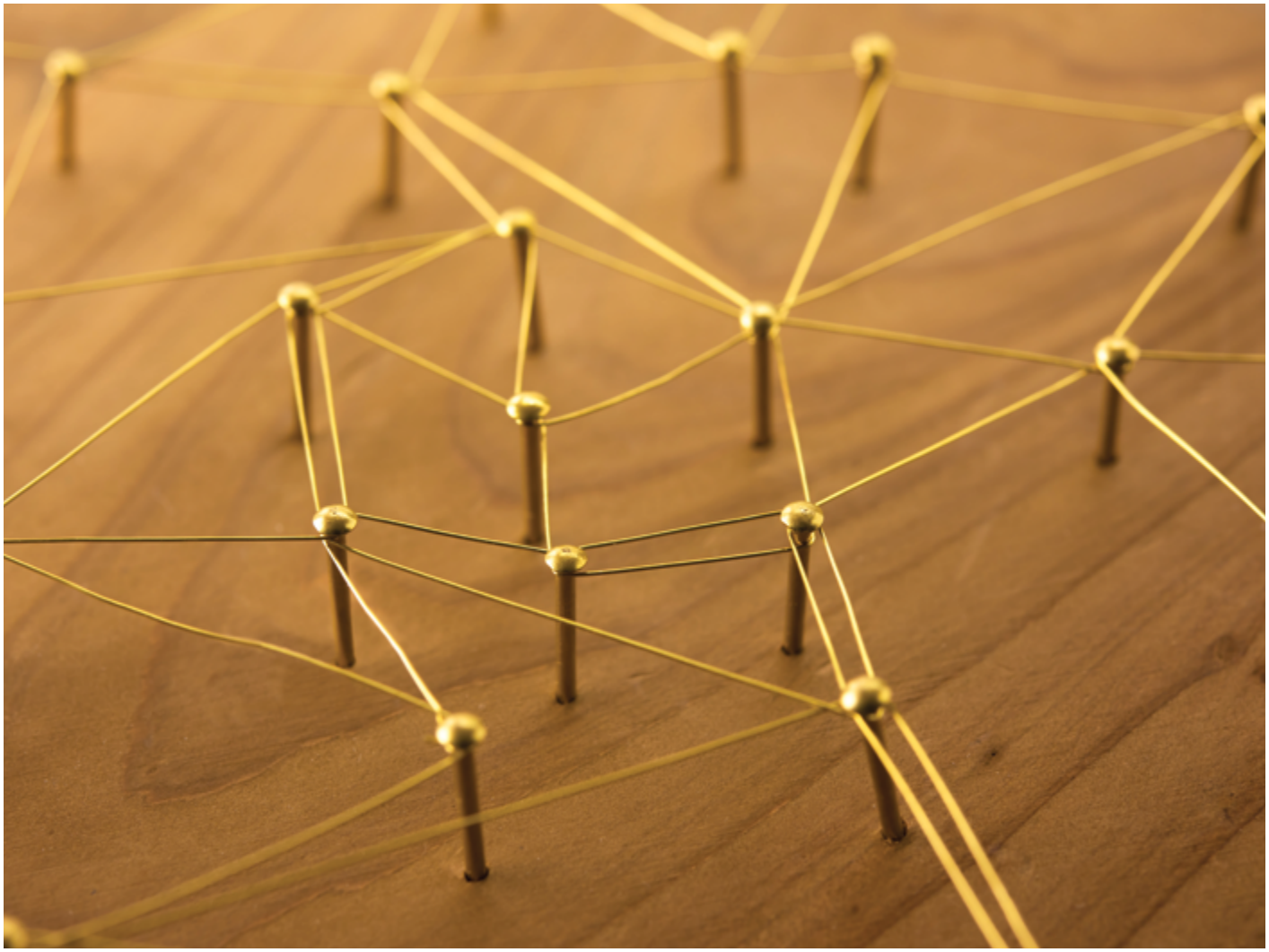
POINT OF VIEW

UNLEASHING THE TRUE POTENTIAL OF BLOCKCHAIN

Infosys® | Finacle



Introduction

A billion $ in VC investments between 2012 to Jan 2016 – half of which came in the year 2015 alone! The Crypto currency theme has certainly been a VC magnet in recent times. As the technology goes through it due 'Hype' cycle, the focus has now squarely shifted from Bitcoin to the underlying Block chain technology.

One of the key trends currently, is the move towards distributed systems. The amount of computing power being added every year worldwide leads one to believe that the future will indeed belong to distributed systems. Bitcoin's blockchain combined several existing techniques to create a unique 'distributed system' capable of handling 'value transfer' securely in a trustless environment.

The technology behind the bitcoin in simple terms is both a network and a database that enforces trust between disparate entities using a set of old techniques combined in a new way. Key techniques used include secure peer-to-peer communication, transactions grouped into blocks, advanced cryptography, distributed multi-party consensus algorithm and multiversion concurrency control

At the core of the technology is a 'Shared Distributed Ledger' that enables participants to have a single view of the ledger without necessarily needing a central intermediary. Further, the technology's ability to allow 'Shared write Access' and arrive at a consensus on the 'true copy' of the data – is revolutionary.

There are various approaches to distributed ledgers, each with advantages and disadvantages (Vitalik Buterin, 2015):

1. Fully public systems

These are decentralized ledgers open to all Internet users. Anyone can read, submit transactions, and participate in the verification and validation of transactions. The block chains in these systems are secured by a combination of economic incentives and cryptographic verification,

using Mechanisms such as proof of work or proof of stake. Participants are typically known only by pseudonyms; and the issuance of an embedded currency provides incentives for participants to verify transactions and maintain the block chain. Examples include, Bitcoin, Ethereum, and other crypto currencies.

2. Fully private systems

Permissions in these systems are assigned by a central entity. Applications include database management and auditing internal to a single company. A private system does not need an embedded currency given that the central entity can assign computers to verify transactions.

3. Hybrid or consortium systems

Here, the consensus validation process is controlled by pre-selected individuals or organizations, such as a consortium of financial institutions, or the customers of a company. The right to read the associated blockchain may be public or restricted to the participants. These systems are considered partially decentralized. Whether these systems need an embedded currency to provide incentives would depend on the degree of trust, which in turn would depend on the degree of decentralization.

Blockchain for banking

Private permissioned systems

While the bitcoin and ethereum public systems continue to thrive, there is now a growing interest in the banking world about the 'private, permissioned ledger'. Private Blockchains enable industry applications by combining new components (with existing components from the public block chains) to better fit use cases.While they might borrow secure peer-to-peer communication, transaction grouping into blocks and cryptographic techniques from bitcoin or ethereum they might choose to change other components. For example, banks can select a more relevant consensus algorithm.

Indeed, the relevance of 'mining' expending huge amounts of CPU power becomes largely irrelevant in permissioned networks. Instead of a competitive mining race, permissioned chains can rely on a list of permitted miners .This, along with a relevant distributed consensus algorithm can prevent groups of miners from controlling the private network. As incentives in a permissioned network are not financial (rather just the privilege of participating) and consensus does not rely on expensive mining, the costs of running a permissioned Blockchain are significantly lower.

The technology has a lot of potential, however one needs to be realistic about capabilities and aware of shortcomings to avoid its application in suboptimal ways.

Applications of Blockchain

The benefits of adopting this technology in banking are multi-fold. Following are some of the applications of this technology.

1. Optimized clearing and settlement

Shared distributed Ledgers can enable faster clearing and settlement cycles. Financial institutions conventionally use a messaging system (such as SWIFT), a money wiring mechanism such as RTGS and also a central clearing entity that is trusted by participants to affect an asset transfer. The network and database nature of Blockchain can possibly reduce dependence on all of these processes and systems, significantly compressing time for clearing and settlement.

Once a trans¬action is recorded on the ledger, the corresponding asset transfer is also reflected in the ledger copy of the beneficiary. Optimized processing using blockchain can lower costs, reduce counterparty settlement risk and bring down fraud. While existing settlement processes allow for netting and margining, these could be supported through 'enabling surround systems'.

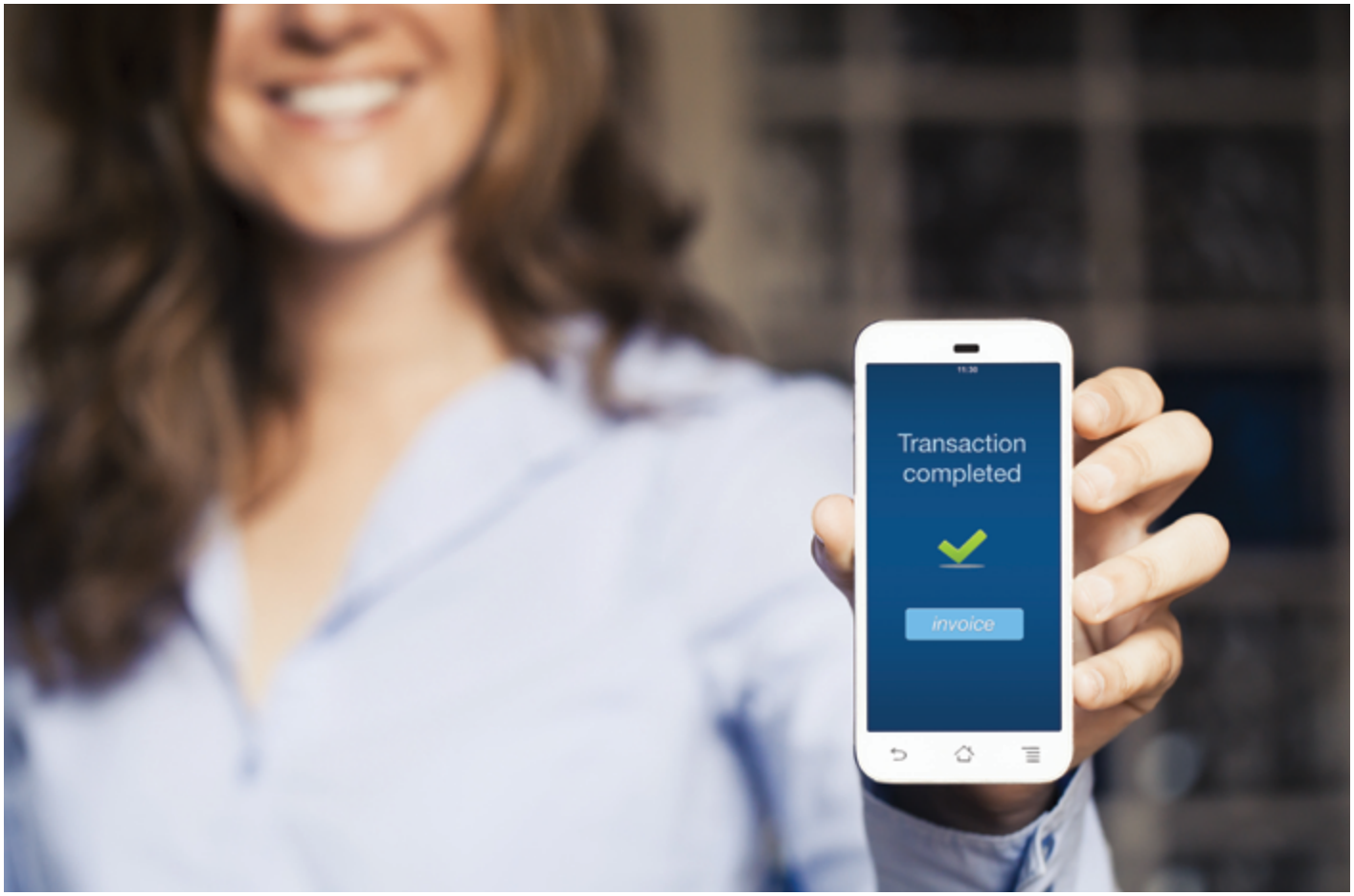
Some of the tell-tale benefits of adopting blockchain for clearing and settlement include:

- **Eliminating multiple bilateral accounts**

  Participating banks save on 'liquidity cost' as they have to maintain only one account that is capable of transacting

Blockchain Features

- A cryptographic transaction network and data store combined into one
- Ability to arrive at consensus on veracity of transactions in a distributed shared write environment
- An immutable database where transactions once created cannot be reversed or modified
- Shared, exactly replicated across multiple entities leading to high fault tolerance
- Asset agnostic with applicability to any type of asset
- Multi-sign enabled transactions supported out of the box enabling multiple levels of approval for a transaction to go through
- Ability to encode processes into 'Smart Contracts' that can be automatically enforced in case specific conditions occur



with all other banks as against Nostro Vostro accounts with each bank

- **Anytime operations**
  Unlike centralized clearing systems, blockchain enabled clearing can provide continuous clearing and netting with near real-time settlement. These systems need not have restricted hours of operation and can provide 24/7/365 services
- **Higher visibility & traceability**
  Participants and even regulators can have greater visibility into the system higher traceability and integrity audit trails
- **Reduced risk**
  Distributed ledgers can provide a near real time record of obligations leading to better risk management
- **Avoid reconciliation**
  As systems reflect a near real time 'net position', the need for maintaining multiple levels of ledgers and reconciling them can be eliminated

2. Secure, tamper-free storage of documents

Financial transactions typically involve exchange of documents and terms of the exchange. Blockchain can serve as a means through which these documents can be exchanged with a non-repudiable immutable audit trail linked to securely stored documents.

E.g. A bank could choose to share KYC information with other banks in the same market. The 'cost of customer acquisition' comes down for the 'acquiring bank', while the bank sharing the information is able to monetize the data. This also in theory leads to an industry level repository of KYC information that can further be used for AML , blacklisting checks etc. leading to higher order prospects of monetizing data .

Banks being the best source of KYC, could share data with other sectors requiring KYC information such as say the telecom sector.

3. Process automation

Smart Contracts can serve as a useful vehicles to automate business processes especially those that transcend organizational boundaries. Smart Contracts in simple terms represent an 'if-then-else' condition i.e. if a certain event happens, do something mentioned in the contract – automatically. Uses cases around

Forward Contracts, Escrow facilities, Bank Guarantees and OTC derivatives represent significant opportunities.

4. Ledger and process consolidation

Institutions with multiple legal entities can consolidate data from multiple traditional ledgers into a single data backbone which can lead to better regulatory compliance at potentially lower costs. In this model, the private blockchain can serve as the central data repository providing a consolidated view of global operations. E.g. for processes such as KYC, there is potential to share KYC documents between IT departments through the blockchain. This can prevent duplicate spends for processing documents for the same end customer.

5. Transparent audit

By design, block chains contain an immutable history of asset movements. This provides great transparency for internal audit purposes and also for regulatory reporting and compliance.

This feature could in theory be used for scenarios such as issuing, cataloging and trading shares of privately-held companies, opening up new business lines for firms.

6. Reduction in systemic and operational risk

As accounts need to be pre-funded before carrying out transactions, Blockchains can potentially eliminate credit and liquidity risk.

Further, the technology enables 'secure' digitization of business processes in the inter–entity space. This includes several processes in the Trade Finance area where banks can leverage the technology to bring down costs across the lifecycle in addition to reducing operational risk. For example, it is possible to leverage the technology to reduce risk around duplicate invoice financing– the reduction in systemic capital risks arising from duplicate invoices between lenders in a market creates a more conducive trading environment which in turn encourages more trading activities using invoice financing. Other use cases include implementing a digitized settlement process for a letter of credit, automating escrow facilities and bank guarantees.

7. Operational improvements in the middle and back office

Blockchain technology has the potential to optimize and possibly eliminate a number of middle- and back-office processes through better standardization of instruments and process .These include processes around trade enrichment, error correction, allocations and counterparty matching

One size fits all?

While the technology has several benefits, can one ledger fit all use cases? While this piece is evolving, it appears that 'Purpose built ledgers' are the answer in the interim simply because different groups and vendors have picked up different pain points to solve. This is also accentuated by financial institutions partnering with technology firms to mould plain vanilla shared distributed ledgers into something that works in their business environment

- Ripple is working in the payments and remittances space. It is also developing protocols which can enable different types of ledgers to talk to each other.
- Digital Asset Holdings is focused on providing purpose-built block¬chains to market participants, with solutions aimed at specific asset classes.
- NASDAQ's Linq platform enables issuing, cataloging and trading of shares of privately-held companies on the NASDAQ Private Market.
- R3 is working with large global market participants in an effort to establish common standards governing blockchain design and deployment.
- BuyCo.io is developing a collaborative procurement platform that leverages blockchain and smart contracts to lower costs of money transmission for buyers.

Deployment models

If we ignore advanced cryptography, block chains do not conceal the content of transactions among participants. This is because, in order to be able to confirm a transaction, the nodes have to be able to see it. Conventional databases have fundamentally different model to access control enforcing who can see what.

Blockchains thus can be considered as shared databases in which all participants are able to see what other participants are doing.

This limitation can be overcome to an extent by some form of cryptography on additional transaction data (such as documents etc.).

Also, the other point to note is, deployment models can be leveraged to make blockchain technology work in specific contexts.i.e instead of a monolithic global blockchain, other deployment models could be explored.

1. Bilateral Blockchains

Implementing a 'visible to all' blockchain can be detrimental in competitive financial markets where participants must not know what others are doing (say a trading scenario) .In such cases, a bilateral blockchain could be explored. The usage of blockchain technology can ensure secure exchange of information that is auditable and transparent to both parties.

2. 'Multi-party system' blockchains

In a situation where participants need to share information with each other, multi-party system blockchains can be explored. This deployment model fits a 'co-operation' paradigm.

3. 'Public to all' blockchains

This type of deployment can be sub-categorized into 2 sub-types viz.

a. All Information on the blockchain is visible to all participants. This is typically good for audit type of scenarios such as ones where contract information needs to be recorded so that it can be enforced .Simple applications such recording an exchange of emails between 2 participants in an auditable fashion over the blockchain can lead to greater transparency and trust (the sender and the receiver of the email cannot deny the correspondence as the information has been committed to an 'immutable' blockchain.)

b. All information on the blockchain is visible to all participants in the network as well as the external world. This type of implementation could be applicable for public notarization type scenarios. E.g. Land /property records, collateral information etc.

4. 'Need to know basis' blockchains

In this deployment model , information such as KYC documents can be encrypted and stored on the blockchain using the sending node's (Say Node A) private key. In case the documents/information need to be shared with another entity (Node B) it can be enabled in a manner that only Node B is able to view.

5. Blockchain on demand

It is possible that the need for corresponding between 2 banking entities is infrequent (say once a quarter) or project based. In this situation, the participants can possibly access a blockchain on demand. I.e. correspond for the duration of the project, archive the data and close down the blockchain after use.

Impact on existing investments

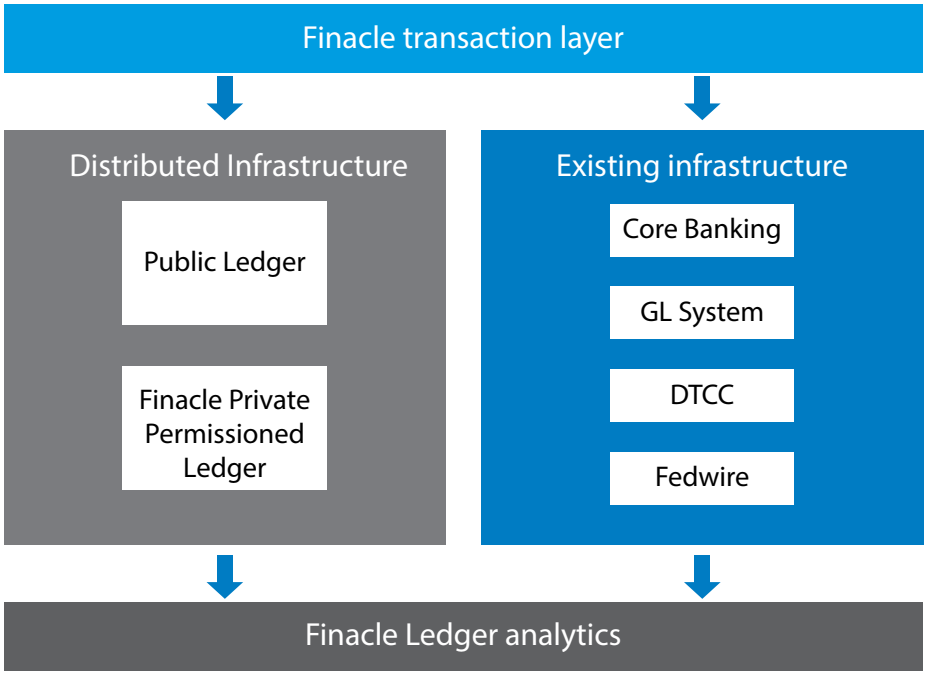
Financial systems work on closed networks with a hierarchy of ledgers:

1. Core Banking Ledger
2. Enterprise-level ledger,
3. Interbank bank ledger (at the central bank).

Blockchain is not meant to replace all of these. Investments by banks in some of the traditional ledger technologies will remain relevant in the blockchain world and Shared ledgers will co-exist and offer interoperability connectors with traditional ledgers.

Following are some principles that can serve as a guide for blockchain transactions:-

- Construct transactions that provide privacy & when required, permit net settlement.
- Instead of replacing existing infrastructure , augment with distributed ledger features
- Commit transaction to traditional and/ or distributed systems
- Assume assets are not issued solely into distributed networks
- Ensure inter-operability of transactions across ledgers.
- Built in Ledger Analytics that can straddle across Traditional as well as Distributed Ledger Systems.



Additionally, integration APIs with Core banking systems can leverage well established protocols such as ISO 8583 which ensure integration with any core banking ledger.

Regulatory opportunity

While regulation might seem like a nightmare, the technology represents a great opportunity for central regulators to gain unparalleled transparency into the financial system at a relatively low cost. Indeed forward thinking regulators such as the Bank of England are now considering Distributed Ledger technology as they re-imagine their RTGS system. The Reserve Bank of India also has recently taken cognizance of the potential of the technology in the context of transforming

the functioning of the back office of banks, increasing the speed and cost efficiency in payment systems and trade finance.

The race to production

Blockchain based systems can transform the financial services world and save billions of dollars in costs infrastructure costs alone.

Firms starting off on the blockchain journey, should begin with a test bed environment to get a first-hand experience of the technology .This can help contextualize the technology to use cases that are most relevant to the firm.

Large financial institutions have already identified 10-20 use cases for technology and business potential evaluation. Top uses being pursued include those in areas of Payments, remittances, Trade Finance, Post Trade Processing, Repurchase agreements, debt distribution and insurance processing.

Initiatives are largely at the POC phase, with pilot projects validating how solutions leveraging Blockchain can replicate or complement existing infrastructure.

However, 2016 will be the year when things move from POC to Production. Indeed a 'race to production' is now underway. We are now at the cusp of an exciting journey, where organizations can leverage blockchain to establish market position and leadership through break-away business models.

As it goes "You don't build a network – You Grow it!" Is your firm ready to take the plunge?

References

1. Mckinsey - Beyond the hype: Blockchains in capital markets
2. DTCC –Embracing Disruption – Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape,
3. Reserve Bank - https://tldrify.com/dpm
4. Bank Of England - http://www.bankingtech.com/428402/bank-of-england-considering-digital-ledger-for-rtgs-in-2017/
5. Vitalik Buterin - On Public and Private Blockchains

Author

Pramod Krishna Kamath
Finacle Product Strategy
EdgeVerve Systems Limited
Pramod_kamath01@edgeverve.com

Pramod is part of Finacle Product Strategy team and comes with an Industry experience of close to 16 years . He has worked in various roles at Finacle including Finacle Engineering and Architecture .

In his present role he looks into areas of Technology Strategy and Innovation initiatives and is currently driving the Blockchain initiative at Finacle.

He holds an MBA from IIM-Calcutta and a bachelor's degree in electronics engineering from Mumbai University.

About Infosys Finacle

Finacle is the industry-leading universal banking solution from EdgeVerve Systems, a wholly owned subsidiary of Infosys. The solution helps financial institutions develop deeper connections with stakeholders, power continuous innovation and accelerate growth in the digital world. Today, Finacle is the choice of banks across 84 countries and serves over 547 million customers – nearly 16.5 percent of the world's adult banked population.

Finacle solutions address the core banking, e-banking, mobile banking, CRM, payments, treasury, origination, liquidity management, Islamic banking, wealth management, and analytics needs of financial institutions worldwide. Assessment of the top 1000 world banks reveals that banks powered by Finacle enjoy 50 percent higher returns on assets, 30 percent higher returns on capital, and 8.1 percent points lesser costs to income than others.

Infosys® | Finacle

For more information, contact finacle@edgeverve.com

www.finacle.com