WHITE PAPER

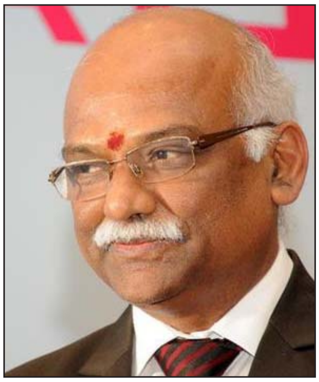
APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

TO BANKING AND FINANCIAL SECTOR IN INDIA

IDRBT
Explore, Enable, Excel

Institute for Development and Research in Banking Technology
(Established by Reserve Bank of India)

CONTENTS



FOREWORD

TECHNOLOGY and banking have a long close association. Both have been benefitting immensely by this association. Innovations, which are by definition leveraging technology in unusual ways, have great potential to be disturbing the standard ways in which systems are operated. However, in that process we do gain, nevertheless it is not uncommon that these innovations do inflict pain on the society. Therefore, a careful analysis of the pros and cons, a thoughtful ring-fencing of risks, closer study on pilot basis before scaling up, fine-tuning based on feedback, etc., are required before we adopt such innovations.

During recent years, banking industry across the globe is closely observing the developments in one such disruptive innovation viz., the blockchain technology (BCT). BCT provides tamper-evident recording of the linked transaction history in a distributed network, and has the potential to disrupt the financial business applications. Sound theoretical underpinnings of BCT such as fault-tolerant distributed computing and consensus have been studied for the past two decades. The nature of BCT addresses risks and inefficiencies in multi-party systems, and that is where its benefits will be most widely received. Applications of BCT for encoding economic signals have been in vogue for the past decade and the claims that it may be useful for digitizing currency are being studied.

Smart-contracts are an advanced application of BCT that can encode complex business workflows for enforcing their conformance, and enhances efficiency through event triggered mechanisms. Several BCT platforms provide the necessary features to encode smart-contracts in a simple and efficient manner.

IDRBT has taken the initiative of exploring the applicability of BCT to the Indian Banking and Financial Industry by conducting a workshop involving all the stakeholders such as the academicians, bankers, regulators and technology partners. In the process, the participants of the workshop came together to bring out this White Paper detailing the technology, concerns, global experiences and possible areas of adoption in the financial sector in India. The Institute has also attempted a Proof-of-Concept (PoC) on the applicability of BCT to a trade finance application with active participation of NPCI, banks and solution provider, the details of which are presented in the White Paper.

I congratulate IDRBT for the timely initiative and trust that the White Paper provides the necessary impetus towards accelerating the adoption of this innovative technology. All members of the Working Group deserve compliments for their inputs and efforts.

R. Gandhi
Deputy Governor, Reserve Bank of India
Chairman, IDRBT

Date: January 05, 2017
Place: Hyderabad

PREFACE

IT is almost two years since a small team of researchers at IDRBT has been studying the structure, security features, process flows and use cases of Blockchain Technology (BCT), especially in the area of banking and finance. In the process, the Institute has been interacting individually with academicians, organizations, banks and technology partners working in the area.

In order to bring all of them together, the Institute organized a brainstorming workshop on Blockchain technology. All the participants of the workshop showed interest and keenness to work jointly to prepare a White Paper on Implementation of BCT in the areas of banking and finance in India. Accordingly, the Institute formed a Working Group with experts from RBI, IBA, NPCI, CCIL, ISI, State Bank of India, Punjab National Bank, Bank of Baroda, ICICI Bank, HDFC Bank, Axis Bank, Citi Bank, Deutsche Bank, Infosys, TCS, IBM Research, Deloitte and MonetaGo as members.

All the members of the Working Group have given inputs from their expertise and experience. The IDRBT coordinating team put together the inputs along with their study results into five chapters.

The first chapter introduces the cryptographic components, protocols and ledger classifications of blockchains. While the second chapter provides the advantages of BCT, the third chapter presents the potential areas of its application, both in currency and non-currency areas. The fourth chapter critically examines the crucial features required in banking and financial sectors – security, privacy, traceability and scalability.

Drawing from the strength of analysis presented in the first four chapters and the global experiences, the Working Group proposes a prospective roadmap for adoption of BCT in Indian banking and finance in the fifth chapter.

In order to gain first-hand experience of the implementation, the Institute organized a Proof-of-Concept (PoC) of BCT for a typical trade finance application with active participation of NPCI, banks and the technology partner. The results of the PoC have been quite encouraging, giving comfort and confidence in the implementability of BCT.

It is a rewarding moment to the Institute and the Working Group to present the White Paper to all stakeholders in the country for further course of action. I am personally happy to get the White Paper, with a foreword from our Chairman, Shri R Gandhi, Deputy Governor, Reserve Bank of India, released by Dr. Duvvuri Subbarao, Former Governor, Reserve Bank of India, during the inauguration of the International Conference on Distributed Computing and Networking (ICDCN) today.

Dr. A. S. Ramasastri
Director, IDRBT

Date: January 05, 2017
Place: Hyderabad

Chapter 1

Introduction to Blockchain Technology

BLOCKCHAIN, a seemingly unassuming data structure, and a suite of related protocols, have recently taken the worlds of Finance and Technology by storm through its groundbreaking application in the modern crypto-currency Bitcoin, and more so because of the disruptive innovations it promises. While Bitcoin has been the most talked about application of the Blockchain technology to date, new applications such as Smart Contracts have tried to exploit more abstract nature of the platform. In this White Paper, we explore Blockchain similarly – as an abstract data structure and development platform to solve generic problems in FinTech.

Cryptographic Components

Blockchain Technology relies heavily on fundamental tools from Cryptology and Data Security, especially in terms of message authentication targeted towards tamper-evidence and tamper-resilience. In its most abstract form, a Blockchain may be described as a tamper-evident ledger shared within a network of entities, where the ledger holds a record of transactions between the entities. To achieve tamper-evidence in the ledger, Blockchain exploits cryptographic hash functions.

Cryptographic Hash Function

A generic hash function maps arbitrary size inputs or messages to fixed size hash values or tags. In order to justify the authenticity of a message through its tag, a cryptographic hash function tries to ensure pseudo one-wayness, that is, the practical infeasibility of generating the input message given the tag, and pseudo collision resistance, that is, the practical infeasibility of generating two input messages that produce the same hash value or tag. Due to these two properties of cryptographic hash functions, it is probabilistically ensured that if a message is inadvertently exposed to errors, or has been intentionally tampered with, its hash value will not match with the original tag, and thus, the tampering will be evident. In fact, for minor differences in the input message, the tag generated by a cryptographic hash function is supposed to exhibit major (random) difference. This allows us to utilize hash functions for creating tamper evident structures.

Hash Pointer

A pivotal construct in blockchain technology is the hash pointer – a combination of a regular pointer structure with the hash value of the data fragment it points to. This produces an inbuilt data integrity mechanism, as storing the hash pointer simultaneously guarantees the location evidence of the data (through the regular pointer) as well as the tamper evidence of the same (through the hash value). In other words, storing the hash pointer to any piece of data acts as a commitment towards the location as well as the integrity of the specific data fragment. The hash pointer is flexible enough to replace the regular pointer in any acyclic pointer-based linked data structure, and hence is capable of producing a variety of data structures with inbuilt data integrity and tamper evidence. An example of such a tamper-evident data structure is the Blockchain.

Blockchain: Tamper-evident Linked-List

Let us consider a linked-list, with the regular pointers linking the nodes replaced by hash pointers – this is precisely what a blockchain data structure looks like. Each block in the blockchain acts as a node in the list (or chain), holding some amount of data, and a hash pointer pointing to the previous block on the chain. The first block in the chain is called the genesis block, and this is the only one that does not have to contain a hash pointer.

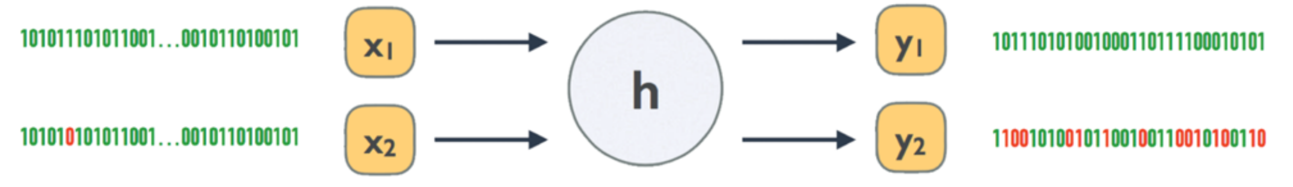


Figure 1. Minor input difference leads to major output difference

It is important to note that if any block in the blockchain incurs an inadvertent error or is tampered with, the block containing the hash pointer of the erroneous block will not match anymore. Thus, any inadvertent error may be traced in a blockchain. If the tampering is intentional, the adversary is forced to fix the hash pointer in all of the blocks following the tampered block, in order to validate the complete blockchain. However, if someone holds the last block of the blockchain as a commitment value, it will be easy to prove any such attempt at tampering, anywhere within the blockchain. Thus, we have a tamper-evident data structure in the form of this blockchain, which allows a constant size commitment. In case, a network of entities tracks the last block of the blockchain, simultaneously, we automatically have a completely decentralized platform to store the commitment and hence a decentralized network to ensure tamper-evidence of the blockchain.

One may extend the chain quite easily; by creating a new block containing the hash pointer to the last existing block in the chain, which in turn appends the newly created block to the existing chain. However, one may not insert a new block in between two existing blocks in the chain as easily. That would require changing an internal hash pointer, which leads to changing all subsequent hash pointers, and hence, all the subsequent blocks in the blockchain. Exactly the same holds for deletion of a block from within the blockchain. Technically, if there are n blocks in the blockchain, insertion and deletion in the chain are O(n) processes, whereas appending is O(1), that is, a constant time process.

In case a decentralized network stores the blockchain in parallel, insertion and deletion becomes impossible as changing O(n) blocks in the chain by a single entity in the network, without involving other members of the network, is not feasible. Note that appending to the chain is fine, and potentially every entity in the network is capable of appending a new block to the existing last block of the chain. This action of appending a block does not require involvement of all entities in the network. It is sufficient, for consistency of records, that the appended block is broadcast in the network so that every entity may update their copy of the blockchain, especially the copy of the last block, which acts as the commitment. This specific property of blockchain proves to be instrumental in constructing a tamper-evident decentralized ledger of records over a network.

Merkle Tree: Tamper-evident Binary Tree

Similar to the blockchain, one may construct a binary tree, replacing the regular pointers by hash pointers, to obtain a Merkle Tree. In a Merkle tree, the leaf nodes contain the data blocks, and the intermediate nodes contain the cumulative hash pointers to the respective subtrees, in a hierarchical fashion. The hash pointer to the root node of the Merkle Tree (top hash) acts as a constant size commitment for the whole tree, similar to the case of blockchains.

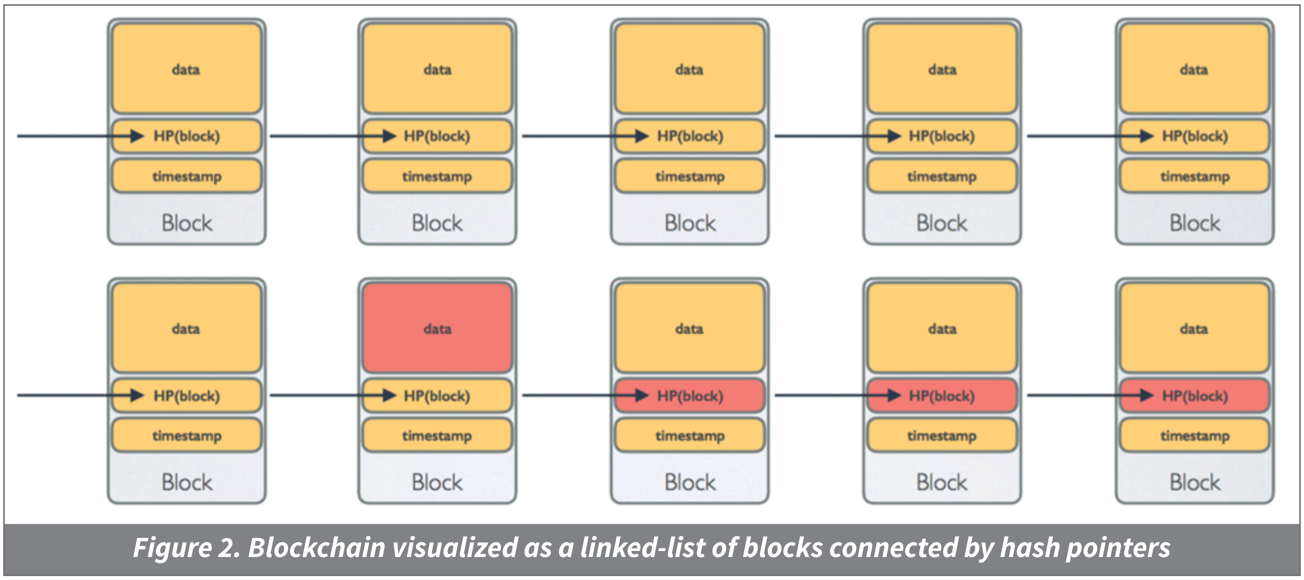


Figure 2. Blockchain visualized as a linked-list of blocks connected by hash pointers

However, contrary to the case of the blockchains, it is possible to both insert and append a node from the Merkle Tree with O(log n) operations, where n is the total number of nodes (data blocks) in the tree, as appending a data block requires an alteration of only the shortest path from the leaf node to the root.

If any inadvertent error or malicious tampering causes the data in any of the nodes of the tree to change, it will be evident to everyone holding the hash pointer to the root node. In case of a network, the hash pointer to the root node may be stored as a commitment in a distributed fashion, with every entity, and in such a case, the Merkle Tree will act as a decentralized tamper-evident storage for data.

It is interesting to note that appending to the tree is exactly the same as inserting a node, and thus, this non-linear structure acts as a generic set, rather than a list. In addition, Merkle Trees allow an O(log n) proof-of-membership for any leaf node, which may be used for consistency or audit proofs in the set of data blocks. To prove the membership of any leaf node in a Merkle Tree, one needs to produce only an O(log n) size proof, in the form of the sibling hash pointers along the shortest path from the leaf node to the root of the tree. Similar proofs may be provided to verify that a collection of data blocks is a certain subset of another.

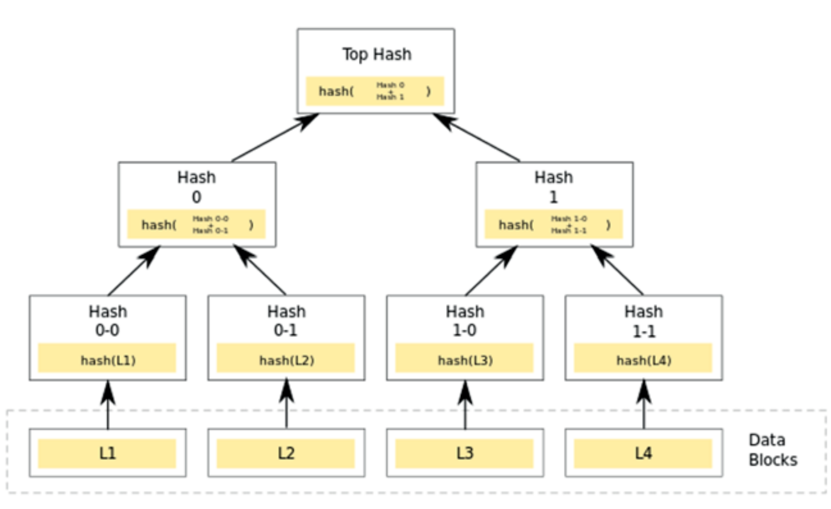


Figure 3. Merkle Tree as a binary tree connected by hash pointers (Source: Wikipedia)

Patricia Tree: Tamper-evident Trie

In addition to the blockchain (linked-list based on hash pointers) and the Merkle Tree (binary tree based on hash pointers), another practical authenticated data structure is the Patricia Tree or the Merkle Trie, which is a modified form of the Trie data structure based on hash pointers, instead of the regular pointers. In case of a Patricia Tree or a Merkle Trie, the collection of data blocks is stored in a (key, value) format, where the maximum length of the key values controls the depth of the tree. Thus, in a Patricia Tree, operations like insertion, appending, proof of membership etc., become O(k), while the commitment remains O(1). This data structure is used in the modern smart contract platform – Ethereum.

Blockchain Protocol

The driving force behind the recent fame and success of blockchain technology is the wide range and flexibility of protocols that can be realized using the basic data structures defined in the previous section. To understand the blockchain protocols, we need to define some essential functional components, as follows:

Network

The blockchain protocol, in its most generality, establishes a consensus over a decentralized network of members involved in the respective protocol. The members participating in the protocol may have various roles and actions in managing the authenticated data structure, as specified in the protocol. Such roles and actions may depend upon a pre-specified access control mechanism, or a set of permissions, as and when applicable, to make the protocol fully flexible. Consequently, the structure of the blockchain network may be peer-to-peer (flat) or hierarchical, as and when required by the respective protocol.

Transactions

A mutual contract struck between any set of entities in the blockchain network is generally termed as a transaction. Owing to the historical origin of blockchain technology from Bitcoin, any such contract is called a 'transaction'. However, in its most generality, a transaction can be a complex multi-party contract encoded as a Boolean logic, implemented in the form of an executable script. These generic blockchain transactions are also called Smart Contracts. The transactions are the fundamental atomic components of a blockchain protocol, and the other structures in the protocol are built on top of transactions. One may in fact view a blockchain platform as a tamper-evident distributed ledger of transactions.

Ledger

A collection of transactions in a blockchain network is generally stored in the form of a Merkle Tree, to ensure tamper-evidence of the set of transactions using a constant size commitment (hash pointer to the root of the tree). Each such set of transactions, recorded as a Merkle Tree, is included in the data segment of a block, and these blocks are stored chronologically (as per their time-stamps) in a blockchain ledger, that is, in the form of a tamper-evident linked-list, as shown in figure 4.

Verification

Blockchain is inherently meant to be a decentralized ledger of transactions. Thus, each transaction or contract between two (or more) members in the network requires verification or validation by the network itself, without going through an independent arbitrator. This is achieved by incorporating a verification scheme in the protocol. In practical blockchain schemes, this verification scheme is often implemented as a part of the transaction in the form of an executable script, which results in either acceptance or rejection of the specific transaction.

In certain practical applications of blockchain technology, the verification routine also connects the current transaction to previously existing transactions in the blockchain, which have been verified earlier as inputs. These connections have been depicted by the dotted lines in Figure 4. Depending on the application, the verification scheme may be designed in such a way that the transactions admit to public verification, or it may be entirely permissioned.

Consensus

The transactions are grouped together in a Merkle Tree, and the block containing this tree is recorded in the blockchain ledger. It is to be noted that in a distributed network, the task of creating a block and appending it to the ledger should also be natively decentralized. The blockchain technology is flexible enough to accommodate a suitable form of decentralized appending process, known as mining in general.

Irrespective of the exact mining process that updates the blockchain ledger, it is imperative to ensure that the ledger is universally accepted across the network at any given point of time. This warrants for a consensus scheme in the protocol. This decentralized consensus mechanism ensures a consistent version of the blockchain ledger amongst all members of the network, and provides the most important tamper-detection and tamper-resilience property to the blockchain. In fact, if any member introduces an inconsistency in the ledger through the mining process, the other members have the

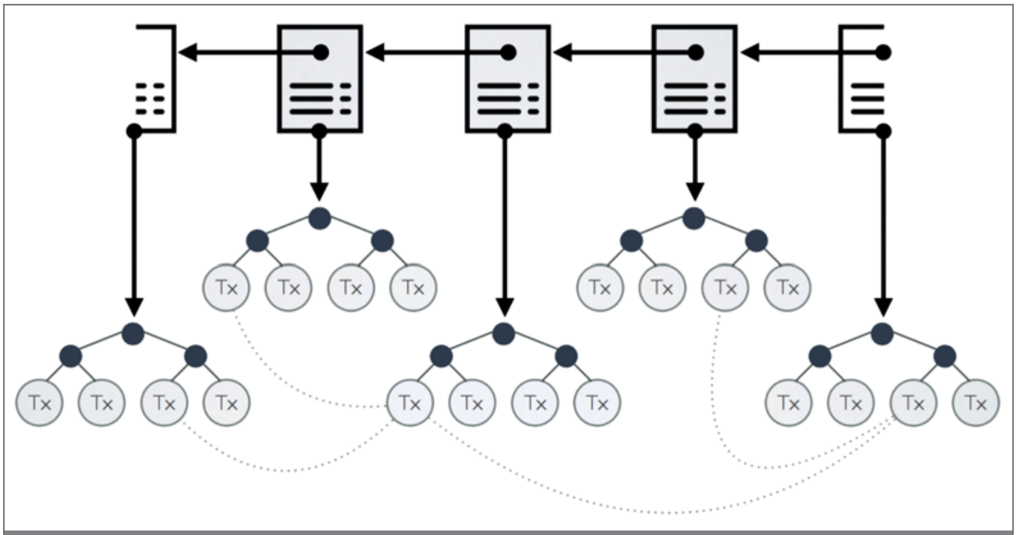


Figure 4. Blockchain architecture as a ledger of transactions

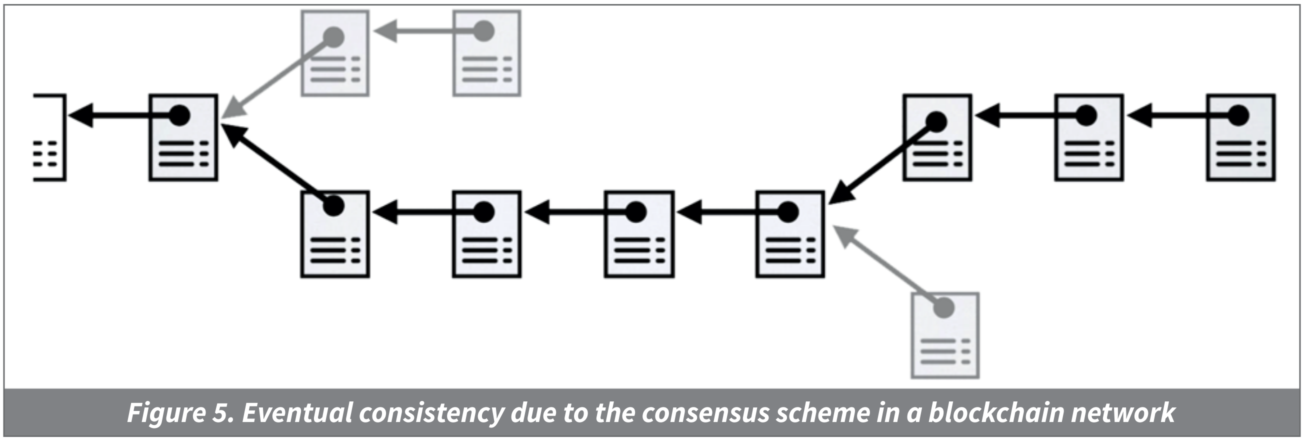


Figure 5. Eventual consistency due to the consensus scheme in a blockchain network

power to negate the block appended by that member, and rectify the ledger by forking the chain.

Depending on the nature of the application and the structure of the network, specific consensus schemes may be constructed for the blockchain to ensure tamper-resilience. Note that the mining and consensus schemes constitute the backbone for any blockchain protocol, and hence should be chosen carefully.

Smart Contracts

"A smart contract is an agreement whose execution is both automatable and enforceable. Automatable by computer, although some parts may require human input and control. Enforceable by either legal enforcement of rights and obligations or tamper-proof execution". (definition by Barclays).

Smart contracts are pieces of software, that extend blockchains' utility from simply keeping a record of financial transaction entries to automatically implementing terms of multi-party agreements. Smart contracts are executed by a computer network that uses consensus protocols to agree upon the sequence of actions resulting from the contract's code. With a shared database running a blockchain protocol, the smart contracts auto-execute, and all parties validate the outcome instantaneously and without need for a third-party intermediary.

Classification of Blockchain Ledgers

Based on the choice of the functional components described above, blockchain architectures may be classified broadly into two categories – public and private. In case of public architectures, the process of generation and verification of transactions is publicly available, so that anyone in the network may perform these actions. In fact, the mining process is also open to anyone in the network. However, most often, the mining process relies on some proof-of-work concepts, which may be monopolized by supremacy in financial or computing power. In case of private blockchain architectures, the processes involving the generation and verification of transactions may be access controlled, and restricted to only a fraction of the members on the network. Quite often, this results in a simpler consensus mechanism, which may or may not require a competitive mining at all.

Another popular nomenclature in this line classifies the blockchain architecture as permissioned and permissionless. A blockchain is said to be permissionless if the transactions can be made or verified by anyone in the network, while a blockchain is said to be permissioned if the transactions can be made or verified by predetermined authorized entities. In addition, the permissioned blockchains might include specifically designed access control structure to determine who in the network can view the blockchain ledger, mine blocks and verify blocks. In permissionless blockchain protocols, like Bitcoin, majority consensus is followed in general, where the longest chain sustains. In case of permissioned blockchains, the miners and auditors are trusted entities, and hence the consensus scheme may be designed to be much simpler in such cases. In fact, the mining may be a delegation scheme, instead of a competitive scheme, in a permissioned setting.

Permissionless Blockchain

Let us illustrate the generic structure of a permissionless blockchain architecture by taking the pioneering blockchain application – Bitcoin – as an example.

Block: A Bitcoin block contains the hash of itself, the hash of the previous block, the Merkle root of the transactions that are included in the block, a nonce that is used by a miner to solve the Bitcoin computational hash-puzzle, and the time at which the block was created. The first block in the ledger is the genesis block, and subsequent blocks form a block chain, publicly maintained in a ledger. Some examples of such ledgers are available at blockchain.info, blockexplore.com, etc. A new block is added approximately every 10 minutes through a mining process.

Transaction: A Bitcoin transaction contains a header, inputs and outputs:

- The header contains the transaction ID, hash of the transaction, number of inputs and outputs, time of the transaction, and a version number that tells the verifier which set of rules to use to validate the transaction
- Input to a Bitcoin transaction is another transaction. Each input contains sequence number of the input transaction, address information about the previous output, input script containing the signature with the private key of the user who is spending the coins, and the value of the transaction
- Each output contains the transaction index, address of the recipient, value of the output, and an output script described below.

Verification: Verification of Bitcoin transactions is performed through scripts, implemented in a Turing incomplete stack based scripting language. There are two types of scripts – input scripts and output scripts. Every transaction contains an output script, which states that – "This transaction can be redeemed (spent) by anyone who possesses the public key which hashes to address of the recipient, and also possesses the signature from the owner of that public key". The verification of a transaction is essentially verification of the digital signature against the corresponding public key. This verification routine combines the new input script of a new transaction with the output script of the input transactions, and executes the combination. It might be necessary in certain cases to obtain the approval of multiple parties in order to process a transaction; this is done in Bitcoin using multisig. Bitcoin scripts are even more flexible, and can allow payments to be redeemed after a certain time interval (defined by a time lock).

Mining: Bitcoin follows a competitive mining scheme, based on a hash-puzzle. The miners have to compete with one another, using the computing resources at their disposal, to append a new block to the blockchain ledger. Bitcoin employs a smart incentive mechanism to ensure honesty of the miners, as well as to regulate the influx of Bitcoins in the market. To further regulate the flow of Bitcoins, the hash-puzzle in designed in such a way that new Bitcoin blocks are created (mined) every 10 minutes, on an average. The mining competition based on the hash-puzzle is also known as a proof-of-work strategy for consensus.

Consensus: Bitcoin follows a standard majority consensus, where each miner may choose which block in the chain to append to, and eventually the longest chain sustains. It is widely believed that as long as honest parties control majority of the computing power, the longest chain will grow and outperform other forks.

Ethereum is another widely used crypto-currency facilitating the users of the platform to extend the

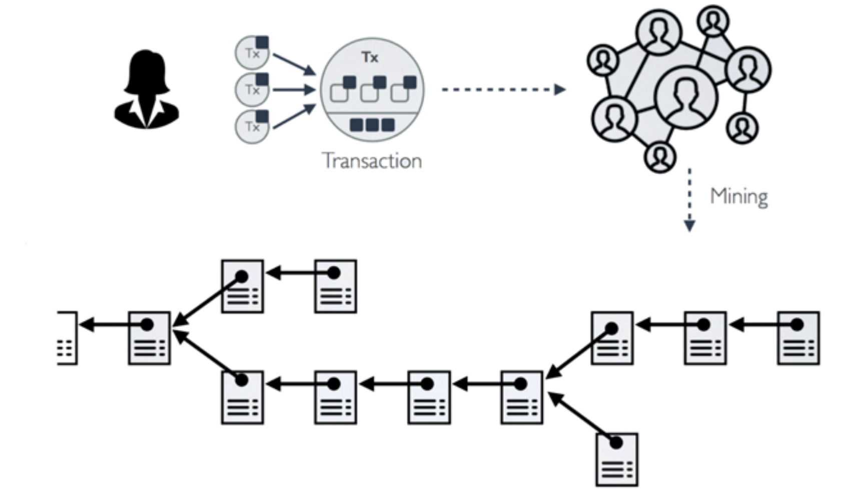


Figure 6. Bitcoin as a specific instance of the Permissionless Blockchain Architecture

basic transaction flow with much richer control flow called smart contract. Ethereum currently uses proof-of-work algorithm called ETHash which is designed to disallow the mining to be done by pools based on Application Specific Integrated Chips (ASIC). This technique allows the GPUs to be used for mining and currently the latency in block creation is 12 seconds as opposed to 10 minutes of Bitcoin. There are proposals to move from this proof-of-work system to proof-of-stake in the next version of Ethereum Consensus algorithm. Like Bitcoin, Ethereum gives an incentive of 5 Ether (Coins in Ethereum).

Ethereum is designed for implementation of complex workflows on the top of distributed ledger. Unlike Bitcoin, Ethereum Virtual Machine allows a workflow involving loops. To facilitate this, the consensus and mining algorithms account for the amount of resources spent for the longer workflows (resource-intensive). Any physical asset such as a car manufactured in a company can be represented as digital entity in the blockchain. Once represented in the blockchain, the complex processes involving the ownership/purchase of this digital entity can be transparently handled through blockchain.

Permissioned Blockchain

The main difference in the structure of a permissioned blockchain as compared to that of a permissionless blockchain arises from the mining process. In a permissioned blockchain, authorized members perform the mining, and in certain applications, the mining process may actually be delegated to authorized members of the network. Verification of transactions and blocks, similarly, may be delegated to authorized members. Consequently, in practical cases, quite often the ledger does not require a consensus scheme to ensure tamper-resilience. In fact, each and every functional component of the blockchain architecture, as discussed earlier, may be custom designed for a permissioned platform. Major design considerations while implementing a permissioned ledger are as follows:

- Identifying the members participating in the system and the role of each
- Identifying the structure of every form of transaction that needs to be performed in the network, and the corresponding verification algorithms
- Designing access control structure to associate the actions (initiate, verify, view etc.) to the members in the network, for each type of transaction
- Designing access control structure for each miner in the network, so as to control who can mine a block and which transactions can be included
- Designing access control structure for each member in the network to define rights of viewing the content of the blocks, and to verify a block
- Designing an appropriate consensus algorithm and an incentive scheme to ensure the honesty of the members in the network, if required.

Each of the above design choices may be adopted based on the target application.

Chapter 2

Advantages of Blockchain Technology in Banking and Finance

BLOCKCHAIN is undoubtedly one of the most talked about technologies in the financial services industry today. Blockchain Technology (BCT)/Distributed Ledgers lead the trend of Gartner Inc.'s Hype Cycle for Emerging Technologies, which allow organizations to connect with new business and payment ecosystems. The shift from a centralized technical infrastructure to distributed, ecosystem-enabling platforms is laying the foundations for new business models in payments, digital banking and financial transaction technologies.

Financial services industry is currently the leader in experimenting with the technology. A number of initiatives that are already underway are driving its progression to an industrial solution which will yield several important benefits in the context of transfer of assets within business networks.

Blockchain holds the potential for all participants in a business network to share a system of records which will provide consensus, provenance, immutability and finality around the transfer of assets within the business network. The reason blockchain can be potentially disruptive is that the distributed ledgers may lead to new business models and the existing processes could move away from a hub and spoke model with intermediaries.

Typically, in the banking industry/financial services, the key transactions in the processes are to underpin asset ownership and asset or value transfer. In order to conclude/settle a transaction, data messages are exchanged between the banks/financial institutions, sometimes including 'trusted' intermediaries. Despite the efforts to reduce the complexities and increase the interconnectedness of participants' transaction records, business networks are still

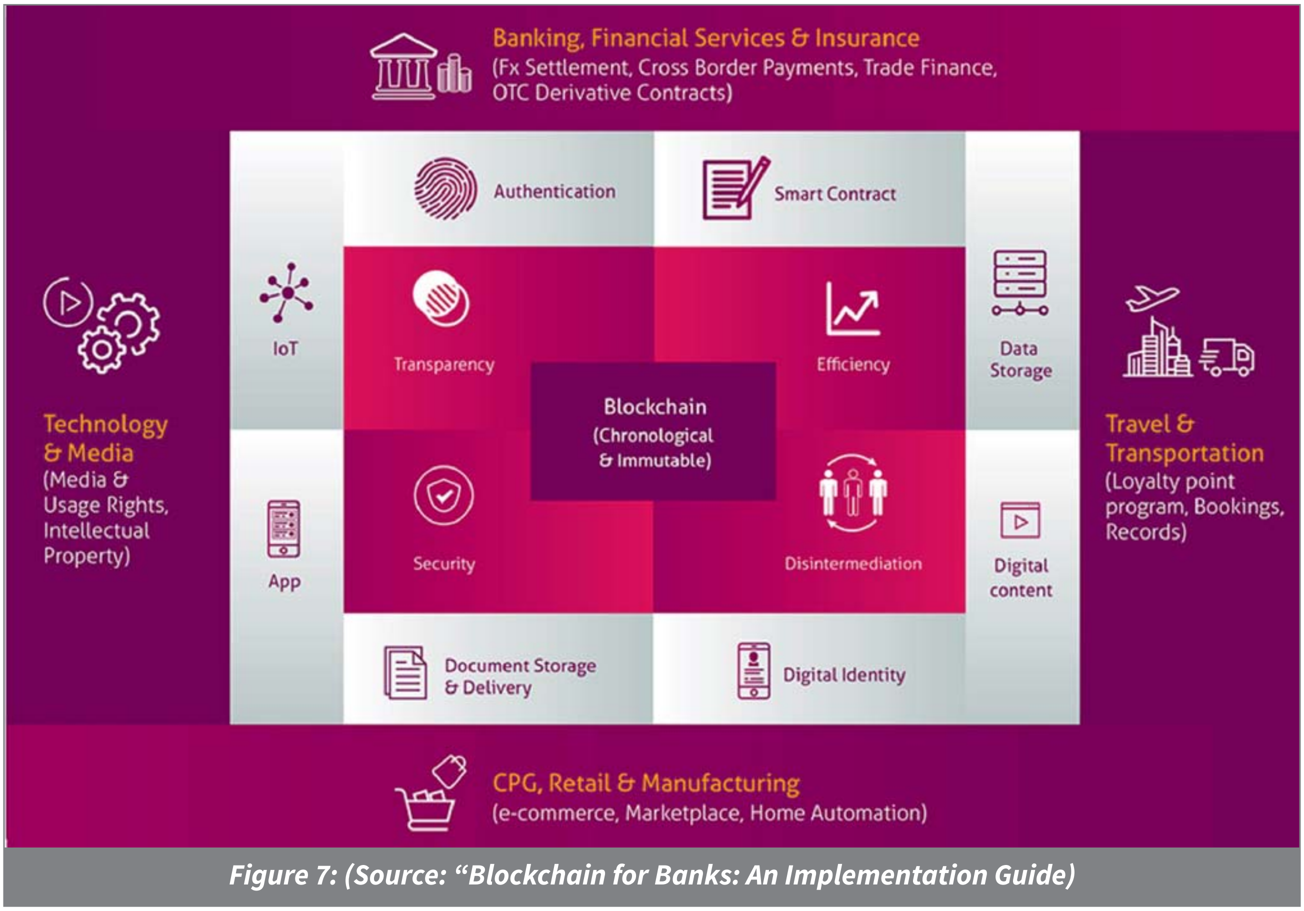

Banking, Financial Services & Insurance
(Fx Settlement, Cross Border Payments, Trade Finance, OTC Derivative Contracts)
Authentication
Smart Contract
IoT
Transparency
Efficiency
Data Storage
Technology & Media
(Media & Usage Rights, Intellectual Property)
Blockchain
(Chronological & Immutable)
Travel & Transportation
(Loyalty point program, Bookings, Records)
App
Security
Disintermediation
Digital content
Document Storage & Delivery
Digital Identity
CPG, Retail & Manufacturing
(e-commerce, Marketplace, Home Automation)

Figure 7: (Source: "Blockchain for Banks: An Implementation Guide)

typically exchanging data or messages between them to conclude transactions. As a result, the processes are sometimes inefficient, expensive, and vulnerable.

BCT has the potential to address certain limitations of the current processes by modernizing, streamlining and simplifying the traditional siloed design of the financial industry infrastructure with a shared fabric of common information. The advantages brought by BCT can be broadly classified into cost savings, efficiency, and transparency.

Cost Savings

Fraud Prevention: As BCT is built on the concept of sharing information across parties and consensus during transactions; it saves on reconciliation cost between banks and prevents losses because of documentary frauds.

Save costs on forex volatility: BCT used in cross border payments can help the consumers and banks to take advantage of the forex marketplace to get the best deal transparently from the market players. Since the transactions are processed in near real-time, the players need not suffer through the vagaries of currency volatility.

Save costs over delayed settlements: In case of a distributed payment network, BCT ensures the transaction settlement information is also processed simultaneously along with the payment messages. Since, the payments and settlements happen in real-time, the participating banks and financial institutions can enjoy reduced pressure on the treasury management to keep their settlement accounts well-funded.

Efficiency

Resilience through redundancy: Being a distributed architecture by design, BCT enables the network to be operated by all permissioned nodes in the ecosystem. All the important members of the payment ecosystem – banks, financial institutions shall effectively become the participating nodes in the BCT network. In the case of an untoward event affecting the ecosystem (like war, floods, earthquakes, cyber-attacks), even if some nodes of the network are unavailable, the consensus algorithms built as a part of the BCT network ensure a transaction can be approved by the remaining nodes in the network. BCT also brings in a high level of redundancy in the network, as the copy of the ledger is available with all the nodes in the network.

Reduced time for processing: Most of the conventional banking processes are linear and hierarchical, akin to the assembly line of the manufacturing industry, e.g., maker-checker/cross check/approval processes. While the maker-checker-approver process helps the banks and FIs to gain control and puts the emphasis on ownership of decisions, it delays in decision making and can lead to longer processing time, costs and lower customer satisfaction. BCT can radically alter the way such transactions are processed by banks and FIs today.

In BCT, the transaction is relayed to all the approving nodes simultaneously, as and when the approvals are provided, the information is updated in the ledgers of all the nodes, instantly. Thus, BCT can help in improving the speed of processing transactions by reduction in decision making time across the organizations resulting in reduced cost of processing and enhanced transparency of decisions to all participating nodes.

Smart Contracts are business terms that are embedded in the transaction database and gets automatically executed when certain business conditions are met. Smart Contract feature in the BCT enables speed of processing and helps banks to create and execute complex business rules that have minimal human intervention and it can address the market needs that could not be satisfied before.

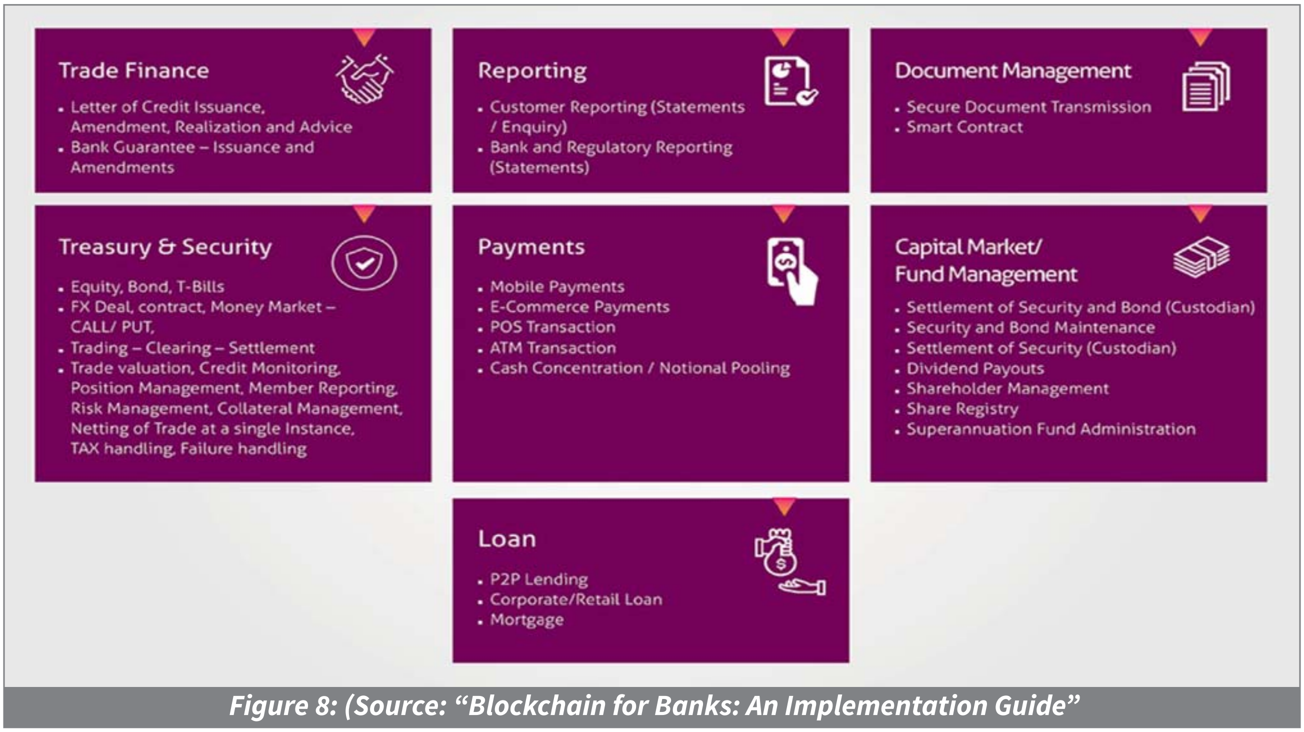
Faster settlements: Blockchain can also help to address KYC and identity management challenges as a lot of the data to prove identity is already in digital form and BCT could enable instant verification. Use of BCT can reduce duplicative recordkeeping, eliminate reconciliation, minimize error rates and facilitate faster payment/asset settlement. In turn, faster settlement means less risk in the financial system and lower capital requirements.

One of the most frequently suggested example where BCT can be readily applied to banking is in the Trade Finance area.

A trade finance solution with letter of credit, bill of lading and multi-signature solutions based on BCT would include the following features:

- Carriers issue bill of lading on the BCT as a digital asset
- Banks issue letter of credit as a digital asset on the BCT
- Multi-signature contracts
- Smart-contract-enabled, event-based fund release to ensure speed and transparency.

Although blockchain is imagined as an open system for transaction processing across the financial system, banks are initially looking inward, experimenting with the distributed ledger approach to create efficiencies and a single version of digital truth. Subsequently, onboard other external parties in the ecosystem for mutual benefits with a permission-based ledger system that can move cash and assets in real-time to settle market transactions.



Trade Finance
- Letter of Credit Issuance, Amendment, Realization and Advice
- Bank Guarantee – Issuance and Amendments

Reporting
- Customer Reporting (Statements / Enquiry)
- Bank and Regulatory Reporting (Statements)

Document Management
- Secure Document Transmission
- Smart Contract

Treasury & Security
- Equity, Bond, T-Bills
- FX Deal, contract, Money Market – CALL/ PUT,
- Trading – Clearing – Settlement
- Trade valuation, Credit Monitoring, Position Management, Member Reporting, Risk Management, Collateral Management, Netting of Trade at a single Instance, TAX handling, Failure handling

Payments
- Mobile Payments
- E-Commerce Payments
- POS Transaction
- ATM Transaction
- Cash Concentration / Notional Pooling

Capital Market/ Fund Management
- Settlement of Security and Bond (Custodian)
- Security and Bond Maintenance
- Settlement of Security (Custodian)
- Dividend Payouts
- Shareholder Management
- Share Registry
- Superannuation Fund Administration

Loan
- P2P Lending
- Corporate/Retail Loan
- Mortgage

Figure 8: (Source: "Blockchain for Banks: An Implementation Guide"

Saving in decision making time: BCT helps in improving the rate of processing transactions by reducing decision making time, thus resulting in reduced cost of processing and enhanced transparency of decisions to all the participating nodes. As BCT brings transparency to the system, availability of audit trails brings in the necessary control and trust to the participating members which may help improve the services through continuous innovation.

Transparency

Immutable Transactions: Maintaining an immutable record of transaction events in a chronological order being a main pillar of its architecture, BCT guarantees much desired attributes to banking and financial transactions such as immutability and finality.

Provenance: In the area of payments, while the exchange of messages reasonably offer clarity on each step in the payment process, BCT could add to it by providing provenance and auditability for these messages and thus bringing about transparency and efficiency in the processes leading to reduction in overall settlement time and risk.

Provenance ensures the finality of the ownership of the asset and it saves efforts and processes to prevent double collateralization of the same asset. As a ledgering technology, blockchain will not replace the payment systems or the messaging systems deployed by banks, but these systems will connect to the blockchain, augmenting existing business networks and providing increased discoverability and trust.

Chapter 3

Applications of Blockchain Technology

IN order to identify the potential application areas of BCT in Indian banking, it may be prudent to look at the various use-cases of BCT taking shape across the world and select cases that will be suitable and can be implemented in India. The use-cases can be broadly categorized into applications with and without native currency.

Digital Currency

Electronic Money, which is an early version of digital currency is formally defined as "value stored electronically in a device such as a chip card or a hard drive in a personal computer". The value stored and transferred needs to be denominated in a sovereign currency to be considered e-money; while, in many cases digital currencies are not denominated in or even tied to a sovereign currency, but rather are denominated in their own units of value. A cryptocurrency is a form of digital currency designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency.

The examples of cryptocurrencies include Bitcoin, Litecoin, Ripple, Ethereum and Dogecoin. Typical cryptocurrencies have their own advantages and disadvantages.

Advantages

Control and Security: Users are in control of their transactions, without foregoing their privacy while overcoming identity theft. Due to the fact that blockchain transactions cannot be reversed, do not carry with them personal information, and are secure, merchants are protected from potential losses that might occur from fraud.

Transparency: All finalized transactions are available for everyone to see thus allowing immediate verification of transactions. Protocols being open source undergo wide scrutiny, thus enabling trust in the underlying platform and guaranteeing that they cannot be manipulated by any single person, organization, or government. It is possible to send and receive money anywhere in the world at any given time, without a central authority.

Very Low Transaction Cost: Currently, blockchain payments fees is very low. With transactions, users might include fees in order to process the transactions on a priority basis. Digital currency exchanges help merchant process transactions by converting them into fiat currency by charging lower fees than credit cards and PayPal.

Disadvantages

Risk and Volatility: Digital currencies are very volatile mainly due to the fact that there is a limited amount of coins and the demand for them increases by each passing day.

A Committee on Digital Currencies set up by Bank for International Settlements (BIS), is cautious about Digital Currencies. They have observed that unlike traditional e-money, digital currencies are not a liability of an individual or institution, nor are they backed by an authority. Furthermore, they have zero intrinsic value and, as a result, they derive value only from the belief that they might be exchanged for other goods or services, or a certain amount of sovereign currency, at a later point in time. Accordingly, holders of digital currency may face substantially greater costs and losses associated with price and liquidity risk than holders of sovereign currency.

The degree of anonymity provided by some digital currency schemes may discourage a range of financial system participants from direct use or from providing facilities for digital currency use to their customers, as AML/CFT requirements may be difficult to satisfy in relation to digital currency transactions. Also increased adoption and use of digital currencies could affect the conduct of monetary policy.

Central Bank Issued Digital Currencies

While there are disadvantages of existing cryptocurrencies, many central banks around the world have stepped up their efforts towards developing digital versions of their fiat currency to leverage the benefits of the underlying technology – BCT.

The Central Bank of Canada has revealed recently that it is developing a digital version of the Canadian dollar based on BCT, called CAD-coin. Other major banks including Bank of Montreal, CIBC, Royal Bank of Canada, Scotiabank and TD Bank, as well as banking consortium startup R3CEV, are said to be involved in the effort. Bank of England is also exploring the area of digital currency.

LHV Pank — the largest independent Estonian bank — became the first bank in the world to experiment with programmable money when it issued €100,000 worth of cryptographically-protected certificates of deposits. Cuber (Cryptographic Universal Blockchain Entered Receivable) Technology, a subsidiary of LHV Pank, focuses exclusively on Bitcoin-based digital securities. Cuber's work comprises two strands: CUBER securities and the Cuber Wallet.

The Dutch central bank is experimenting with a bitcoin-based virtual currency called "DNBCoin". Russian government-controlled Sberbank of Russia owns "Yandex.Money" – electronic payment service and digital currency of the same name. In 2016, a city government in Switzerland, first accepted digital currency in payment of city fees. Zug, Switzerland added bitcoin as a means of paying small amounts, up to Sfr 200, in a test. Swiss Federal Railways, government-owned railway company of Switzerland, sells bitcoins at its ticket machines.

BCT Applications without Native Currency

Trade Finance: One of the most frequently suggested examples of where blockchain can be applied is in the trade finance area. If some banks decide to put the letters of credit – on the blockchain, then that is pretty powerful – but to be really powerful the big corporates, the big shippers, and manufacturers, need to be on board, as well as the customs authorities. As both letters of credit and bills of lading have very complex and intricate information flows, even if only a few participants were using a blockchain solution this would generate significant advantages.

Barclays and an Israel-based start-up company have carried out what they say is the world's first trade transaction using BCT, cutting a process that normally takes between seven and 10 days to less than four hours. The transaction guaranteed the export of almost $100,000 worth of cheese and butter from Irish agricultural food co-operative Ornua – formerly the Irish Dairy Board – to the Seychelles Trading Company. The deal was executed via a blockchain platform set up by Wave, a firm that came through a Barclays development programme.

Bank of America, Merrill Lynch, HSBC and the Infocomm Development Authority of Singapore have claimed success in demonstrating the application of distributed ledgers to replace paper-based Letters of Credit in trade finance transactions. The application enables exporters, importers and their respective banks to share information on a private distributed ledger. The trade deal can then be executed automatically through a series of digital smart contracts once certain conditions are satisfied. The parties involved in the transaction can visualize data in real-time on their devices and see the next actions to be performed. The application uses the open source Hyperledger as blockchain fabric, supported by IBM Research and IBM Global Business Services.

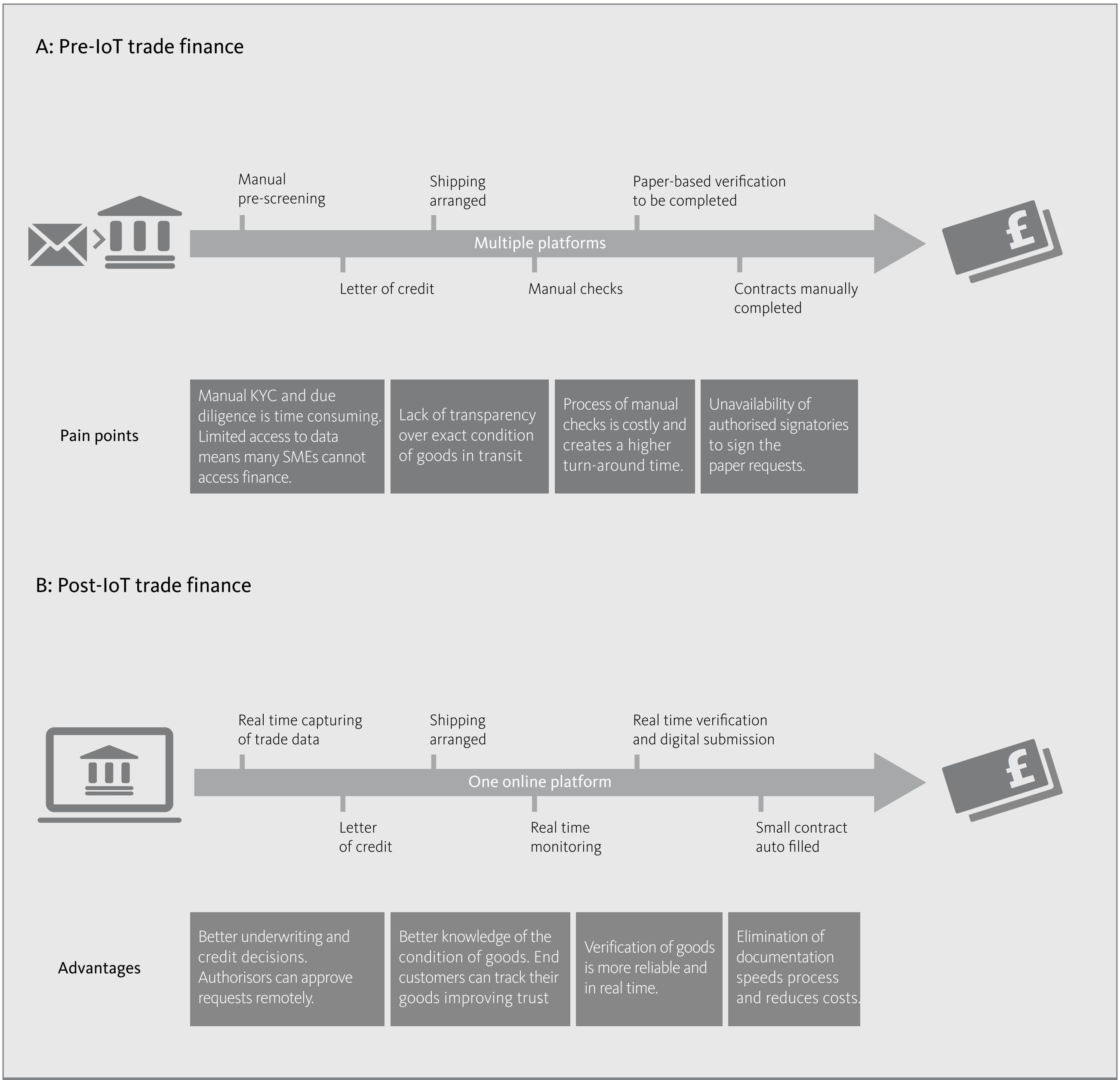

A: Pre-IoT trade finance
Manual pre-screening
Shipping arranged
Paper-based verification to be completed
Multiple platforms
Letter of credit
Manual checks
Contracts manually completed
£
Pain points
Manual KYC and due diligence is time consuming. Limited access to data means many SMEs cannot access finance.
Lack of transparency over exact condition of goods in transit
Process of manual checks is costly and creates a higher turn-around time.
Unavailability of authorised signatories to sign the paper requests.
B: Post-IoT trade finance
Real time capturing of trade data
Shipping arranged
Real time verification and digital submission
One online platform
Letter of credit
Real time monitoring
Small contract auto filled
£
Advantages
Better underwriting and credit decisions. Authorisors can approve requests remotely.
Better knowledge of the condition of goods. End customers can track their goods improving trust
Verification of goods is more reliable and in real time.
Elimination of documentation speeds process and reduces costs.

Figure 9: Pre- and Post IoT trade finance highlighting advantages of the IoT (Source: "The Fintech 2.0 Paper: rebooting financial services")

Cross-border Payments: Ripple is using distributed ledger technologies to transform the cross-border payment business, to make international payments easier and faster and has added a few banks to its network. The recent cyberattacks in Bangladesh, Vietnam and Ecuador have highlighted the vulnerabilities in cross-border transaction banking. Distributed ledgers present an opportunity to help banks partially overcome such vulnerabilities in the future.

Santander Bank launched a new app to facilitate live international payments (foreign remittances), powered by BCT. The app uses core technology provided by Ripple.

FX Trading: Currently multiple records for currency trade have to be created for buyer, seller, broker, clearer and third parties and then continuously reconciled across multiple systems. Cobalt DL uses BCT, eliminating multiple trade records for buyer, seller, broker, clearer and third parties from each transaction. By presenting a shared view of a trade, Cobalt DL frees up back- and middle-office resources that are currently overwhelmed by the need for continuous reconciliation across multiple systems. This is backed by eight major banks and financial institutions.

The technology is designed to integrate seamlessly with all trading sources and venues, providing immediate efficiency benefits, analysis of which has shown to deliver a significant cost reduction when compared with existing infrastructure. FX market participants incur multiple unnecessary license fees, ticketing charges, IT overheads and staff costs as a result of the complexity of existing structures.

BCT in Capital Markets: R3 is a financial innovation firm that leads a consortium partnership with over 50 of the world's leading financial institutions, to work together to design and deliver advanced distributed ledger technologies to the global financial markets.

BCT can revolutionize the Capital Market trading processes. There are several intermediaries involved in a trade, like exchanges, central counterparties (CCPs), central securities depositories (CSDs), brokers, custodians and investment managers. For correct accounting and to complete the business transaction, intermediaries need to update their respective ledgers based on the messages exchanged between them. This creates a delay and also additional cost. Sometimes, to enable a particular transaction and the corresponding ledger updates, intermediaries may need to complete a few additional ledger transfers in the form of realignment, securities borrowing or cash management. This introduces additional delays in the transaction lifecycle, increasing the time for final settlement.

BCT will benefit Capital Market Services at all stages of Trade and securities servicing.

Pre-Trade: A blockchain system that stores and facilitates KYC data will help in reducing cost and eliminating the number of KYC checks. It will also help in Transparency and verification of holdings, leading to reduced credit exposures.

Trade: BCT ensures a Secure, real-time transaction matching, and immediate irrevocable settlement; it also helps in Automatic DVP on a cash ledger and automatic reporting & more transparent supervision for market authorities, establishing higher AML standards.

Post-Trade: Eliminates intermediaries as no central clearing is needed for real-time cash transactions; results in reduced margin/ collateral requirements; faster and efficient post-trade processing; fungible use of assets on BCT as collateral; auto-execution of smart contracts establishes the liabilities of parties over the life-cycle, like in derivatives.

Custody & Securities Servicing: Securities are directly issued onto a blockchain to the parties; the servicing processes are automated and duplication avoided. Fund subscriptions and redemptions are processed automatically making it simple for accounting, allocations and administration.

Pre-IPO shares allotment: NASDAQ announced that it has issued its first investor shares on the platform Linq, a blockchain-based service, to issue pre-IPO shares of companies.

Loan Syndication: Financial services giant Mizuho has announced a BCT trial to be focused on syndicated loans, including Information Services International-Dentsu (ISID), blockchain startup Currency Port and Microsoft Japan.

Bond Trading: IBM and SBI Securities, a subsidiary of SBI Holdings, are looking to create new mechanisms for trading bonds, using IBM's Hyperledger as a basis for the trials. The goal of the collaboration between SBI and IBM is to test commercially viable platforms for blockchain-based bond trading.

Supply Chain Financing: The IBM business unit deals with 4,000 suppliers, financing customers and partners who conduct about three million transactions per year, worth $44 billion. About 25,000 disputes arise annually over issues such as the wrong number of computer parts in an order or deliveries that go awry. Normally, it takes an average of 44 days to resolve such issues. Furthermore, employees use roughly six to seven software applications to verify steps taken in the arrangement as well as having to call banks, financial institutions, and associated partners. IBM said the use of

Distributed Ledger Technology (DLT) records faster and more accurately than IBM's traditional resources, has resulted in a 10-day resolution period. The same solution can be deployed by any big corporate and banks for supply chain finance.

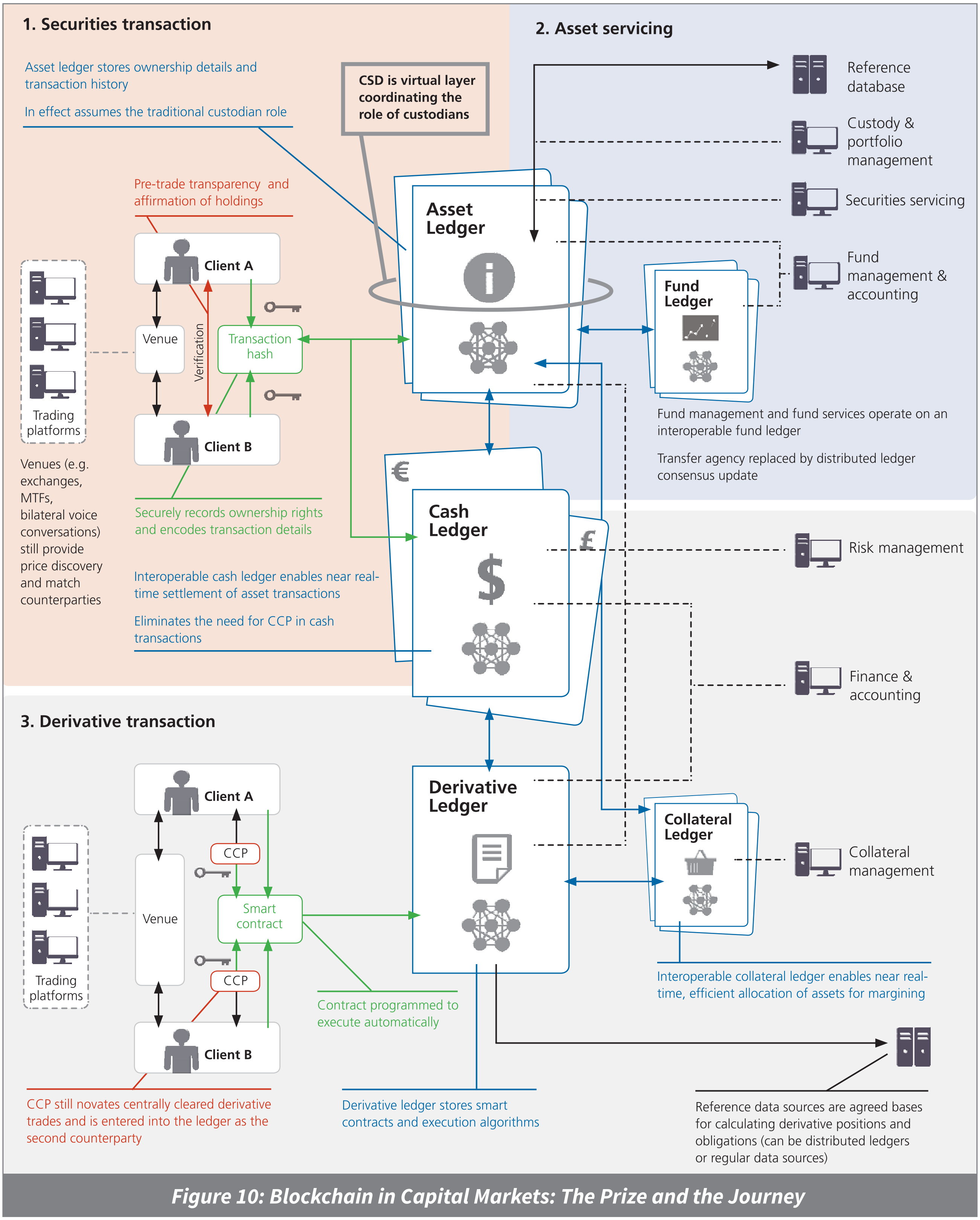

1. Securities transaction
Asset ledger stores ownership details and transaction history
In effect assumes the traditional custodian role
CSD is virtual layer coordinating the role of custodians
Pre-trade transparency and affirmation of holdings
Client A
Venue
Verification
Transaction hash
Client B
Trading platforms
Venues (e.g. exchanges, MTFs, bilateral voice conversations) still provide price discovery and match counterparties
Securely records ownership rights and encodes transaction details
Interoperable cash ledger enables near real-time settlement of asset transactions
Eliminates the need for CCP in cash transactions
2. Asset servicing
Reference database
Custody & portfolio management
Securities servicing
Fund management & accounting
Asset Ledger
Fund Ledger
Fund management and fund services operate on an interoperable fund ledger
Transfer agency replaced by distributed ledger consensus update
Cash Ledger
€
£
$
Risk management
Finance & accounting
3. Derivative transaction
Client A
Venue
CCP
Smart contract
CCP
Client B
Trading platforms
Derivative Ledger
Collateral Ledger
Collateral management
Contract programmed to execute automatically
Interoperable collateral ledger enables near real-time, efficient allocation of assets for margining
CCP still novates centrally cleared derivative trades and is entered into the ledger as the second counterparty
Derivative ledger stores smart contracts and execution algorithms
Reference data sources are agreed bases for calculating derivative positions and obligations (can be distributed ledgers or regular data sources)

Figure 10: Blockchain in Capital Markets: The Prize and the Journey

Monitoring of Consortium Accounts

IBA is suggesting an innovative usage of BCT – Monitoring of Financial Transactions of a borrower financed by a consortium of banks. This will help in preventing "diversion of funds", which is a major concern of the banks today. The borrower moves funds from one bank to another and the end-usage is not known to the lenders. In the absence of a central entity, it is not operationally feasible to securely and reliably track the movement of money between accounts maintained across multiple financial institutions. A collaboration-based approach among financial institutions, on the other hand, can enable them to monitor money movement and perform the desired analytics thereon to detect anomalies as per the mutually agreed rules and patterns. The blockchain-based collaboration can also assist the participating banks/institutions to have better visibility of the use of loan money provided to corporates by tracking the movement of funds and analyzing how the said money was spent/paid and generating leads therefrom for auditing and scrutiny. Use of BCT will make the information of movement of funds available to all consortium members and help strengthen the monitoring mechanism.

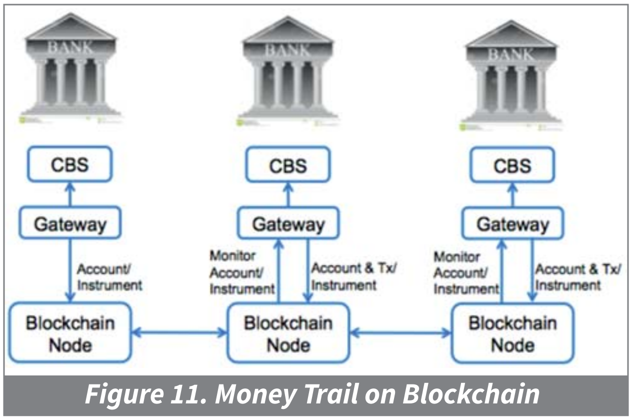


Figure 11. Money Trail on Blockchain

KYC

The increasing cost of regulatory compliance is among every banker's top concerns, having to comply with regulations such as Anti-Money Laundering (AML) and Know Your Customer (KYC).

Every bank and financial institution has to perform the KYC process individually, and upload the validated information and documents to the central registry that stores digitized data tagged to a unique identification number for each customer. By using this reference number, banks can access the stored data to perform due diligence whenever customers request for a new service within the same banking relationship, or from another bank.

A blockchain-based registry would remove the duplication of effort in carrying out KYC checks. The ledger would also enable encrypted updates to client details to be distributed to all banks in near real-time. The KYC ledger would provide a historical record of all documents shared and compliance activities undertaken for each client. This will form the evidence to be provided to the regulators. It would be useful to identify entities attempting to create fraudulent histories. The data within it could be analyzed to spot irregularities or foul play – directly targeting criminal activity.

SWIFT launched the SWIFT KYC Registry in December 2014, and more than 2000 banks have already enrolled with it. Banks are struggling to manage and integrate all the data required for KYC compliance to obtain a consolidated view of the customer, which explains the popularity of central registries like the one managed by SWIFT. SWIFT is now exploring the use of BCT for the same.

Chapter 4

Security, Privacy & Scalability Aspects of Blockchain Systems

BLOCKCHAIN platforms are starting to be embraced by the financial industry in various aspects of their business operations and technology. By definition, a distributed ledger platform contradicts a financial institution's need for control of its data. This is now changing as financial firms are recognizing commoditized operational functions and leveraging Distributed Ledger Technology to streamline those processes. Blockchain platforms have the potential to solve various weaknesses in existing financial technology, but there are important concerns around security, privacy and scalability that must be considered. This section explores all three of these issues.

To understand these issues and concerns surrounding the technology, we need to explore several aspects of its architecture, such as:

Acceptable level of security considering multiple components and entry points that are present in BCT systems

- Consensus mechanisms
- Encryption of data
- Network configuration
- Component configurations for scalability at all levels.

Different applications of BCT may have differing architectural requirements. The design of platform will need to be carefully considered to balance these concerns. Quite often there may be a need for trade-offs between security, privacy and scalability requirements based on the business context and use case.

Security Aspects of a Blockchain Deployment

Financial institutions rely heavily on security procedures and technology to ensure the safety of their data. BCT provides a secure and naturally decentralized framework for transaction processing. One of the major advantages of BCT is integration of data processing, consistency and security into an algorithmically enforced protocol. Blockchain systems can be public (or permissionless) or permissioned in nature. Participants in permissionless blockchain are anonymous by default and anybody with a valid version of the software can participate and create transactions. Due to legal and technical concerns, institutions that operate financial ledgers or registries may be inclined to utilize permissioned blockchains as they form a more controlled and predictable environment than permissionless blockchains.

Blockchains have the potential to address the holy grail of Info Security – the CIA trinity (Confidentiality, Availability and Integrity). Being a fundamentally distributed system, blockchain ensures high availability and integrity of the transaction data. As all nodes are in essence agreeing to the state of records based on a historical 'chain' of transactions – integrity of the data is maintained. By appropriate use of cryptographic keys, confidentiality of transactions can also be addressed. This makes blockchain systems robust from an InfoSec perspective.

However, while considering security in blockchain systems, a holistic view is essential. One needs to look beyond traditional endpoint protection and adopt a holistic approach that includes authentication and authorization of entities accessing the blockchain, transaction and communication infrastructure security, business security through transparency and audit, and security from malicious insiders, compromised nodes or server failure.

Security in general needs to be multi-level and one that encompasses all components and entry points in the system. Let us take a look at the different levels at which security aspects need to be addressed in detail.

Blockchain systems typically need to look at security from the following perspectives:

- Ledger level security
- Network level security
- Transaction level security
- Associated surround system security
- Smart Contract security.

Ledger Level Security

Membership to the blockchain needs to be restricted to participants who have been subject to required scrutiny. Typically, members will be institutions who have real world legal credentials and are unlikely to disengage (as opposed to retail users who can withdraw from participation). The processes required to onboard entities onto the blockchain network must ensure that only legitimate entities are allocated the required credentials. All transactions initiated from member nodes need to be signed so that only valid participants can create transactions in the network.

Network Level Security

Blockchain systems typically consist of multiple sub-components in addition to the blockchain software – these may include conventional "shadow" databases, messaging, and other services. It is recommended that communication between components of different nodes is made secure from a networking standpoint.

The network must be resistant to many different attack vectors, both external and internal to the network. The ledger must have provisions to withstand DoS attacks where an attacker can potentially spam the network with spurious transactions or acquire control of significant percentage of the nodes or block creation/validation in a manner that they effectively control the network. For a permissioned network, the effectiveness of DoS attacks may be reduced by peer validation (e.g. whitelisting node IPs within the network) since all nodes and participants are known. Internal transaction spamming attacks (node delinquency) may be dealt with by quickly blacklisting the delinquent node since the source of the attack is not distributed.

Blockchain is a distributed processing system and as such to derive the true benefits of blockchain, it may be best to avoid centralization of any process, i.e. ensure there is no single point of failure for any process. This includes ledger on-boarding processes.

Transaction Level Security

Transaction level security is critical for financial institutions. Transaction accuracy and immutability is what drives the firm's books and records. Here are some key concepts in securing transactions:

- Relevant details of transactions must be encrypted using PKI concepts so that transaction details are not compromised to unintended parties
- Transactions consist of moving an asset from one address to the other (a few use cases may not involve assets), the transaction model must be such that parties having access to the ledger are not able to trace activities or transactions done by other participants by observing transaction addresses. This is to enforce the notion of 'unlinkability' of transactions
- Associated transaction information such as documents must also be encrypted so as to allow only concerned nodes to interpret the information
- Transaction creation identity and authorization must be safeguarded. i.e., only institution 'A' should be able to perform transactions using institution A's name/ID
- Transactions should be unmodifiable i.e., transaction information committed to the ledger should be probabilistically near impossible to modify – no one should be able to change the payment amount, the sender information, the recipient information or any other associated transaction information
- Transactions should be generally censorship resistant i.e., if a transaction complies with the ledger protocol and validation rules, it should eventually be added to the ledger
- For sensitive transactions, utilizing the multi-signature feature available in blockchain systems can be explored.

Associated Surround System Security

Blockchain systems might typically include associated systems such as shadow databases, key stores, etc. Security of these systems is also of paramount importance.

- Access to associated surround system components such as shadow databases etc. must be controlled through implementation of appropriate authentication and authorization mechanisms
- Privileges/roles applicable to the blockchain node must be linked to the surround systems as well with a view to prevent intentional or unintentional "privilege escalation"
- As the use cases might involve sharing of documents, there is a need to implement some mechanism which prevents proliferation of malware – viruses /worms, etc.
- Deployment of components of a node might need to take into account appropriate placement with regards to corporate firewalls (if applicable)
- An 'n' tier deployment model can be used for different components to be grouped and deployed in different tiers. Segregation of components makes for a more secure system.

Contract Security

Smart contracts (also called self-executing contracts, blockchain contracts, or digital contracts) are simply computer programs that act as agreements where the terms of the agreement can be pre-programmed with the ability to self-execute and self-enforce. Smart contracts are written using programming languages such as C++, JavaScript, Java, Go, Python, etc.

As with any computer program, there is a possibility that the creator of the contract program intentionally or otherwise creates a flawed program which can introduce vulnerabilities for the assets controlled by the contract. To circumvent this, contracts loaded onto the blockchain should conform to certain base rules outlined by the network and should be thoroughly audited for vulnerabilities or unfair bias before deployment.

Additionally, smart contracts may require data from external sources as inputs to their functions, which introduces the possibility of receiving tampered or false data. Services that provide trusted data to smart contracts, referred to as Oracles, may provide cryptographic proof that the data submitted has not been tampered with and came from a trusted source.

Other Considerations

Handling Server Corruption/Outages

Blockchain systems by their distributed design are 'highly available' systems. There is an implicit assurance that a transaction will always be processed – data is processed by multiple nodes and stored in multiple places. This design clearly has many advantages. One factor that needs to be ensured is that a corruption event at one of the nodes in the network does not cascade across the entire network. For resiliency, critical functions should never be served by a single node. Should all nodes performing a critical function be unavailable, then transactions may be queued by the remaining nodes and fed to the failed nodes for processing, once they are brought back online.

Native tokens

Many blockchain systems have a native token or digital currency associated with the ledger. These tokens or digital currencies might be acting as a fuel for the functioning of the ledger either by burning the token during transactions or as a form of incentives to participants. In case this native token or digital currency has value in the external world, then one needs to consider the impact of volatility of the value with regards to normal functioning of the ledger. A crash or spike in the value of the native token might impact business models drastically. Malicious events that happen in the external world can impact the functioning of the ledger in this case.

It might be therefore prudent to have a ledger that is asset agnostic and one which does not have any native token or currency that has value of its own in the outside world.

Privacy Aspects of a Blockchain Deployment

Background

The original, and still the most well-known, use for blockchain is in the Bitcoin cryptocurrency. One of the principles of Bitcoin is that all transactions will be visible to all participants, so that anyone can verify if a particular transaction is valid (i.e., does not represent a double spend) or not.

On the face of it, this might seem like it violates the privacy of every user. However, the anarchic world of Bitcoin does not require anyone to identify themselves, and therefore, direct identification of the parties in a transaction is impossible. Indirect identification consisted of tracking a set of coins through several transactions until something hit the real world, but that had its own uncertainties. Also, each Bitcoin user can create any number of "bitcoin addresses" (which is a 256-bit number that is effectively random), wherein linking transactions (i.e., identifying transactions that were made by the same person), is much more difficult.

In the "permissioned" world, however, there are no unknown players. Every member of the blockchain must be "known" in some manner. Applied naively, therefore, this combines with the inherent properties of a blockchain to create a total lack of privacy for the members: not only their identities, but all their transactions and who they transact with would be laid bare.

Clearly, a situation where everyone knows everything is untenable. A simplistic approach is to say that every transaction is only known to the transacting entities, but that does not address requirements of auditability or regulatory compliance, both of which are important mandatory requirements in most cases.

The problem, thus, is to determine the minimum amount of such dissemination that is required to run the blockchain, without losing the advantages of verifiability that a blockchain provides, and without compromising everyone's privacy thoroughly.

Digging into the problem

At this point it may be useful to delve a bit deeper into what exactly the privacy mechanism needs to deal with. We can divide the privacy requirements into the following categories:

Transactional Privacy

This is the simplest to understand – only the transacting parties, as well as any regulators and auditors who are given access to the transaction, should be able to see specified details of a transaction.

This is, indeed, the absolute minimum information that is required as far as visibility into the transaction details is concerned. However, it makes it impossible for an entity that is not part of this transaction, to be able to trust any future transactions where the content of this transaction are relevant. It is assumed that participating nodes have a mechanism to validate transactions considering availability of funds, especially in cases where transaction is entirely encrypted.

Unlinkability

We have established, above, that arbitrary entities may not know the details of transactions between others. However, depending on how that problem is solved, some information may leak. That is, despite not knowing the identity behind any specific transactions, it may be possible to mine the data from several transactions and use their combined information to figure out who the parties may be, perhaps by connecting this data with external events. The notion of unlinkability is about preventing such deductions from being made.

Auditor/regulatory access

While maintaining transaction privacy and unlinkability, the system also needs to make sure that some specific parties, such as duly appointed auditors or a regulatory body, or their appointees, are able to access specific data to the level they need to perform their functions. In some cases, this might mean that they need to access everything, but most of the time this will be ad hoc, perhaps using a request-response mechanism of some kind. This means the system should be able to implement access with the required granularity, as well as supply keys to an authorized entity in order to process the audit function.

Privacy against auditors

The almost-unfettered access that auditors have, may itself be misused, either intentionally or inadvertently. This needs to be considered and, where possible, mitigations applied.

Privacy in multi-chain environments

The number of blockchain implementations continue to increase. There are several variants on the basic theme, with different design choices made at various points. Also, even if the blockchain technology used is identical, two different deployments may not be able to talk to each other.

However, it is clear that interoperability between different blockchains is a highly desirable feature. As and when that gets solved in some manner, considerations of privacy need to be handled. This is especially true if the two chains had different notions of what should be private and what need not be.

Scalability Aspects of a Blockchain Deployment

The scalability of any potential commercialized blockchain may be limited by multiple factors. Blockchain platforms may face different choke points and constraints on scalability which are dependent on the specific use cases addressed by the platform in question. Hardware limitations will be driven by software and administrative configurations. Certain retail applications may also be limited at the interface level by consumer technology penetration, however with over 30% of the Indian population having access to smartphones or internet connectivity in 2016, and a fast continuing growth of access to these services, this presents a more distant limitation on retail scalability than the immediate hardware resources required by blockchain platforms.

Scalability will be affected by the architecture and configuration of the blockchain platform due to variable requirements for processing power, network bandwidth and data storage. Bandwidth and storage may be of particular concern in a blockchain type network because of the replication and distribution of data between all participants, rather than just the counterparties involved in a transaction. This can multiply the amount of data exchanged by each node considerably compared with a traditional network model.

Effect of block size and block generation time on scalability

In blockchain systems block size, block generation time window and propagation of blocks across the network are aspects that can have a significant impact on the scalability of the system.

The size of block determines number of transactions or artifacts that can be accommodated in a block. For systems where a high volume of concurrent transactions are happening, the size of the block determines how many transactions can be confirmed simultaneously.

The block generation time is the window between two successive blocks getting generated. Let us assume this is 'M'. To determine 'M' correctly, one needs to take into account two aspects:

- Time for propagation of block and supplementary data (auxiliary data like documents) to all nodes (X)
- Time required for nodes to determine validity of the previously added block (Y).

It becomes clear that 'M' will need to be greater than X+Y.

Depending on the use cases and the business context, the values of the block size as well as the block generation time 'M' need to be determined to create systems with appropriate scalability for the business context.

Effect of Consensus and Validation Mechanism

Various methodologies exist for solving the Byzantine Generals' Problem that decentralized systems face. Some methods are more suitable for public permissionless implementations and others are suitable for controlled membership 'permissioned' implementations. Current public permissionless blockchains often use either “Proof-of-Work” (PoW) or “Proof-of-Stake” (PoS) algorithms. The PoW algorithm relies on a computationally expensive process to achieve near immutability of recorded transactions in a public environment but introduces latency and operational costs to the process.

It is unlikely that any institutional application will rely on public networks and instead will rely on permissioned implementations which have the advantage of being able to sacrifice total decentralization in favour of a trusted network where only authorized and trusted participants may operate. In such permissioned implementations, much more efficient solutions to the Byzantine Generals' Problem can be used. Multiple variations of consensus algorithms exist and eliminate the requirement for heavy processing power. These algorithms may be selectively implemented to alleviate the scalability limitation from processor intensive consensus mechanisms.

Effect of Security/Privacy Mechanism

Blockchain platforms usually rely on public key cryptography for the implementation of security, permissions and ownership. Verification and validation of keys is a comparatively efficient process requiring only small amounts of processing power, and so does not introduce significant sources of latency. However, proposed methods for ensuring the privacy of transactions can introduce a significant source of latency.

Transactions in financial networks often require total privacy for the counterparties involved. The decentralized nature of a blockchain validation process means that information about transaction contents may be required by all nodes for the purpose of validating the transaction. As mentioned in the privacy section, it is difficult to productionize homomorphic encryption and while Zero Knowledge Proof has been used in some blockchain implementations, generation of the proof is computationally expensive and so introduces additional latency in processing of transactions. This can negatively affect scalability of a high throughput system in favor of privacy and may not totally stop information leakage. There is much development focus on Zero Knowledge Proofs across the blockchain community, and more efficient solutions may emerge with time to improve these limitations. Alternatively, a trusted administrator or third party may be in charge of validation; however, this may introduce single points of failure and so should be architected with resiliency in mind.

Not all financial blockchain applications require homomorphic style encryption. Blockchains that do not hold balance information may not require validation of transactions for the purpose of maintaining accounting rules, and therefore more standard forms of encryption may be suitable to ensure privacy. Such a use case example may be a KYC-focused or messaging based blockchain.

File System Architecture

Many applications require the exchange of large transaction payloads, such as documents or KYC information, or a high volume of smaller payloads in the case of digital currency or payments. This can create heavy bandwidth usage and data storage requirements as the data is replicated on ledgers at every validating node. If all data relating to a transaction is stored on the blockchain itself, the size of the blockchain and the bandwidth required to share the data between all nodes may become a considerable limitation. This problem may be addressed by storing part or all of a transaction payload on a shared file system, and including a hash pointer of the stored data in the blockchain transaction. This ensures that the data is tamper evident and can be stored and accessed efficiently without unnecessary replication across the blockchain network. This greatly decreases the consumption of bandwidth and storage, and increases scalability. The choice of file system type and configuration will also impact the capability of the platform to process data, and so should be considered carefully.

Any blockchain platform which is expected to run for a long period of time will likely require some form of regular archiving of historical transaction data to keep the size of the blockchain data to a manageable size. The storage of archived data should be designed in such a way as to maximize the security and integrity of the data, but to store it with a replication factor much lower than the number of nodes holding copies of the blockchain which is inefficient in terms of balancing storage space against integrity. Sharding techniques will be useful in this scenario.

“Smart Contract” Implementation

Many blockchain platforms allow for the implementation of “smart contracts”. Each platform may provide a different architecture for the execution of smart contract code, with varying advantages/ disadvantages and abilities. Some of these architectures require more resources for execution than others. Each call to run code in a smart contract usually involves the execution of the code on multiple validators and then consensus is reached on the output of each of those individual instances. This adds latency and additional messaging overhead which may limit scalability of the network depending on the usage of smart contracts.

Deployments for Scalability

Any blockchain implementation may have a combination of factors from each of the above mentioned sources that makes the scalability of the blockchain highly dependent on its specific architecture and application. There is often a compromise between security, privacy, functionality, risk, and scalability which must be taken into consideration when designing the appropriate architecture of a platform.

The decentralized and distributed aspects of blockchain technology mean that the throughput and processing capability are not necessarily directly correlated to the number of processors or size of the network. The opposite is often true, where beyond a certain point, additional nodes may slow down the overall throughput of the network. However, adding additional storage and bandwidth resources will linearly increase the overall data capacity of a network. The cost of these additional resources must be weighed against the requirement for scaling. Today's cloud-based commoditization of computing resources may present an optimal solution for making the resources available to a blockchain scalable in both directions, in near real-time, to accommodate fluctuating demands on the network.

The capabilities and scalability of many proprietary and open source blockchain platforms that may be suitable for permissioned implementations remains to be extensively tested and independently verified. Most are still in active development with constantly evolving abilities, so it remains difficult to quantify the scalability of available platforms in their current state. It is possible to customize and configure blockchain platforms to improve scalability and balance other requirements as necessary, for specific use cases.

Chapter 5

A Prospective Roadmap for the Adoption of BCT to Banking and Finance in India

HAVING had a good understanding of the various aspects around the blockchain technology including – the sound basis underlying the technology, the advantages to be had by its adoption, the variety of its applications that are being explored around the globe, security, privacy and scalability concerns and potential countermeasures, we recommend that the time is ripe for its adoption in India.

The use cases of blockchain can broadly be classified into information sharing based and digital currency based applications. The set of use cases of the first category have ready applicability in BFSI Sector. These use cases help in bringing disparate entities on a common information sharing platform for deriving mutual benefits, while protecting their security privacy concerns. The information is maintained in a distributed fashion, mitigating the inherent delays resulting from the currently centralized systems.

A suggested roadmap for the adoption of BCT to Indian banking is as follows:

Intra-bank

Banks may setup a private blockchain for their internal purposes. This not only helps them to train human resources in the technology, but also benefits by enabling efficient asset management, opportunities for cross-selling, etc.

Interbank

Proof-of-Concept implementation and testing may be carried out in the following order of increasing application complexity – mainly because of the number of stakeholders involved in the transaction.

Centralized KYC: Secure, distributed databases of client information shared between institutions helps reduce duplicative efforts in customer onboarding. Secure codification of account details could enable greater transparency, efficiency in transaction surveillance and simplifies audit procedures.

Cross-Border Payments: BCT enables real-time settlement while reducing liquidity and operational costs. Transparent and immutable data on BCT reduces fraudulent transactions. Smart contracts eliminate operational errors by capturing obligations among FIs to ensure that appropriate funds are exchanged. BCT allows direct interaction between sender and beneficiary banks, and enables low value transactions due to reduction in overall costs.

Syndication of Loans: Underwriting activities can be automated, leveraging financial details stored on the distributed ledger. KYC requirements can also be automatically enforced in real-time. BCT can provide a global cost reduction opportunity within the process execution and settlement sub-processes of syndicated loans.

Trade Finance: BCT usage for trade finance enables automation of LC creation, development of real-time tools for enforcing AML and customs activities, and associated cost savings.

Capital Markets: BCT brings the following advantages in the clearing and settlement processes – reducing or eliminating trade errors, streamlining back office functions, and shortening settlement times. ASX (Australian Securities Exchange) has been working on a blockchain based test-bed to be a potential replacement for CHESS.

Further areas where BCT can be applied advantageously in BFSI sector would be supply chain finance, bill discounting, monitoring of consortium accounts, servicing of securities and mandate management system.

Central Bank

In a bid to evolve towards a cashless society, many central banks around the globe including Canada, England, Sweden, and Netherlands have started exploring the use of BCT for digitizing their currency, and many more are converging to the idea. From a technological perspective, we feel that BCT has matured enough and there is sufficient awareness among the stakeholders which makes this an appropriate time for initiating suitable efforts towards digitizing the Indian Rupee through BCT.

Annexure

Blockchain Application to Trade Finance - PoC

A Proof-of-Concept (PoC) was structured and customized to facilitate the feasibility analysis of blockchain technology for Indian banking and finance sector with two use cases that highlight banking and consumer interaction: Domestic Trade Finance with a sight letter of credit and 'Enhanced Information' payments (EIP). A scaled down version of a production network was simulated for the PoC to enable the analysis of the work-flow, authentication, performance baseline, and privacy of the blockchain implementation.

Architecture

The architecture for the PoC required setting up a blockchain network that simulated 5 banks along with a regulated clearing authority for both use cases. Hyperledger Fabric is used as the underlying platform with the network having been configured and deployed on a cloud environment. Banks are represented on the platform with individual validating peers and associated application servers, while the clearing authority has a clearing peer and a clearing server. The purpose of the application servers is to serve the interfaces to the users and the blockchain, and perform any required business logic for the use cases (file encryption, storage, retrieval, event listening etc.).

The file storage component is structured in a manner whereby large data files can be stored in a shared environment securely. The file storage is distributed and replicated, and is analogous to using HDFS.

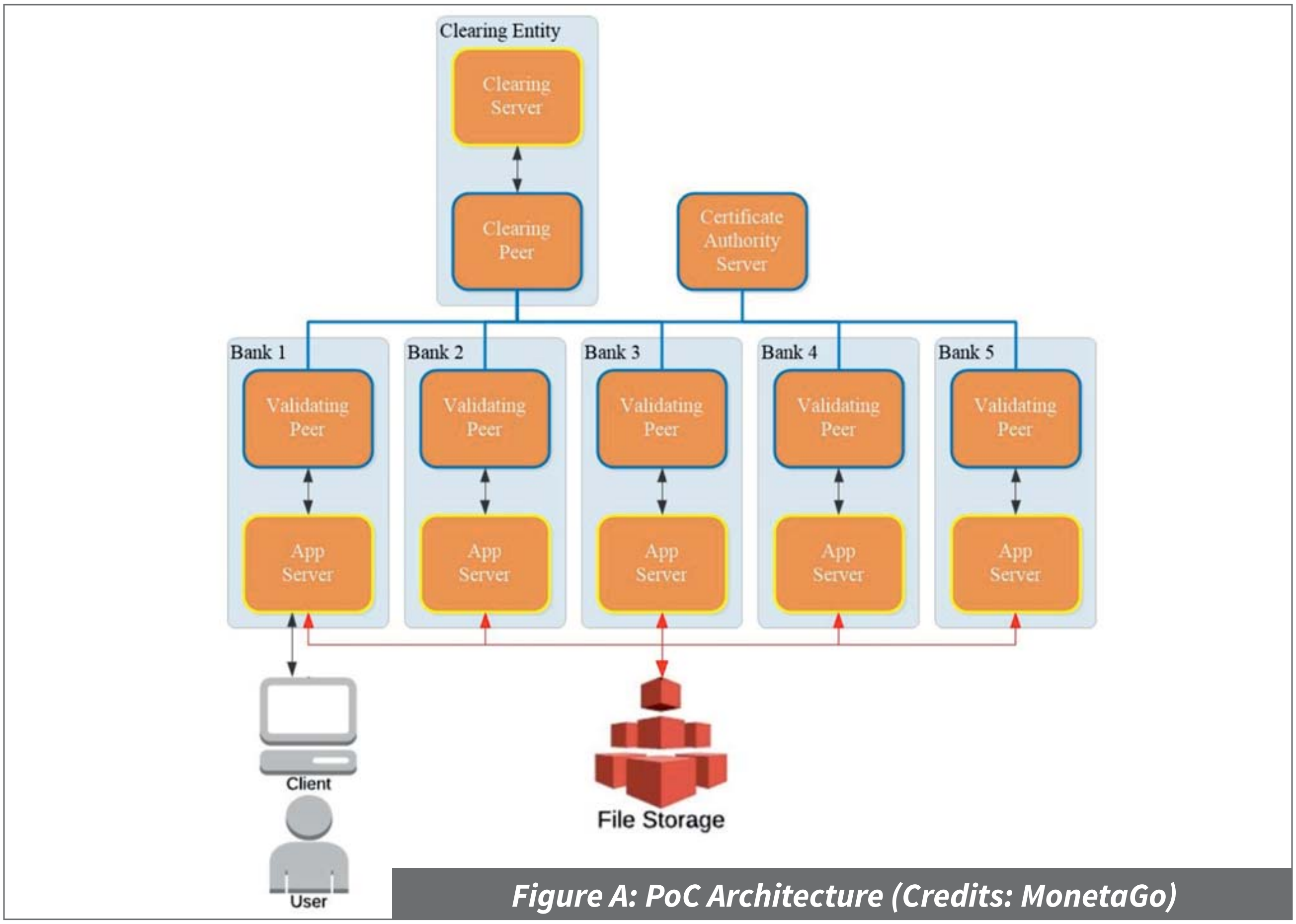


Figure A: PoC Architecture (Credits: MonetaGo)

Specifications

Hardware

- Validating peers – 8 Xeon cores, 32GB RAM dedicated servers
- Application Servers – 4 Xeon cores, 16GB RAM dedicated servers
- Certificate Authority Server - 4 Xeon cores, 16GB RAM dedicated server.

Software

- OS - Ubuntu 14.04
- Validating peers – Hyperledger Fabric 0.6.1 preview
- Application Servers – Node JS, React & Redux with Fabric NodeSDK.

Hyperledger Fabric & Chaincode

Hyperledger Fabric 0.6.1 is used as the blockchain platform to maintain the distributed ledger and run the chaincode. Each use case has its own chaincode, transaction type and ledger. The validating peers representing each of the banks run the Fabric peer service which executes chaincode, broadcasts and receives any resulting state change to the ledger, reaches consensus on the state changes through a standardized PBFT algorithm, and records state changes to the local ledger. Each validating peer and user of the validating peers (the banks) must register with the certificate authority server to gain access to the network and submit transactions. The certificate authority server runs the Fabric 'member services' service. This mechanism makes it a 'permissioned' network.

The chaincode provides the methods by which the state of the ledger is changed or queried. Any action that results in a change of state to the ledger must be called with an 'Invoke' function call. Any action that simply returns information from the ledger without resulting in a state change is called with a 'Query' function call. The chaincode allows for authentication of the caller to verify if the caller is authorized to use a specific function. Using this mechanism, the chaincode can control access to the information stored in the ledger. In the case of the EIPS and Sight LC chaincode, only parties that have been named on the transaction may gain visibility into the contents, maintaining the privacy of the parties involved. For EIPS, the remitting bank, receiving bank and clearer may view the transaction contents, and for the sight LC the buyer's bank, seller's bank and clearer may view the transaction contents. Any external party attempting to query the transaction will have its call rejected. The ledger data is also encrypted to stop external parties from gaining access to the raw data stored on it. Certificates issued by the certificate authority (member services) are used for authenticating a user in a transaction.

Application Servers

Hyperledger Fabric peers do not provide many tools beyond those described above. Most tasks are performed by the application servers. The application logic must be managed by an application that interacts with the Fabric peers to process the workflow of a transaction. The application server primarily provides the interface to the users of the blockchain network. The chaincode simply defines the rules of a transaction.

The application servers initiate new transactions, listen to new events and react to those events appropriately. In the case of EIPS and the sight LC they also handle the file data that is associated with a transaction, as only the hash of the files is kept 'on chain'. The files are uploaded to the application server, encrypted, hashed and stored on a shared distributed file system. The hash of the file is stored in a field in the blockchain transaction. When file retrieval is required, the application server will fetch the file, rehash it to compare with the original hash stored in the transaction to ensure it has not been tampered with, decrypt it and present it to the user. Application servers must also deal with the cryptographic key management for file encryption.

One or multiple clearing servers may be charged with communicating transactions to an external clearing organization at the appropriate times for real-world settlement of any monetary exchange in the transaction.

Use Cases

Domestic Trade Finance Letter of Credit

The sight letter of credit (LC) use case highlights the ability of the blockchain platform to leverage chaincode to implement any complex workflow with a shared document repository, automatic settlement and recording of full transaction history on a single system. Simple user interfaces have been built for demonstration and to allow manual execution of review and approval actions with the transaction running through multiple states. UIs have been provided for:

- The buyer to initiate an LC application after a purchase has been agreed
- The buyer's bank to review, process the application and attach the approved LC document
- The seller's bank to review the LC
- The seller to upload and attach shipping documentation after acceptance of the LC and shipping of the goods
- The clearer to process settlements at the appropriate time in the transaction.

Access to the transaction details and the associated documents is restricted to the counterparties involved. A full and real-time transaction history is available to counterparties with all associated documents securely stored and encrypted.

Below is a simplified workflow diagram of the LC use case.

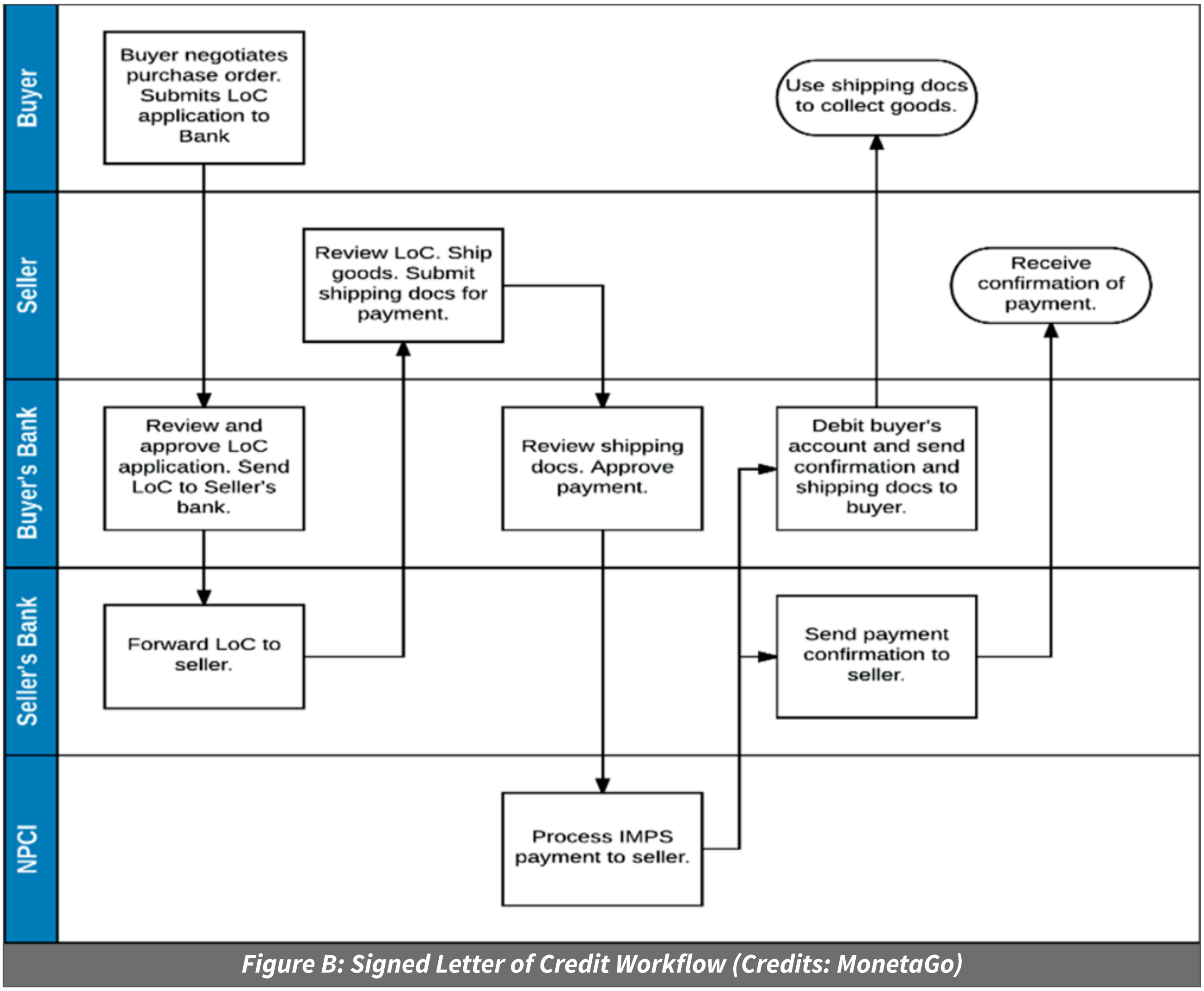
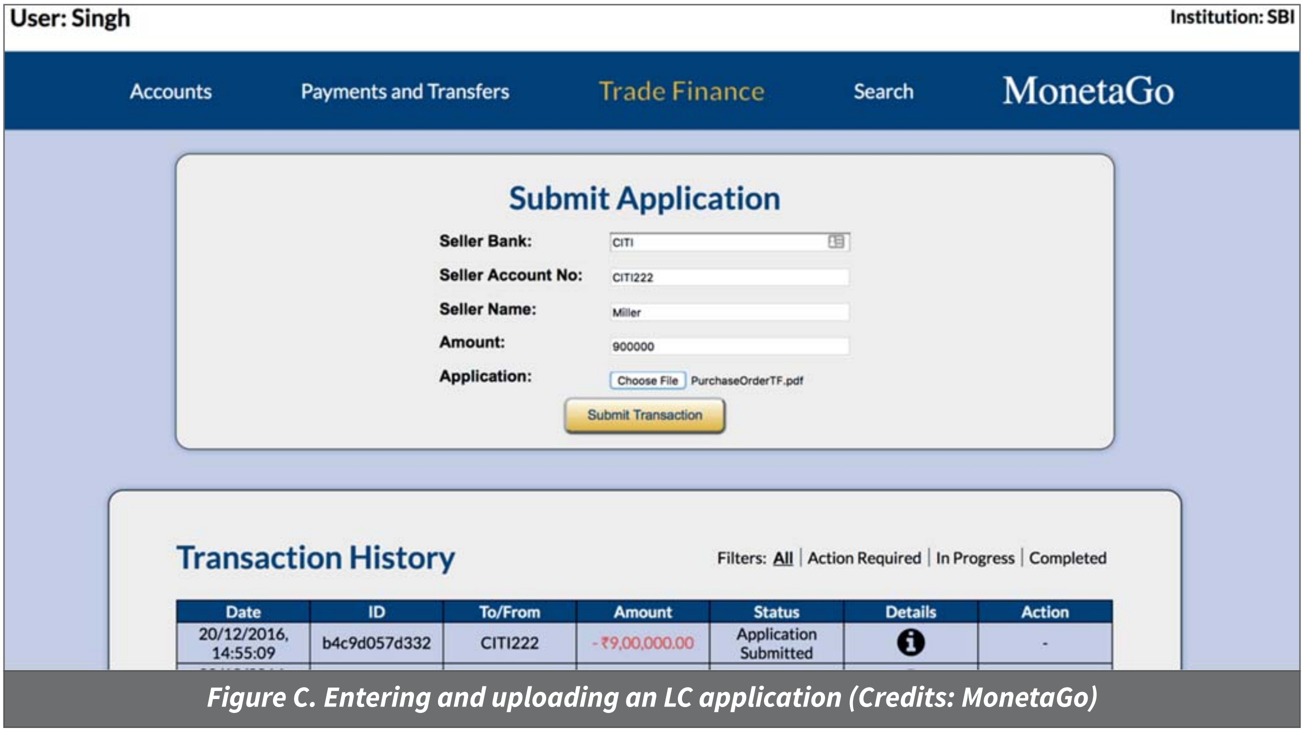

Buyer
Seller
Buyer's Bank
Seller's Bank
NPCI
Buyer negotiates purchase order. Submits LoC application to Bank
Use shipping docs to collect goods.
Review LoC. Ship goods. Submit shipping docs for payment.
Receive confirmation of payment.
Review and approve LoC application. Send LoC to Seller's bank.
Review shipping docs. Approve payment.
Debit buyer's account and send confirmation and shipping docs to buyer.
Forward LoC to seller.
Send payment confirmation to seller.
Process IMPS payment to seller.

Figure B: Signed Letter of Credit Workflow (Credits: MonetaGo)

Screenshots from Live Demonstration of Domestic Trade Finance PoC



User: Singh

Institution: SBI

Submit Application

Seller Bank: CITI

Seller Account No: CITI222

Seller Name: Miller

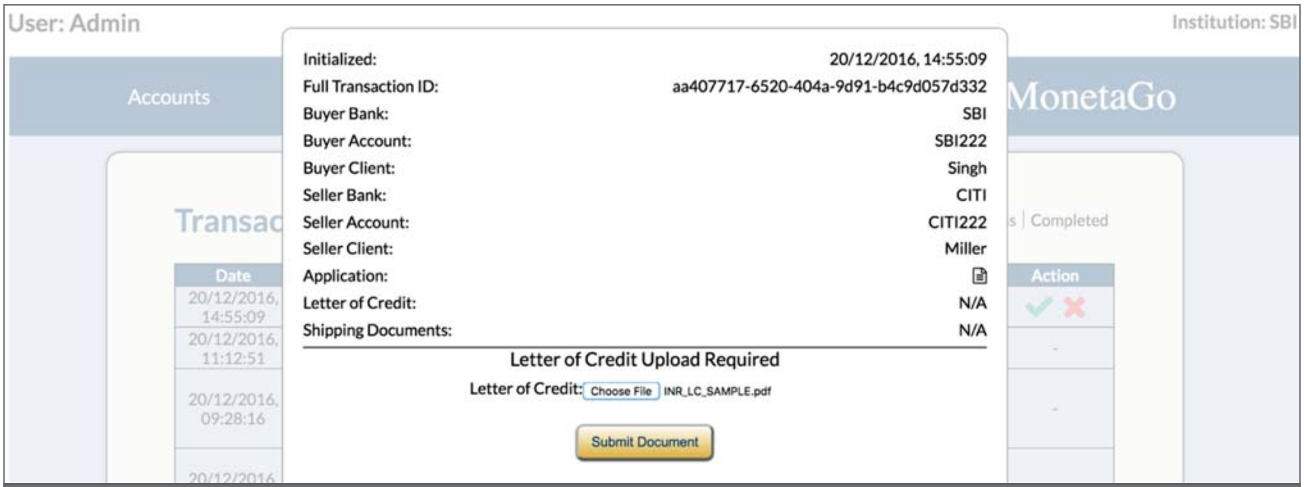
Amount: 900000

Application: PurchaseOrderTF.pdf

Transaction History

Date	ID	To/From	Amount	Status	Details	Action
20/12/2016, 14:55:09	b4c9d057d332	CITI222	- ₹9,00,000.00	Application Submitted	ⓘ	-

Figure C. Entering and uploading an LC application (Credits: MonetaGo)



User: Admin

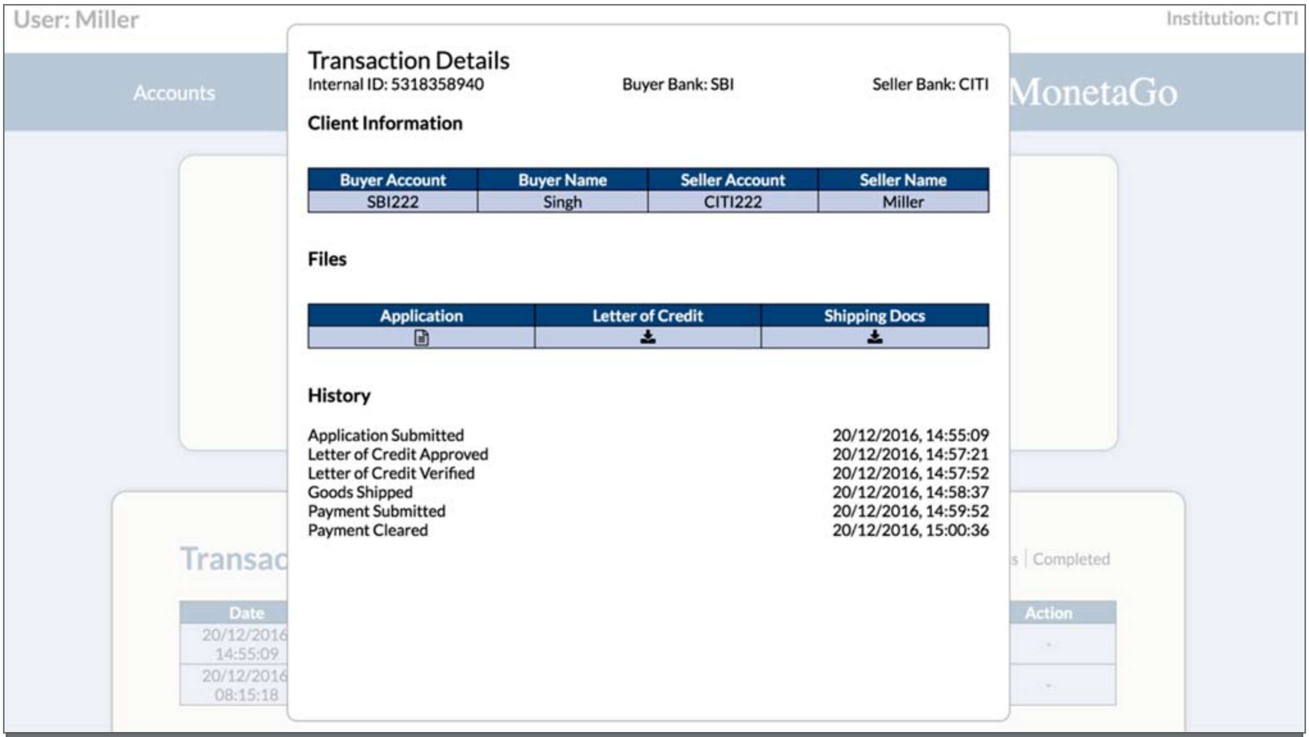
Institution: SBI

Initialized:	20/12/2016, 14:55:09
Full Transaction ID:	aa407717-6520-404a-9d91-b4c9d057d332
Buyer Bank:	SBI
Buyer Account:	SBI222
Buyer Client:	Singh
Seller Bank:	CITI
Seller Account:	CITI222
Seller Client:	Miller
Application:	🗎
Letter of Credit:	N/A
Shipping Documents:	N/A

Letter of Credit Upload Required

Letter of Credit: INR_LC_SAMPLE.pdf

Figure D. After approval of the application, the letter of credit is attached to the transaction (Credits: MonetaGo)



User: Miller

Institution: CITI

Accounts

MonetaGo

Transaction Details

Internal ID: 5318358940 Buyer Bank: SBI Seller Bank: CITI

Client Information

Buyer Account	Buyer Name	Seller Account	Seller Name
SBI222	Singh	CITI222	Miller

Files

Application	Letter of Credit	Shipping Docs
🗎	⤓	⤓

History

Application Submitted	20/12/2016, 14:55:09
Letter of Credit Approved	20/12/2016, 14:57:21
Letter of Credit Verified	20/12/2016, 14:57:52
Goods Shipped	20/12/2016, 14:58:37
Payment Submitted	20/12/2016, 14:59:52
Payment Cleared	20/12/2016, 15:00:36

Transac

s | Completed

Date	Action
20/12/2016 14:55:09	-
20/12/2016 08:15:18	-

Figure E. Completion of transaction. Full history of the transaction recorded with all associated documentation. (Credits: MonetaGo)

Enhanced Information Payment

Supplementing data on a payment provides valuable analytics for banking institutions. In both commercial and retail banking, providing rich data directly associated with a payment can provide streamlined processes (i.e. automated reconciliations for net settlements of multiple invoices in wholesale banking, referred to as information settlement), KYC (i.e. linking key regulatory documents associated with an individual to his payment history) and many other useful cases where any kind of document may be associated with payment (pay slips, contracts, invoices, etc.).

The enhanced data use case facilitates a file upload that will be performed during the payment transaction. The sender will upload the file along with the payment information. The file is encrypted and a hash is generated on the encrypted data. The encrypted file is stored in a shared distributed file system with the hash pointer being stored on the blockchain transaction. The hash pointer allows for the transaction to stay "light" on the blockchain and provides high throughput as the file data is stored outside of the blockchain ledger.

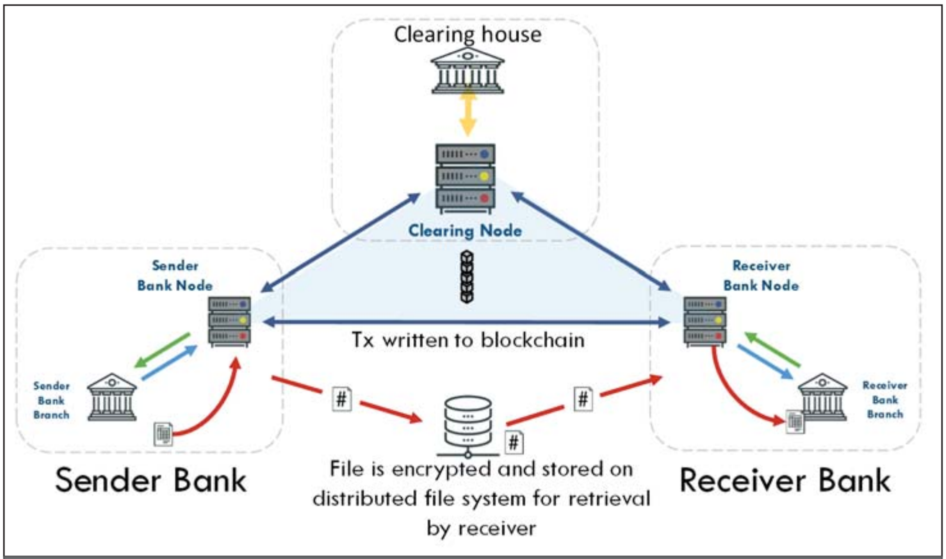


Figure F: MonetaGo's Enhanced Information Payments

Enhanced Information Payments can be used as the foundation for many more complex use cases such as the domestic trade finance example, where a transaction is processed with associated documentation, and is extensible to many more use cases.

PoC Validation and Experience

The PoC provided a good overview of the workings of the Blockchain eco-system demonstrating the following key aspects:

- Complete transparency of various events triggered by various counter-parties
- Immutability/Tamper-Evidence
- Automated flow triggered by the occurrence of specific events.

The PoC handled a simplified business workflow with IMPS providing the payment backbone, that can be easily extended to incorporate additional validation/flow components as part of the chain code. The interfaces were user-friendly and the process appears to provide a handle on the audit trail of all the events. It demonstrated the possibility of integrating payment information with payment initiation which has been a key requirement from the corporate/retail users alike.

Features to be explored further

During the PoC, the focus was only on validating the business workflow and the system's ease-of-use. Scalability and security aspects need to be studied in detail.

Hyperledger Fabric version 0.6 was used for the PoC. In this version, each server participating in the blockchain network performs all the required tasks of validating, consenting, committing and ordering, which introduces a barrier to scalability. By separating those roles in the new architecture, latency and networking overhead is greatly reduced in large networks, as fewer servers can be designated to each task whilst still maintaining sufficient security and resiliency for the network. Also, the implementation of privacy features is incomplete, increasing the possibility of information leakage between participants. Hyperledger is developing version 1.0 to address the above shortcomings.

Summary

Overall, the PoC provided a good demonstration of the use-cases and helped to broaden the understanding of the technology and its potential to other real-life applications.

Participants of PoC and their roles

S No.	Participant	Role
1	IDRBT	Coordinator, technical inputs, review
2	NPCI	Inputs on payments component
3	Banks (SBI, PNB, HDFC, Citi Bank, Deutsche Bank)	Inputs on business processes, and test scenarios; and review
4	MonetaGo	Implementation of the technical platform

BLOCKCHAIN WORKING GROUP

Mentor

DR. A. S. RAMASASTRI, DIRECTOR, IDRBT

Members

- **Shri Prasant K. Seth**
  Reserve Bank of India
- **Shri Supriya Bhattacharyi**
  Reserve Bank of India
- **Shri Jagadeesh Kumar**
  Reserve Bank of India
- **Shri Dilip Asbe**
  National Payment Corporation of India
- **Shri R. Vishweshwaran**
  National Payment Corporation of India
- **Shri Praveen Mata**
  The Clearing Corporation of India Ltd.
- **Shri K. Ramachandran**
  Indian Banks' Association
- **Shri Ajay Lande**
  Axis Bank
- **Shri Harshit Pagariya**
  Bank of Baroda
- **Shri Munish Bansal**
  Citi Bank
- **Shri N.K. Subramaniyam**
  Citi Bank
- **Shri Sandeep Menon**
  Citi Bank
- **Shri Ram Kumar**
  Deutsche Bank
- **Shri Deepak K Mudalgikar**
  HDFC Bank
- **Shri Maheshwara Yaddanapudi**
  ICICI Bank
- **Shri Abhijit Singh**
  ICICI Bank
- **Shri Rakesh Kumar**
  Punjab National Bank
- **Shri Charanjeet Singh Arora**
  Punjab National Bank
- **Shri Dhananjay Aravind Tambe**
  State Bank of India
- **Shri Sudin Baraokar**
  State Bank of India
- **Shri Shankar Lakshman**
  Deloitte
- **Shri Nitin Mahajan**
  Deloitte
- **Dr. Dilip Krishnaswamy**
  IBM Research
- **Shri Deepak Hoshing**
  Infosys
- **Shri Savvas Mavridis**
  MonetaGo
- **Shri B. Taylor**
  MonetaGo
- **Shri Atul Khekade**
  MonetaGo
- **Shri K. Srinivasan**
  Tata Consultancy Services
- **Shri Sitaram Chamarty**
  Tata Consultancy Services
- **Dr. Sushmita Ruj**
  ISI Kolkata
- **Dr. Sourav Sen Gupta**
  ISI Kolkata

Coordinators

Dr. M. V. Sivakumaran, IDRBT

Dr. N. V. Narendra Kumar, IDRBT

Dr. S. Nagesh Bhattu, IDRBT

IDRBT
Explore, Enable, Excel

Published by:

Institute for Development and Research in Banking Technology
(Established by Reserve Bank of India)

Castle Hills, Road No. 1, Masab Tank, Hyderabad - 500 057, India.
EPABX : +91 - 40 - 2329 4999, Fax : +91 - 40 - 23535157
Web : www.idrbt.ac.in E-mail : publisher@idrbt.ac.in