

Blockchain Based Compliance Management System

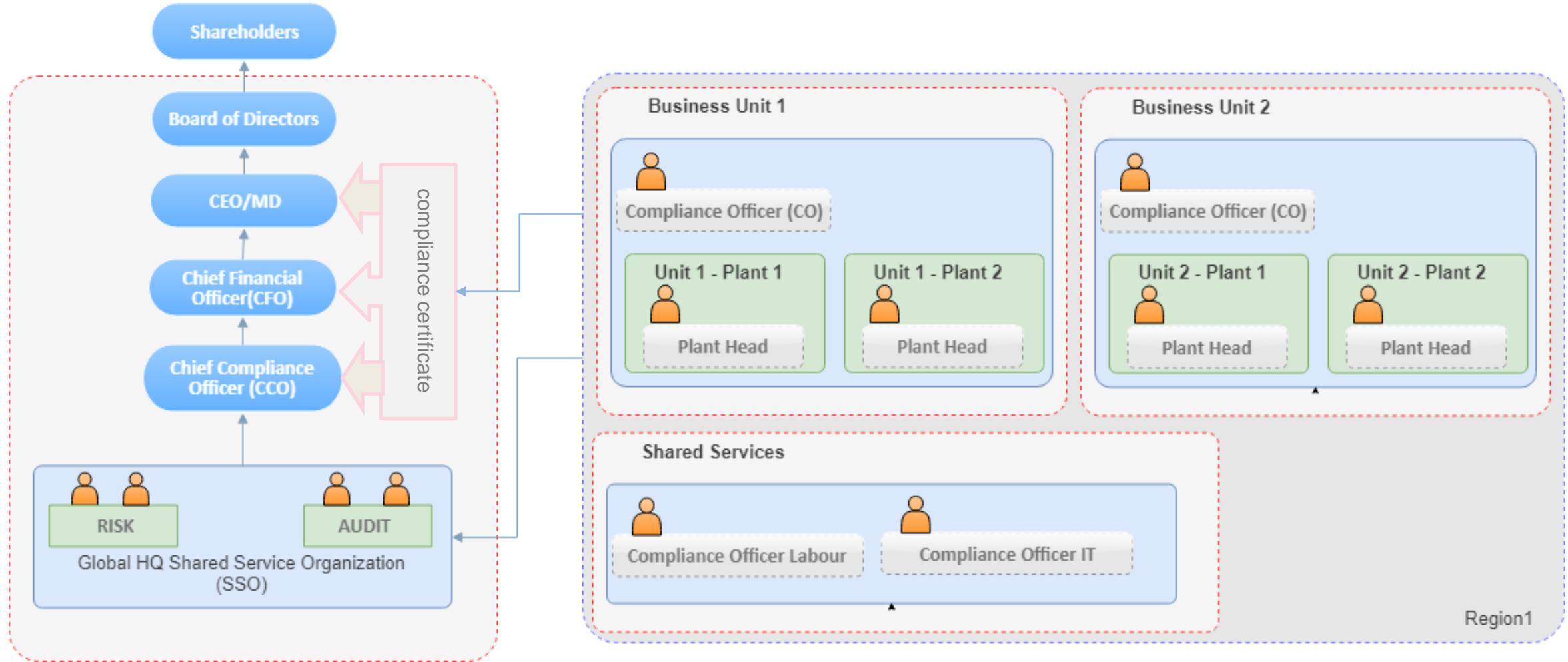
Ashish Jadhav
Vice President – Reliance Jio Infocomm Limited
Certified Blockchain Developer and Expert

Agenda

1. Compliance organizational structure
2. Traditional compliance management process
3. Reconciliation the forefront
4. What, why and how blockchain for compliance management
5. Blockchain application in compliance management
6. Blockchain system configurations

1. Compliance organizational structure

Compliance organizational structure



2. Traditional compliance management process

Traditional compliance management process

1. The current compliance process varies quite a bit among the counterparties and entities involved as all don't use the same process or technology. If a few of them are still using the old time-consuming processes, it can protract the reconciliation process for all.
2. Due to various sources of data there are chances for mismatch, missing information and timely available of complete data.
3. Identifying a framework to safeguard the integrity of data throughout an organization, and ensuring the end-to-end workflow of data transformation, complex integrations with multiple sources format, customized reconciliation processes is a activity high on the agenda within the industry.

3. Reconciliation the forefront

Reconciliation the forefront of regulatory compliance procedures

How can firms ensure quality data is being captured and reported?

How can firms Reduce the risk of regulatory scrutiny as a result of erroneous data?

Reconciliation the forefront of regulatory compliance procedures

Reconciliation procedures play a significant role in the protection of data integrity across all compliance lifecycle stages. Accuracy, completeness and timelines of data submissions allow regulators to effectively monitor the industry for malpractices, and forms the basis for investigations, fines and enforcement actions

The requirement to report trade information to a competent authority on a daily, quarterly or annual basis is now part of the business-as-usual (BAU) process for many companies, and the ability to demonstrate data integrity across an organization has become a principal component in most business models. Why? Because the information provided to the regulator can form the underlying evidence needed to find the firm guilty of unethical market practices.

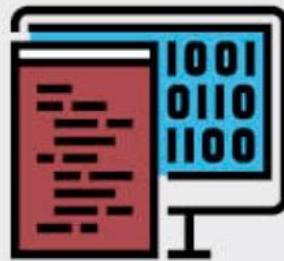
4. What, Why and How Blockchain for compliance management ?

Blockchain Technology

WHAT IS BLOCKCHAIN TECHNOLOGY?



A digital ledger that keeps a record of all transactions taking place on a peer-to-peer network



All information transferred via blockchain is encrypted and every occurrence recorded, meaning it cannot be altered



It is decentralised, so there's no need for any central, certifying authority



It can be used for much more than the transfer of currency; contracts, records and other kinds of data can be shared



Encrypted information can be shared across multiple providers without risk of a privacy breach

Blockchain Concept

Blockchain technology is based on the following concepts-

1. Hashing
2. Digital Signature
3. Block in a Blockchain with mining process
4. A Chain of Blocks
5. A Distributed Chain of Blocks

Blockchain advantage over traditional technology

1. Trustless - You don't have to trust on anyone to trust on the ledger's data
2. Confidentiality – Permission Management and Encryption
3. Fault tolerance - Disaster recovery is excellent
4. Availability - Any number of nodes can go down without affecting the Blockchain
5. Verifiability & Auditability - Easy to audit any transaction & the trail of it

5. Blockchain application in compliance management

Blockchain application in Compliance Management

Blockchain unlocks huge benefits of reconciliation

- Using Blockchain, the participants can work in real time on shared common datasets.

Regulatory compliance management

- Enabling secure compliance management & offer better visibility to regulators with lesser efforts.

Regulatory Governance Improvement

- Create auditable records of any action of users/applications/servers with provenance & non-repudiation.

Regulatory Data security

- Most secure system for maintaining and sharing critical & sensitive data internally & externally

Blockchain Unlocks Huge Benefits for Reconciliation

1. Blockchain technology can be effectively leveraged by companies to streamline their reconciliation processes and make them a lot more efficient. Using Blockchain, the market participants can work in real time on shared common datasets. As a group of independent parties work with their universal data sources, automatic reconciliation happens simultaneously among all the participants. The transparent and real-time data availability offers immense benefits to settlement operations and perfect accounting data reconciliation, thereby eliminating any potential for disputes among the counterparties
2. The data storage capability of Blockchain is shared across all the participating nodes in real time so that transactions captured in the transactional ledger are shared downstream with all the other nodes. This makes real-time reconciliation a distinct possibility.

Regulatory Compliance Management

A Blockchain based compliance and record management with authenticity proof to maintain in verifiable, safe and secure manner.

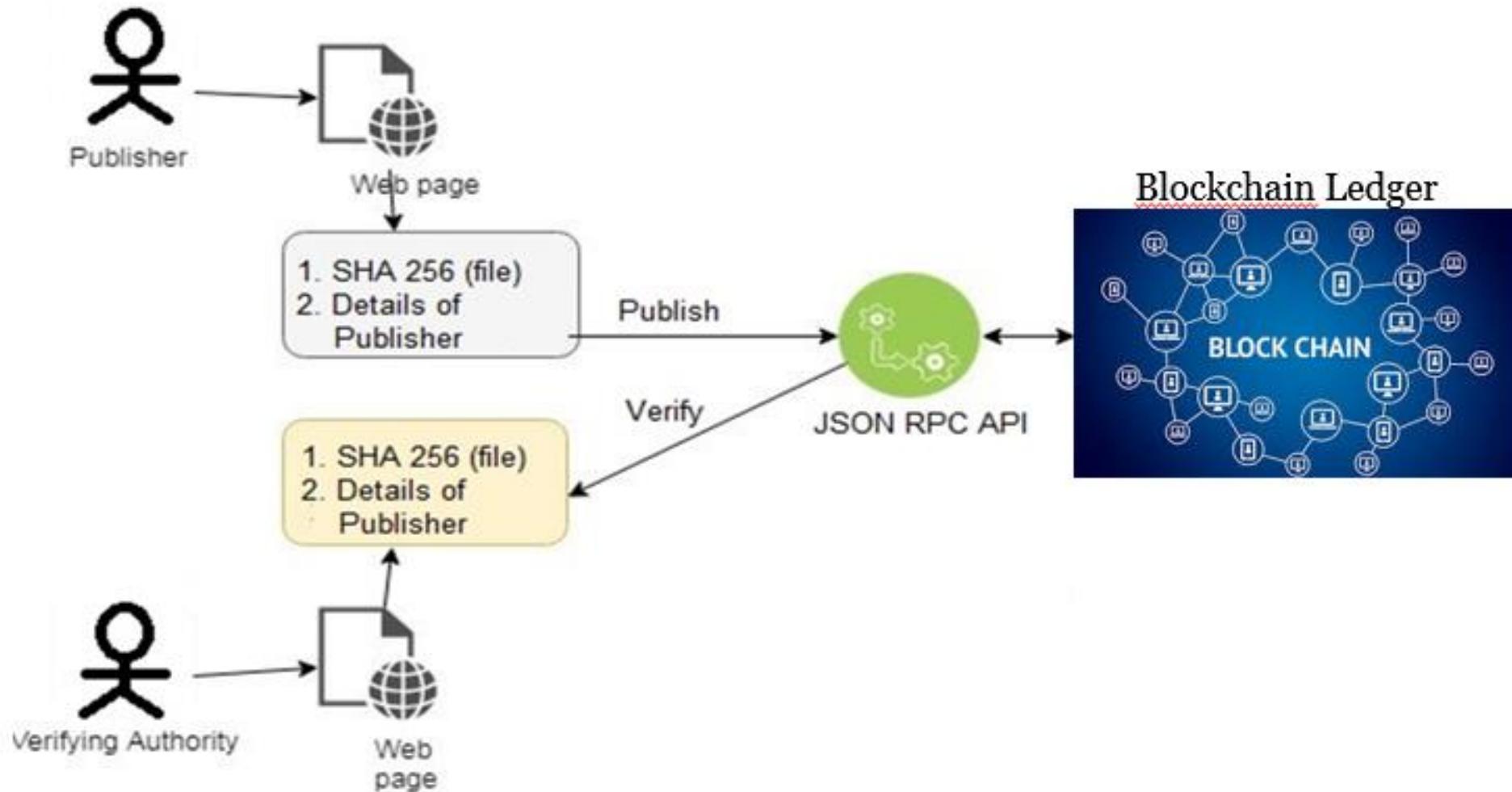
Blockchain can create immutable and independent verifiable digital objects such as data, documents, emails, audio, video, etc. Thus when a need arises to check the authenticity and time stamp for a given record (certificate, agreement etc.), it will be easily and immediately verified and any tampering can be detected.

1. During generation of any regulatory records, their unique signature (SHA 256) can be published into the Blockchain Database
2. The actual records (files) will be stored in IPFS, DMS, FileSystem etc.
3. The Record sequence & signature information (File Digest) can be stored in the Blockchain
4. The compliance applications can use JSON RPC APIs to verify if their report has been tempered and same can't go unnoticed.

Regulatory Record Management

1. The auditors and regulators can be given read only access to produce any kind of audit trail
2. The compliance officer are not required to do any data verification, the Blockchain will verify the data itself with higher trust and security
3. The read access can be controlled by permission management, but only application will have write access to the Blockchain, making the system completely secure
4. Such solutions fundamentally can be difficult with traditional technologies

Regulatory Record Management



Regulatory Governance Management

A Blockchain based governance management for controlling poor governance & to increase the data visibility & audit trail. Blockchain can enable the production of an immutable audit trail to record changes made to an compliance tasks, user actions etc. Each blockchain entry will contains details on who made the change, the time and date the change was made, and some details regarding what was changed.

1. All actions of business stakeholders will be recorded into the Blockchain along with tracking details
2. All actions will be constitute a shared & auditable trails of actions for better visibility & governance
3. All the records will create the tamper-proof audit trails for the administrative or regulatory auditor
4. Can also be used in legal matters & disputes
5. This will also remove the reconciliation process for data verification

Audit History

Compliance Task Data		Hash Data of Compliance	Compliance Data	
Original Source	Verified Proof		Compliance Data	Attachments
Hash of data	Hash Submitted on: 01-02-2018 11:20:35 IST		[{ "_id": "5b950a3171733599697fe419", "index": 0, "guid": "8096bf38-a7b6-421f-8aa5-14b4a0730904", "isActive": false, "ActAuthority": 1003, "ACtLawtype": "IR", "ComplianceAlert": "yes", "ComplianceEntry": "Retail" [{ "compliedDate": "10-09-2017", "DueDate": "20-09-2017", "createdby": "RetailUserbase10", "Approvalstatus": 1, "ApprovalComment": "OK", "ApprovalBy": "SSOCCRetailGroupR1" }], "ComplianceTimeExtension": 05, "Calculatedduedate": "15-09-2017", "ComplianceUploadDocument": "Yes", "uploadpath": "hostentryinMCMC", "MapperActSection": "section256A", "MapperComplianceEvent": "LabourESIC", }]]	0c86843bebad0ff4 9b531abf59fa7fd4f 9be0ae6d24848f2f 1c7db648a1eee3a
0efb96b5cdcbc5d2f696d19f3d8c7c426dbc2384e1116e824344815150e146d80	Hash of data			
Host Node	0efb96b5cdcbc5d2f696d19f3d8c7c426dbc2384e1116e824344815150e146d80			
https://250.65.155.165	Hash of Host			
Hash of Host	a5bf56f6d6d46815ae3b7fcdb0407673030c44b54d07a57fc4dec85a732f9c10			
a5bf56f6d6d46815ae3b7fcdb0407673030c44b54d07a57fc4dec85a732f9c10	Result			
User	Verified			
ashish.jadhav	Yes			
11351a532935a134fb06aaaaa7e6bbd3a0c2d394e4cc66fc53848fc784c252f2	Block Id			
	675436	Block ID of transaction		

Blockchain Explorer

The auditors can use block id to view information about [blocks](#), [addresses](#), [transactions](#), [assets](#), [streams](#) on the web based blockchain explorer .

Block # 675436

BlockHash	0000000000000000000023a218374e73abc0fb1c00110393a5fee9e3f7b1a1219	
<h3>Summary</h3>		
<hr/>		
Number Of Transactions	15	
Height	675436	
Block Reward	NA	
Timestamp	Feb 01 , 2018 5:47:43 PM	
Mined by	RtIFrmtdNode02	
Merkle Root	0c4b796d0deb1e534b44f2c236495...	
Previous Block	675435	
Difficulty	126	
Bits	172819a1	
Size (bytes)	1234	
Version	127	
Nonce	567	
Next Block	675437	

Regulatory Data Security

1. Any kind of data (signed or unsigned) can be published into the Blockchain
2. Digital signatures help ensure that the author of a transaction is, in fact, the individual who holds the private key. Every transaction has a different digital signature that depends on the private key of the user
3. The Blockchain based **data verification and authentication** for data security.
You can also save a cryptographic signature of a document or file on a Blockchain
4. Anyone can verify the data's authenticity & integrity at the time of retrieval
5. All the records will create the tamper-proof audit trails for the administrative or regulatory auditor
6. Any data corruption will be instantly identified and mitigated

Regulatory Data Security

1. Sign (Message, Private Key) -> Signature

Given the message we want to sign and a private key, this function produces a unique digital signature for the message.

2. Verify (Message, Public Key, Signature) -> True/False

Given the message we want to verify, the signature and the public key, this function gives a binary output depending on whether the signature is authentic

6. How did we Implement the blockchain system design for compliance platform?

Blockchain system design

1. Deployment of private blockchains, for within and between organizations.
2. Multiple blockchain networks, and separate for each business
3. To ensure that visibility of blockchain's activity must be kept within the chosen participants as per the segments
4. You can control over which transaction are permitted
5. The system will only stores transactions related to participants
6. You can full control over permissions at the network level for connect, send, receive, issue, create, mine, activate and admin
7. You can restrict blockchain access to a list of permitted users by expanding the “handshaking” process that occurs when blockchain nodes connect

Data Stream DB

A “stream” can be used for general data storage and retrieval that stands “transaction” nature of blockchains

1. It is shared immutable key–value and time series databases
2. To enable a blockchain can be used as a general purpose append- only database, with the blockchain providing timestamping, notarization and immutability.
3. Each record/item will be digitally signed by one or more publishers.

Native Assets

1. You will create and track of assets at the network level
2. You will provide users to perform save multi-asset and multi-party atomic exchange transactions

Mining And Block Signatures

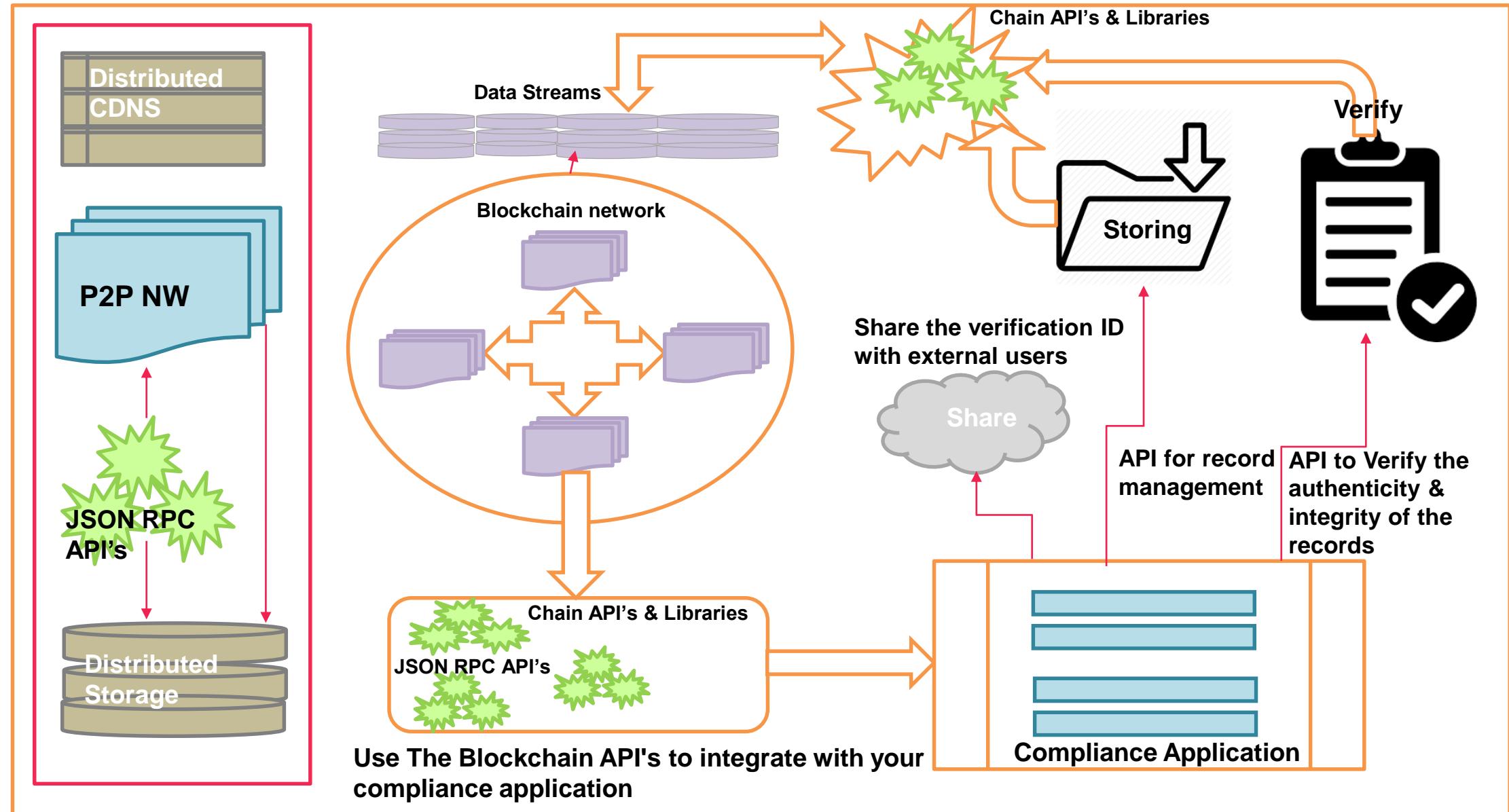
The Block creators will prove their identity by signing blocks.

1. The payload signed by the block creator is the full block header, with the following modifications
2. The merkle_root is recalculated based on the txid of the coinbase transaction to prevents a dependency loop from block signature → coinbase txid → merkle root → block header → block signature
3. The mining process will follow the mining diversity with each permitted miner allowed to mine on rotation basis

Blockchain Explorer

1. Blockchain Explorer (Web-based explorer) is block chain browser that allows you to view information about [blocks](#), [addresses](#), [transactions](#), [assets](#), [streams](#) on the blockchain.

MultiChain JSON-RPC API



Thank you

Ashish.Jadhav@ril.com

Ashish_Jadhav@Hotmail.com



<https://ashishjadhavtechnologyforum.tumblr.com/>



<https://www.linkedin.com/in/ashish-jadhav-2364082/>