LTI

Let's Solve

Whitepaper

How Blockchain is Transforming Capital Market

Author : Dyuti Bhushan Bhattacharyya

A Larsen & Toubro Group Company

Contents

Executive Summary

Blockchain technology has become a much-talked-about topic in recent times. It is predicted to have a huge impact on the way financial institutions interact with each other, and how trades are processed and settled. The technology, with its peer-to-peer interaction in the blockchain network and cryptographic security to establish trust, is expected to settle transactions in a faster and safer manner. The regulatory bodies can have oversight on transactions in almost real-time, and the auditing team can gain better insights with clear visibility of the audit trail.

In addition, blockchain technology allows for smart contracts, which are computer programs that get executed under certain events, and can make automated payments and conduct validity checks. To make early inroads, several financial institutions of repute and startups have begun investing to explore the potential of this new technology. They forecast that blockchain will be critical to a firm's future, since it is going to transform how the industry operates.

However, the technology is still at an evolving stage, and has several challenges to overcome before it becomes feasible and gains widespread acceptance. Blockchain has the potential, but to what extent and how this evolving technology would be adapted to improve existing processes within capital market infrastructure, is still a matter of much discussion and debate. The current paper explores the areas of the capital market which can embrace it, and the various ongoing pilot projects that attempt to understand the benefits and limitations of blockchain.

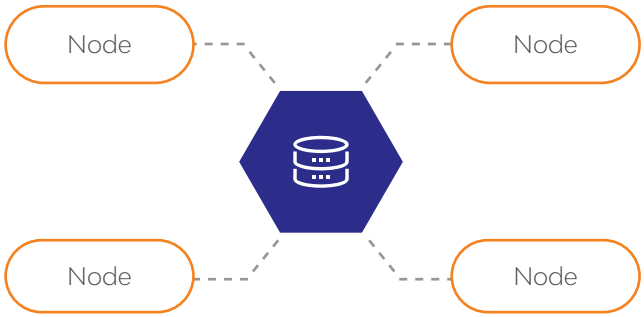
Background

If the internet was a disruptive technology of the 1990s, then blockchain, the underlying technology for cryptocurrencies such as Bitcoin, is the next big thing, and is expected to revolutionize transactions done over the internet. Blockchain is based on a peer-to-peer distributed ledger system, with mutual consensus among the participating nodes or members of the network, and involving smart contract, cryptography, and advances in the internet and computing power. The distributed ledger system, which offers a decentralized recording of transactions in almost real time, facilitates value transfer without the need of a trusted third party or centralized monitoring agency. In this paper, we will look into the necessary building blocks of blockchain, how the technology works, and where blockchain could be applied to capital market systems.

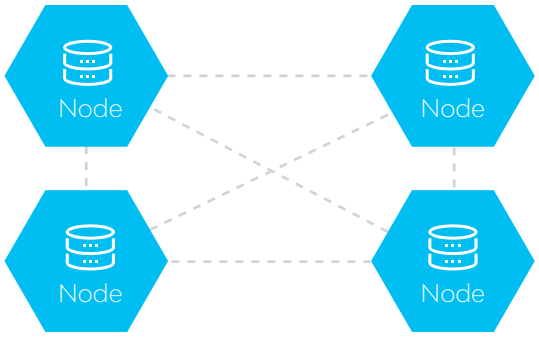
The traditional centralized model that exists today is time-tested. It has long been relied upon for settling trades with strict regulatory oversight infrastructure in place, to ensure the safety of the trade being processed. However, it suffers from various limitations such as multiple versions of the information being maintained in isolated systems and their evolution over a number of decades, making those systems very complex in nature. This is where blockchain technology steps in, promising to maintain only one version of the information, thereby eliminating reconciliation to provide better security, with its digitally signed transactions and almost instantaneous trade settlement with peer-to-peer technology.

In a traditional centralized network, operational control is maintained from a single location and transactions are verified by a central authority. In a distributed ledger system, each node or participant in the network has its own copy of the ledger, and validates a transaction before it is added to the blockchain database. This database is composed of blocks which contain historical transaction or digital ownership data. In a capital market transaction, the traditional model has intermediary in-betweens with their own database, whereas the blockchain structure will have no intermediaries and a distributed ledger system on a peer-to-peer basis, with the exchange between parties happening in almost real time.

Digital ledger can be coded to hold any value such as title, intellectual property, or any type of financial instrument or transactions. It also records business logic that has been agreed to between parties, for financial transactions. This digital ledger can be distributed at the network nodes, either across 'permissionless' (public) or 'permissioned' (private) networks. This ledger represents an incorruptible truth that can be accessed without compromising personal identity, because of the mass collaboration among the network nodes, which in turn validates any transactions before it is added to a block.



Centralized Ledger Network



De-centralized Ledger Network

Building Blocks of Blockchain

The main component of the blockchain technology is its distributed ledger, with its peer-to-peer architecture, decentralized consensus mechanism, and cryptographic digital signature. Below are the brief explanations of some of the important aspects of a blockchain.

Distributed Ledger

A blockchain is a distributed ledger, wherein data is stored independently by each participant of the distributed network. This occurs without any interference by any central authority, and uses a consensus-based check to verify a transaction. Data is stored in the ledger in blocks, and each block has a reference to the previous block.

Blockchain

The blockchain data structure is a list of transaction blocks, wherein each block is added to its existing chain only after the decentralized consensus mechanism. Each block will have a link to its preceding block, all the way to the genesis block.

Nodes

Nodes are the participants in a blockchain network. Nodes can be 'full nodes' — which can store the complete blockchain ledger locally, validate and block data. They can also be 'partial nodes', with limited or restricted permissions on the network.

Permissioned or Private

A permissioned system is one which manages blockchain in a private network having selected participants, whose access to the blockchain is tightly controlled, and their identities are validated through some sort of KYB or KYC procedures. Such private blockchain is preferred by financial institutions to have complete control or oversight over the transactions being processed. In contrast, a permissionless system, or public blockchain, is an uncontrolled network, in which anyone with any identity can join the network.

Validation/Consensus Mechanism

Once a new transaction is broadcasted via a message to the blockchain network, it gets added to a temporary pool of unverified transactions. Each node will validate this transaction against a list of criteria to mark them as valid. These are then aggregated into a block by each node. Once a specific member (or node) in the network is successful in validating the block (or proof of work), it broadcasts the validated block to other validators in the network, to update and change their local copies of the ledger, accordingly. Validators need to verify that the transition initiator possesses the asset that would be transferred according to his/her most recent information.

Smart Contracts

Smart contracts are self-executing contractual clauses that are stored on the blockchain. These allow transactions between parties based on predefined rules, without the inefficiency or risk of intervention created by an intermediary counter-party agent. A smart contract can be implemented for a number of accounts of different types, and an exchange of assets takes place as soon as an event triggers the application with these terms. For example, a smart contract can provide for automated payment of dividend and interest, and collateral payments on the occurrence of certain events. These events can be the receiving of a margin call based on an agreement clause related to such payments. As smart contracts are written or coded in the ledger itself, validation of their execution follows the same procedure as discussed earlier. However, it is still to be seen how smart contracts, written in programming codes, are enforced by the law and treated by various regulatory bodies.

Cryptographye

The transaction sent to a blockchain network is cryptographically encrypted, so that the content remains confidential and can only be decrypted by the recipient. For any transaction, the sender will have a randomly-generated private key, as well as a corresponding public key. The sender can now use his private key to encrypt or digitally sign the message, and send his public key to the recipient, and the recipient with his own private key can duly decrypt and read the message.

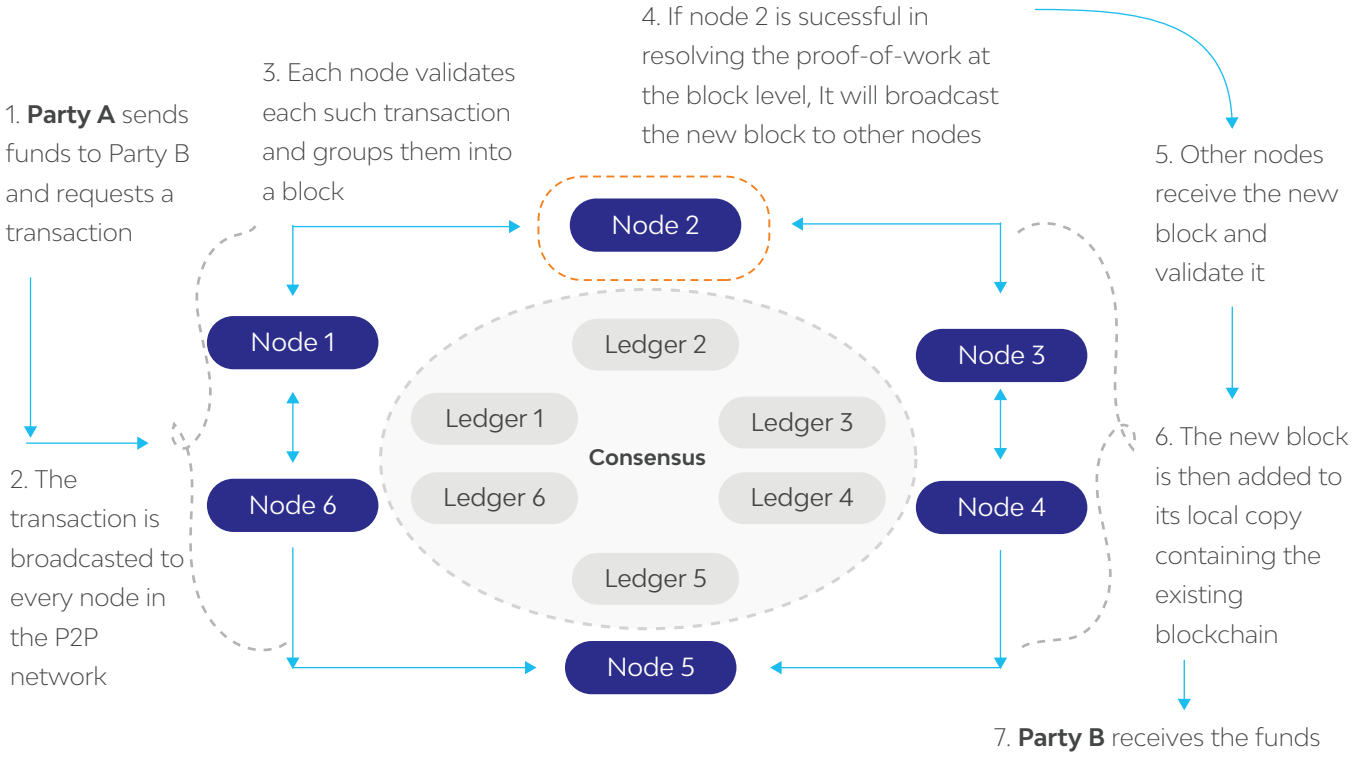
How a transaction takes place in a blockchain?

With this new technology, when a transaction is submitted in the blockchain network, the information is broadcasted to all the nodes existing in a network, be it public or private. In a private or permissioned network, only a restricted set of users have the rights to be part of this network and validate it, and only a few nodes would be restricted to do the validation.

The transaction requested is broadcasted to all the nodes in the network for validation, using some criterion. After proper validation checks, each node aggregates transactions that have occurred recently, and groups them into a block.

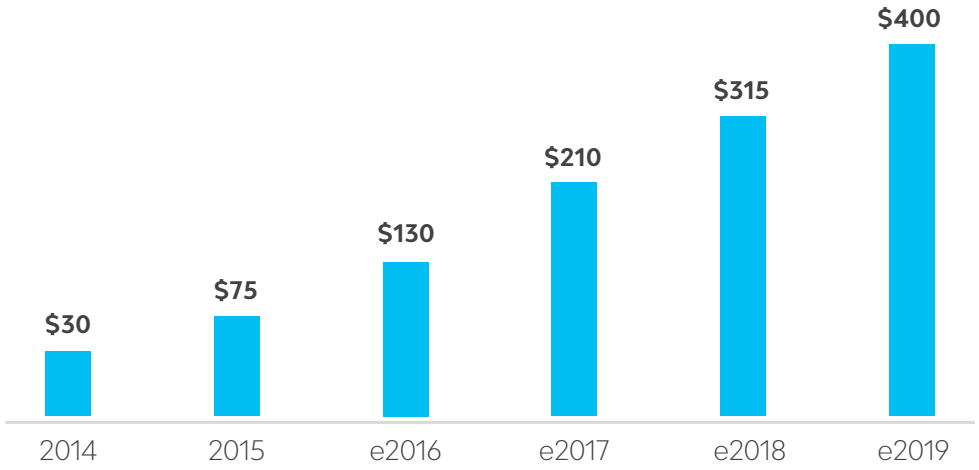
Each node, by way of brute force, tries to find a solution to a Proof of Work (PoC) algorithm, which would make the block valid. In this competition among all the nodes working to find the solution to this puzzle, once a node wins in finding the solution, it broadcasts this new block to all its peer nodes in the network. Each of these then starts working on independent validations of a new block. This ensures that only valid blocks are added to an existing chain. The digital wallet of the receiver is then updated, and the transaction is complete. Each block does not only keep record of the current transaction, but also the history of all previous transactions, starting from the original one. A block cannot be modified once it is added to the chain.

As the database in blockchain is shared, integrity of the datasets is important, and is maintained by agreement among all the participating nodes through mutual consensus verification protocol, to update their records collectively. This verification method not only safeguards against any malicious manipulation (or cyber risk), but also ensures that no single point of failure exists.



Financial Institutions evaluating Blockchain

A number of financial institutions have already started taking interest in blockchain, and are investing heavily to explore its potential. Goldman Sachs has applied for a patent to employ its cryptographic currency on a security settlement system. A total of 42 major financial institutions, including Goldman Sachs, have joined a blockchain consortium launched in 2015 by R3 CEV, a financial technology firm. According to a study by the Aite Group (www.aitegroup.com), investments by financial institutions in exploring blockchain is expected to increase five times to USD 400 million by 2019, as compared to 2015.



Estimated Capital Market Spending in Blockchain (in US$ million)

Source: Aite Group

Stock Markets embracing Blockchain

The stock exchanges are working on various projects to take advantage of blockchain architecture, in order to reduce cost and increase the speed of settlement processes. The biggest names in the industry are exploring this technology.

For example, the Australian Stock Exchange (ASX) will allow both the buyer and the seller, as participants in its peer-to-peer network, to confirm transactions, instead of settling trades via the exchange. The registered brokers in the network will record the parties involved in the transactions in their ledger, along with the number of securities sold, prices, and the time of exchange of funds and securities. The objective is to push the settlement part to the blockchain, although the price discovery will still be made in the existing centralized exchange.

Such peer-to-peer exchange will cut down on intermediaries, reduce settlement time, and operational inefficiencies involved with that. Furthermore, this means that there will be no need for a clearing house, custodians, auditors for verification of trades, and require minimal paperwork, leading to huge savings. Settlement can be almost instantaneous, when compared to the existing T+3 settlement cycle.

The London Stock Exchange (LSE), which is working aggressively on blockchain, formed a working group in 2015 to analyze how blockchain technology can be used in clearance and settlement of trades, and their reporting in the European market. The working group, named as 'Post Trade Distributed Ledger Working Group', includes key players such as UBS, CME Group, Societe Generale, LCH.-Clearnet, and Euroclear.

On the other hand, Deutsche Bundesbank and Deutsche Börse were working on a prototype to study if such blockchain technology can be applied for financial transactions, and for a better understanding of it. Recently, they presented the prototype, and aim to analyze the technical performance and its scalability in the coming months.

The Japanese Stock Exchange, along with IBM, is working on a PoC to investigate how blockchain can be used for trading with low-volume transactions, and after running two separate trials, has concluded that the digital ledger indeed has the potential to transform the capital market's structure.

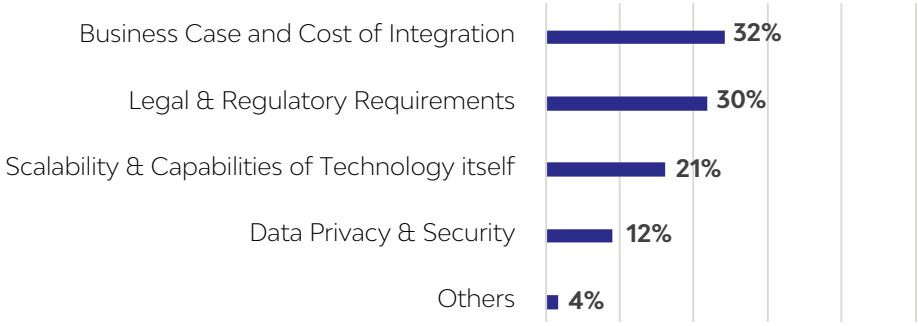
Stock Exchange	Experimentation with Blockchain
NASDAQ	In 2015, Nasdaq unveiled its Nasdaq Linq blockchain ledger technology, used to successfully complete and record private securities transactions for Chain.com — the inaugural Nasdaq Linq client. In May 2017, Nasdaq, along with Citi Treasury and Trade Solutions, announced a new integrated payment solution that enables direct payment processing and automates reconciliation by using a distributed ledger to record and transmit payment instructions. The partnership between Citi and Nasdaq leverages Chain's platform, and draws on core competencies from industry leaders who are at the forefront of innovation in the global financial sector. This integration can allow businesses such as the Nasdaq Private Market to address challenges of liquidity in private securities, by streamlining payment transactions between multiple parties.
ASX	In 2017, the Australian Stock Exchange (ASX) selected US-based blockchain startup Digital Asset Holdings, LLC to develop distributed ledger-based solutions for clearing and settling trades. It made an investment of USD 14.9 million to acquire a 5% equity interest in Digital Asset, which was later raised to 8.5% through additional investments. ASX's project timeline mentioned end-2017 as the key decision point to implement Digital Ledger Technology (DLT) as the alternative technology to replace Clearing House Electronic Subregister System (CHESS).
JPX	In 2016, IBM and Japan Exchange Group (JPX) announced an agreement to test the potential of blockchain technology to be used in trading in low transaction markets.
Deutsche Borse	: In November 2016, Deutsche Borse and Deutsche Bundesbank presented a functioning prototype for the blockchain technology-based settlement of securities. Further development over the next few months was expected to help them "analyze the technical performance and the scalability of this kind of blockchain-based application."
LSE	The London Stock Exchange, part of the PDTL Group, is involved in ways to improve the post-trade space using blockchain.
NSE (India)	Starting early September 2016, NSE has been conducting a blockchain trial involving the country's leading banks — IDFC, Kotak Mahindra, ICICI, IndusInd, and RBL, as well as HDFC Securities. The blockchain trial was related to know-your-customer (KYC) data, enabled by blockchain startup Elemential.

(MOEX) Moscow	The Moscow Exchange (MOEX) successfully conducted e-voting for bond-holders via blockchain, at the National Settlement Depository (NSD). The pilot version was launched in 2017.
Luxembourg	The Luxembourg Stock Exchange has already introduced a blockchain security system, wherein the officially generated signature by appointed mechanism (OAM), along with document type and document URL, are stored in the blockchain.

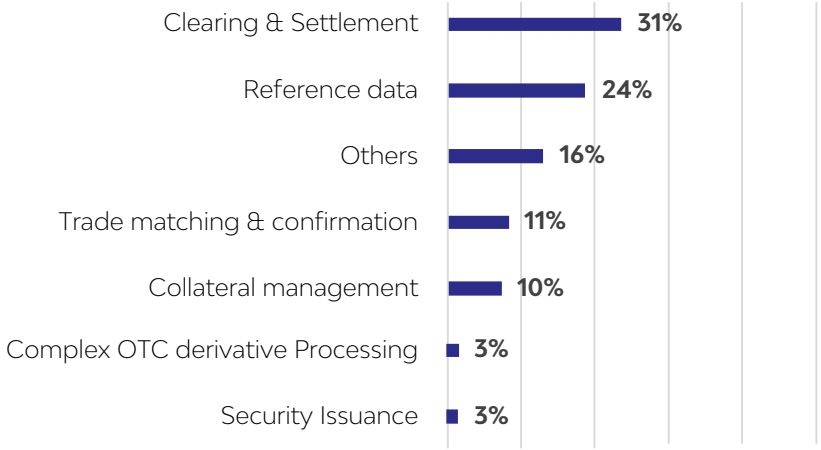
Source: Various

Back in 2016, the Depository Trust & Clearing Corporation (DTCC) held a symposium on blockchain and collected feedback from the audience poll. Some of the questions and their responses are given below, to highlight the interest that was shown on this new technology.

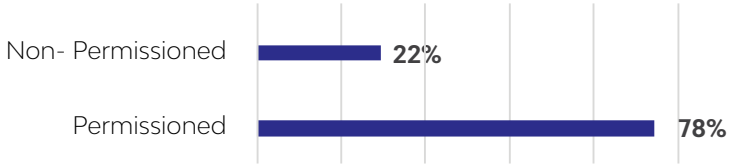
What aspects of implementing Blockchain technology do you believe present the greatest challenges?



Which Blockchain Use Case should be the Industry's highest priority?



Which governance model do you think will ultimately be used in financial services?



About 36% of the respondents believe that production-ready distributed ledger solution is likely to be adopted by the industry in another 3-4 years, whereas 27% believes the adoption to take place in another 1-2 years.

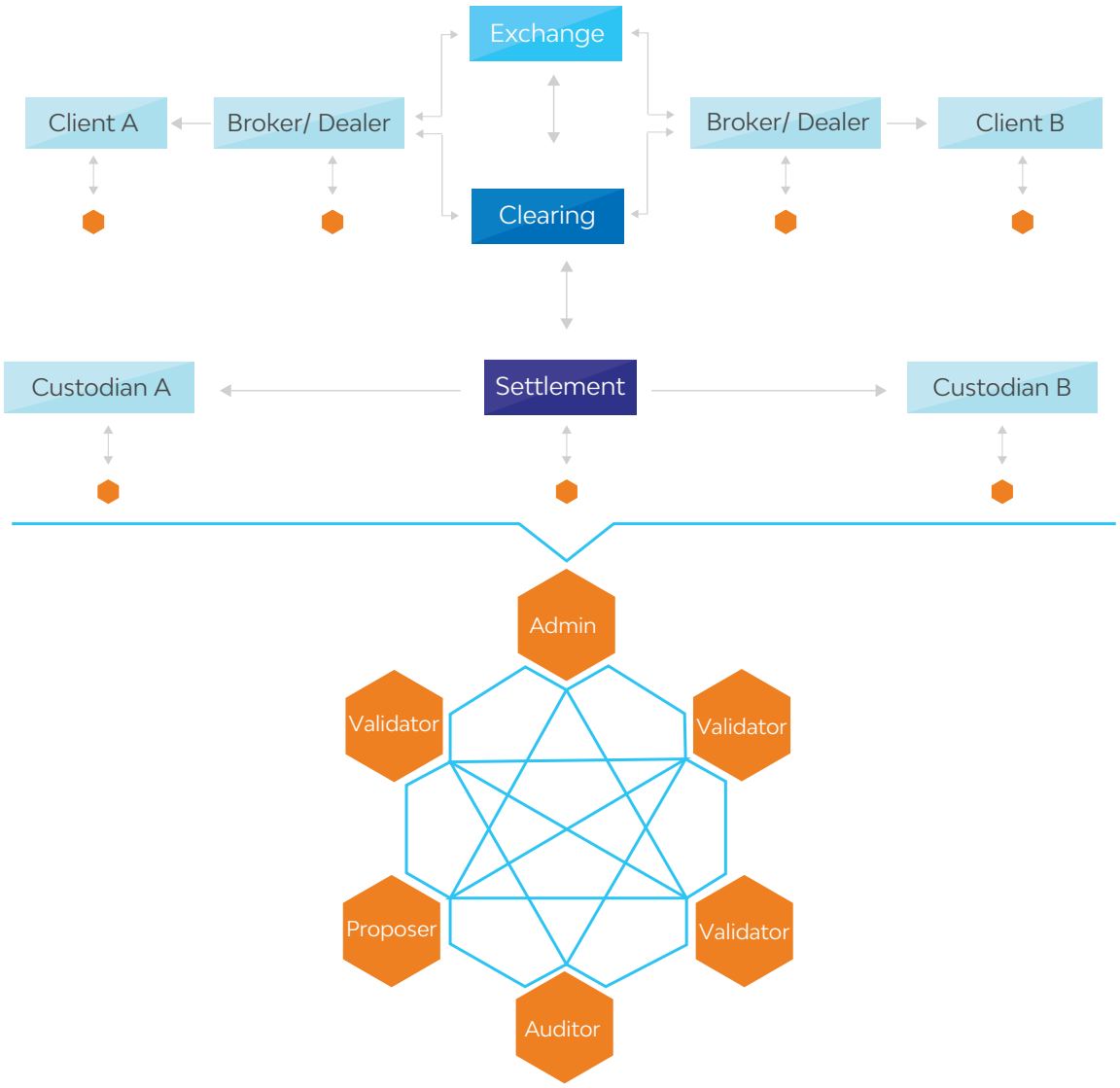
Key areas where Blockchain could be deployed

In the current model, each participant has its own dataset, and no visibility of the entire trade life cycle. This kind of fragmented data storage leads to replication of data, which in turn can be changed, added and deleted. Reconciliation of this data is necessary, as each participant has its own way of capturing and storing data, leading to a trust-less data model. Furthermore, each participant has to have reconciliation within its own structure. For example, a broker/dealer will have to reconcile data within its front-office, middle-office, and back-office datasets.

In the blockchain model, each participant acting as a node in the network maintains the same ledger to store the same sets of data. These are stored on a consensus basis, leading to trustworthy data. The distributed ledger is a permanent, immutable and verifiable record of truth that everyone can see, in this case. This eliminates the need for costly reconciliation processes among participants, and leads to faster settlement as the exchange of data is done in almost real time.

The blockchain network can be designed in a flexible manner to meet the objective of security settlements, like giving the nodes different roles or permissions. It is possible to have a few nodes with the ability to propose changes to the block, and a few nodes with the permission to validate such proposals to make the change. Specific nodes can act as auditors, which will only have an oversight and viewing capability without the permission to make any change. The admin will have the right to give access to the system, and its dispute settlement and regulatory reporting mechanism.

Current Model for an Institutional Trade



Blockchain Model for an Institutional Trade

Whereas in the blockchain model, each participant acting as a node in the network, maintains the same ledger to store the same sets of data as these are stored on a consensus basis leading to trustworthy data. Further, the distributed ledger is a permanent, immutable and verifiable record of truth that everyone can see. This eliminates the need for costly reconciliation process among the participants and leads to faster settlement as the exchange of data is done in almost real-time.

The blockchain network can be designed in a flexible manner to meet the objective of security settlement like to make the nodes to have different roles or permissions. It is possible to have few nodes to have the ability to propose changes to the block and few nodes might have the permission to validate such proposal to make the change. Some node can act as an auditor, which will only have an oversight and viewing capability without the permission to make any change. The Admin will have the right to give access to the system, dispute settlement and regulatory reporting.

Asset Classes that can bebeneficially adopted for Blockchain

Cash equity

The settlement of cash equity can be reduced to T+0 from the current T+3 settlement cycle. There will be automatic reconciliation, as all the participants/nodes will be sharing the same ledger. Similarly, the front and back offices will be relying on the same ledger, leading to increased operational efficiency. The only glitch is that such transactions will be processed in huge volumes, and the blockchain needs massive computing power to process and validate such volumes of data.

Fixed income

These trades are based on fixed contract parameters, and can hence be the ideal asset class for blockchain validation. However, fixed income securities are currently settled on a T+0 basis, and thus, adopting blockchain will not add much value in reducing the settlement cycle.

IRS, Equity Options, Futures, and Repos

Blockchain can simplify processing of the trade lifecycle, maintain one common ledger among the participants, and use smart contracts to trigger period payment(s) based on events. As the blocks made are immutable and maintain all the records from the start, an efficient audit trail can be maintained.

Exotic derivatives

Standardized terms and conditions will allow automatic validation of economic parameters and adding to a blockchain, with automatic payoff triggered by events and automated settlements. A distributed ledger will also allow transparency to other participants of verified asset holdings.

Blockchain in OTC Derivative

The use of a distributed ledger system and smart contract is likely to enhance efficiencies in trans-acting derivative products in the OTC market. The benefits of using blockchain technology can be:

1 Automating the execution of OTC agreements by using smart contracts on the blockchain network, wherein agreement terms can be implemented and confirmed without any human intervention.

2 Peer-to-peer architecture will allow parties in an OTC trade to transact directly with their counterpart, without the need of a third-party.

3 Maintaining the same ledger with both sides of the transaction increases transparency, which allows counterparties to view the data during the life cycle of the swap.

4 Regulators can access any information in real time, by using their authorized nodes in the blockchain network.

A few notable initiatives in this area include that of 2017 by Axoni, a technology firm that specializes in distributed ledger infrastructure, along with eleven other firms such as BNP Paribas, Citi, Credit Suisse, Canada Pension Plan Investment Board, Goldman Sachs, and JP Morgan. They announced the completion of a pilot test to manage equity swap transactions and related post-trade lifecycle events. In June 2017, a group of Japanese banks, including Nomura and Mizuho Financial, started testing OTC derivative contracts on a blockchain platform developed by R3.

Potential Areas in Trade Processing where Blockchain can be deployed

Reconciliation

The main benefit expected from using blockchain technology in the capital market is the reduction of intermediaries involved in processing of trades, thereby reducing costs and effort that goes in reconciling information kept at isolated legacy systems.

Trade Validation

Blockchain supports smart contracts, where rules of the contract are embedded into a code or deployed on the blockchain. The introduction of the smart contract technology could validate contractual data by entering the distributed ledger, which should make processing simpler and reduce exception correction time. The nodes in the network can monitor and detect contracts for changes of ownership and contract rules. This would enhance trade validation in terms of efficiency. The trade validation on blockchain is applicable mainly for contract-based asset trades, basic cash equities and fixed income, repurchase agreements, and swap transactions across all asset classes. As any record written to the distributed ledger is immutable, any modifications, cancellations and corrections can only be done by "reverse" transactions.

Reference Data

Reference data consists of asset or security information, calendar days, ticker symbols, client data, and so on, and is essential for processing a trade to its final settlement. Companies across the industry store reference data in their own legacy systems, resulting in highly time-consuming reconciliations with data of other participants involved in the trade. In addition, data reconciliation is necessary between internal systems within an enterprise. The common reference data can be implemented on blockchain, with its standardized validation rules among the participants in the network and auditable change history. This would allow regulators and other participants to view how the data record is being created in the ledger in real time, and which nodes validate the data creation.

Netting and Clearing

In blockchain, the question is whether it will settle trades either on a gross or net basis. Some advocate that blockchain can allow delay in trades, so these can be netted at the blockchain level, thereby reducing risk and liquidity requirements. Further, clearing to reduce settlement failure (in addition to multilateral netting) using central

counterparty for each trade could also be deployed in blockchain, through appropriate rules. To this end, several solutions are now under development.

Faster Settlement

In theory, the blockchain technology could reduce processes involved in clearing and settlement, because once a transaction is confirmed and committed to the ledger, the associated token (digital representation of an asset or any sensitive data element) is simultaneously settled in the digital wallet of the beneficial owner. The faster settlement is likely to reduce costs, and lower settlement risks.

Collateral Management

This can be embedded into blockchain in the form of smart contracts, which will contain rules to automate triggering of margin calls, and so on. As both the sender and receiver are on the same blockchain network, the movement of digital recording of assets through tokens substitute sensitive data with a non-sensitive equivalent with the ability to track asset movement, and proper design and rules allow exchange of assets for collateral purposes. This can also be extended to the distributed ledger technology.

Regulatory Reporting

As all the participants will be maintaining one version of the truth, there will be no need for costly reconciliation. Regulators will have visibility of transaction in real time and have monitoring efficiency on the activities of transacting parties. Further, the current use of disparate systems, both externally and internally, provides many bottlenecks when doing Know Your Customer (KYC) and Anti Money Laundering (AML) checks. Verification of information and repetitive information exchange between parties during client onboarding consumes much time. This is likely to be eliminated when there will one version of the truth maintained among all the participants in the blockchain.

Audit Trail

As all entries are written on the ledger, falsification of such record to conceal activity is practically impossible. In addition, as companies can write their transactions directly into a distributed ledger, it eliminates the requirement to keep separate records based on transaction receipts. Given the digitized nature of transactions, auditing of such transactions can also be done electronically, eliminating much of the manual work, and the time and cost associated with it. Another important aspect of blockchain is that each block has a reference to its previous block, thereby maintaining a full history of all transactions and providing a completely traceable audit trail.

Key Challenges

Non Reversibility

Any transaction recorded in blockchain cannot be directly modified in case of any change in contractual parameters, or any exception thrown on validation. The only way to correct the transaction is to pass another entry of the opposing type. This inability to subsequently edit the historical information in the blockchain database is a critical element of its value proposition, but might be a hurdle for trade validation.

Trade Matching and Exception Management

The current blockchain technology does not have the ability of matching in place, and how any mismatch and exception processing will be handled is still a question. Furthermore, any modification or correction to existing data cannot be done due to the non-reversibility of blockchain.

Netting of positions

As of now, Bitcoin transactions using blockchain allow settlement only on payment basis, i.e., on a gross basis and not net. This would lead to higher collateral and capital requirements, unless netting is fully implemented in blockchain. Resolution of this area is still under discussion.

Cash leg of a transaction

Although blockchain allows a security transaction to be settled in almost real time, the biggest hurdle is how to handle the cash leg of it. Digital currency does not have the support of all global central banks, and the high volatility of its value can create a major distrust among parties of a transaction. Cryptocurrency has witnessed a huge growth in the digital market, but the question is whether it would get widespread acceptance like that of fiat money. The second problem is on how to ensure that the value of such cryptocurrencies does not swing wildly, and requires the central banks to have some control over the issue of its volatility.

Operational challenges

Operational risks come into play through the adoption of new technologies. It remains to be seen how, and to what extent, the blockchain can be used to modernize existing models and legacy systems. There is also an apprehension that privacy of parties and sensitive transaction information might get compromised, as multiple copies of transaction are kept across all the nodes in a network.

Scalability

The technology must have enough scalability to deal with high transaction volumes, before it can be implemented on a mass scale. Currently, Bitcoin transactions using blockchain are used with a limited transaction volume, resulting in high processing speed. It still needs to be seen if the blockchain can maintain the high speed of processing, when it deals with high transaction volumes.

Privacy

The privacy aspect is the most important factor when one deals with public (permissionless) blockchain networks, and the open source community is working aggressively on it, to limit access to private information and transactions. This is despite the fact that blockchain networks, by the

nature of its architecture, provide better security compared to a traditional centralized model, as it does not allow tampering with data in the distributed ledger once a transaction is recorded.

Regulatory impact

New regulations are expected where blockchain technologies become an integral part of the market infrastructure. There are significant regulatory considerations, particularly around privacy protections for personal identification information. A considerable number of laws need to be reinterpreted to deal with the new way of processing trades.

Conclusion

The potential of blockchain is immense, but the question is how effectively one can adapt to it to realize its benefits in the long run. Some of the main aspects of blockchain that can have massive impact on current capital market processes include peer-to-peer exchange without any centralized monitoring authority, and consensus mechanism to validate and maintain the same ledger copy among all network participants. The technology is still at an evolving stage, and the question of security is still in the minds of many financial institutions.

Scalability is another concern, as the blockchain technology should be robust enough to deal with much larger volumes of data. Regulations and legislations are other aspects, which will require an overhaul to deal with this technology. Many start-ups are working aggressively to create prototypes, in order to better understand blockchain's limitations and potentials, before taking the dive. To infer, blockchain has the potential and is attracting a lot of interest, but still needs to be worked on, for universal acceptance and adoption. Exciting times are ahead, but that should not drive one to traverse this uncharted area without being cautious.

About the Author

Dyuti Bhushan Bhattacharyya
Senior Consultant – Consulting Group, LTI

Dyuti Bhattacharyya is working with LTI as a Senior Consultant in the Consulting group, dealing with BFSI clients. He possesses rich experience in the capital market domain, especially in the area of derivatives.

info@Lntinfotech.com