

Blockchain Technology and Its Application in Libraries



Nabi Hasan, Ph.D., PDF
Librarian & Head, Central Library
Indian Institute of Technology Delhi
Email: hasan@library.iitd.ac.in

Outline

- Background
- Blockchain: Conceptual Understanding
- What is Blockchain Technology?
- The Three Pillars of Blockchain Technology
- Why is Blockchain Popular?
- What is Distributed Ledger?
- Blockchain for Enterprise Application Developer
- Possible Areas of Implementation of Blockchain Technology in Libraries

Background

- The theory behind Bitcoin was first explained in a 2008 white paper written under the pseudonym “Satoshi Nakamoto.”
- In fact, Blockchain 1.0 is moved to Blockchain 3.0 since 2008: “blockchain 1.0 refers to digital currency, Blockchain 2.0 to digital finance, and Blockchain 3.0 to digital society”.
- Blockchain is a list of records called blocks that store data publicly and in chronological order. The information is encrypted using cryptography to ensure that the privacy of the user is not compromised and data cannot be altered.
- Information on a Blockchain network is not controlled by a centralized authority, unlike modern financial institutions.
- If you are a participant in the Blockchain network, you will have the same copy of the ledger, which all other participants have. Even if one node or data on one particular participant computer gets corrupted, the other participants will be alerted immediately, and they can rectify it as soon as possible.

Blockchain: Conceptual Understanding

- A blockchain is a decentralized database and peer to peer network that stores a registry of transactions secured with cryptography.
- Blockchain is the ledger, or record keeping, side of the transaction and subsequent transactions.
- In simpler terms, Blockchain technology uses a distributed database (multiple devices not connected to a common processor) that organizes data into records (blocks) that have cryptographic validation, are timestamped, and are linked to previous records so that they can only be changed by those who own the encryption keys to write the files.
- Blockchain records the date, time, participants and any other contractual or legal pieces of a Bitcoin transaction.
- Blockchain is a key part of the infrastructure underlying Bitcoin and other cryptocurrencies.

Features of Blockchain

- We have a public distributed ledger, which works using a hashing encryption.
- Every block has a hash value, which is the digital signature of the block.
- All the transactions are approved and verified on the Blockchain network using a proof-of-work consensus algorithm.
- The Blockchain network utilizes the resources of the miners, who are there to validate the transactions for rewards.

What is Blockchain Technology?

- Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the “chain,” in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a ‘digital ledger.’
- Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secured.
- In simpler words, the digital ledger is like a Google spreadsheet shared among numerous computers in a network, in which, the transactional records are stored based on actual purchases. The fascinating angle is that anybody can see the data, but they can’t corrupt it.

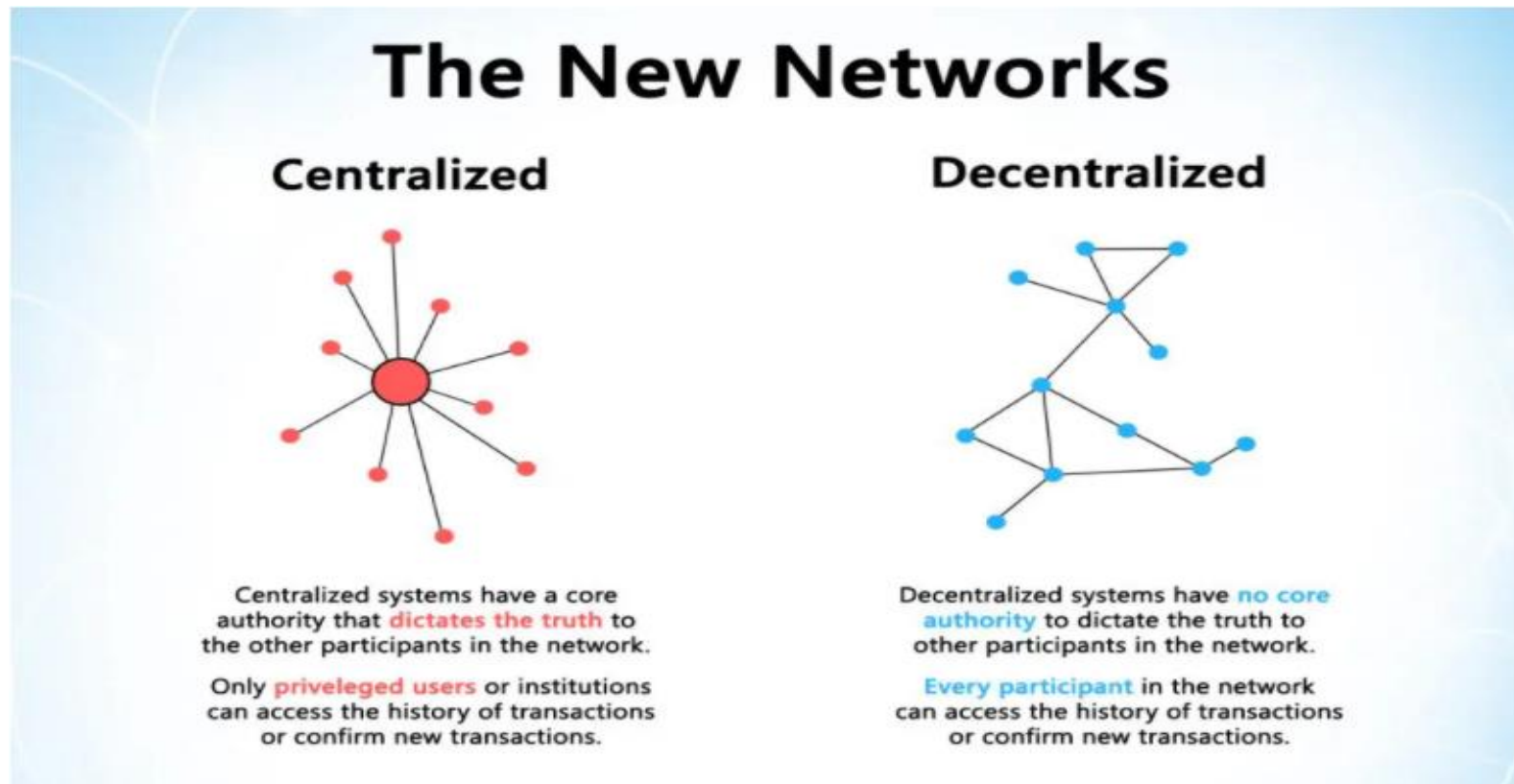
The Three Pillars or Main Properties of Blockchain Technology...

The three main properties of Blockchain Technology which have helped it gain widespread acclaim are:

- Decentralization
- Transparency
- Immutability

The Three Pillars of Blockchain Technology...

Decentralization: In a decentralized network, if you want to interact with your friend then you can do so directly without going through a third party. That was the main ideology behind Bitcoins. You and only you alone are in charge of your money. You can send your money to anyone you want without having to go through a bank.



The Three Pillars of Blockchain Technology...

Transparency: One of the most interesting and misunderstood concepts in blockchain is “transparency.” A person’s identity is hidden via complex cryptography and represented only by their public address. The following snapshot of **Ethereum** transactions depicts as what it actually shown:

TxHash	Block	Age	From		To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...	➡	0x2bdc9191de5c1b...	0,004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...	➡	0xf14cb3acac7b230...	0,744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...	➡	0x2d42ee86390c59...	0,016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...	➡	0xd39681bb0586fb...	0,01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...	➡	📄 0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...	➡	0x8a91cac422e55e...	0,029594 Ether	0.000294

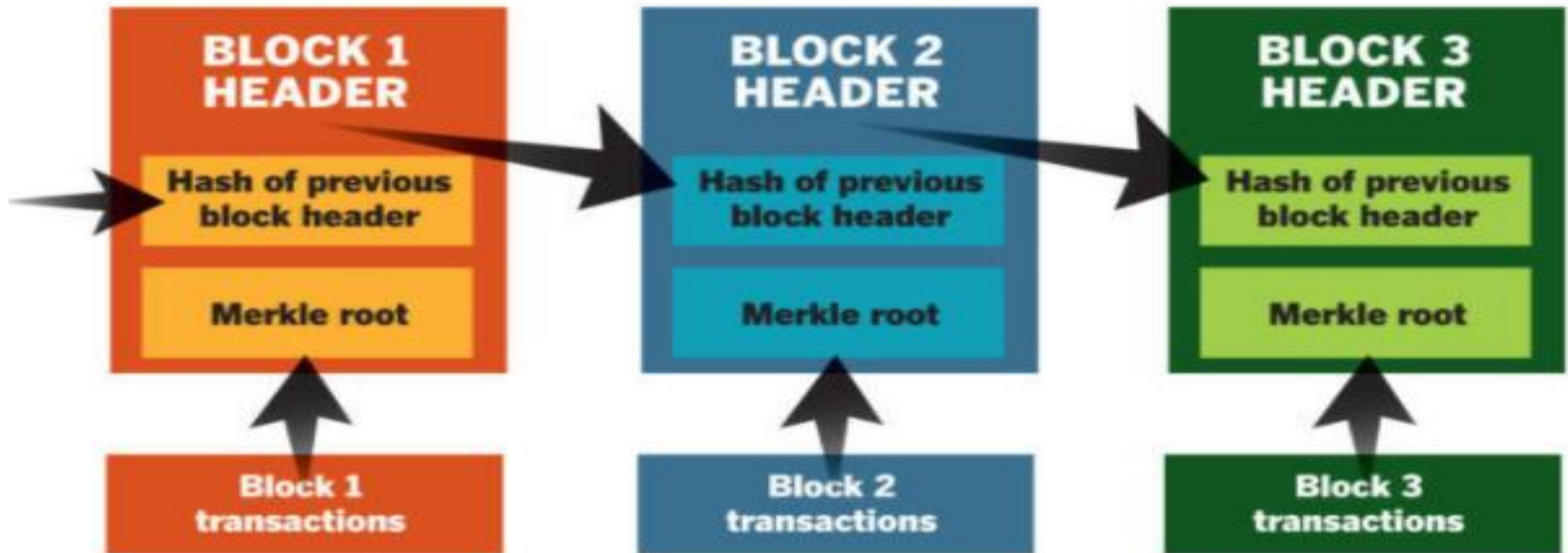
The Three Pillars of Blockchain Technology

Immutability: Immutability, in the context of the blockchain, means that once something has been entered into the blockchain, it cannot be tampered with. The reason why the blockchain gets this property is that of the cryptographic hash function. In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length.

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

What is a Block?

With Blockchain technology, each page in a ledger of transactions forms a block. The block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or blockchain.



Why is Blockchain Popular?

Blockchain is an emerging technology with many advantages in an increasingly digital world:

- **Highly Secure:** Blockchain technology uses a digital signature feature to conduct fraud-free transactions making it impossible to corrupt or change the data of an individual by the other users without a specific digital signature.
- **Decentralized System:** Conventionally, you need the approval of regulatory authorities like a government or bank for transactions; however, with Blockchain, transactions are done with the mutual consensus of users resulting in smoother, safer, and faster transactions.
- **Automation Capability:** Blockchain technology is programmable and can generate systematic actions, events, and payments automatically when the criteria of the trigger are met.

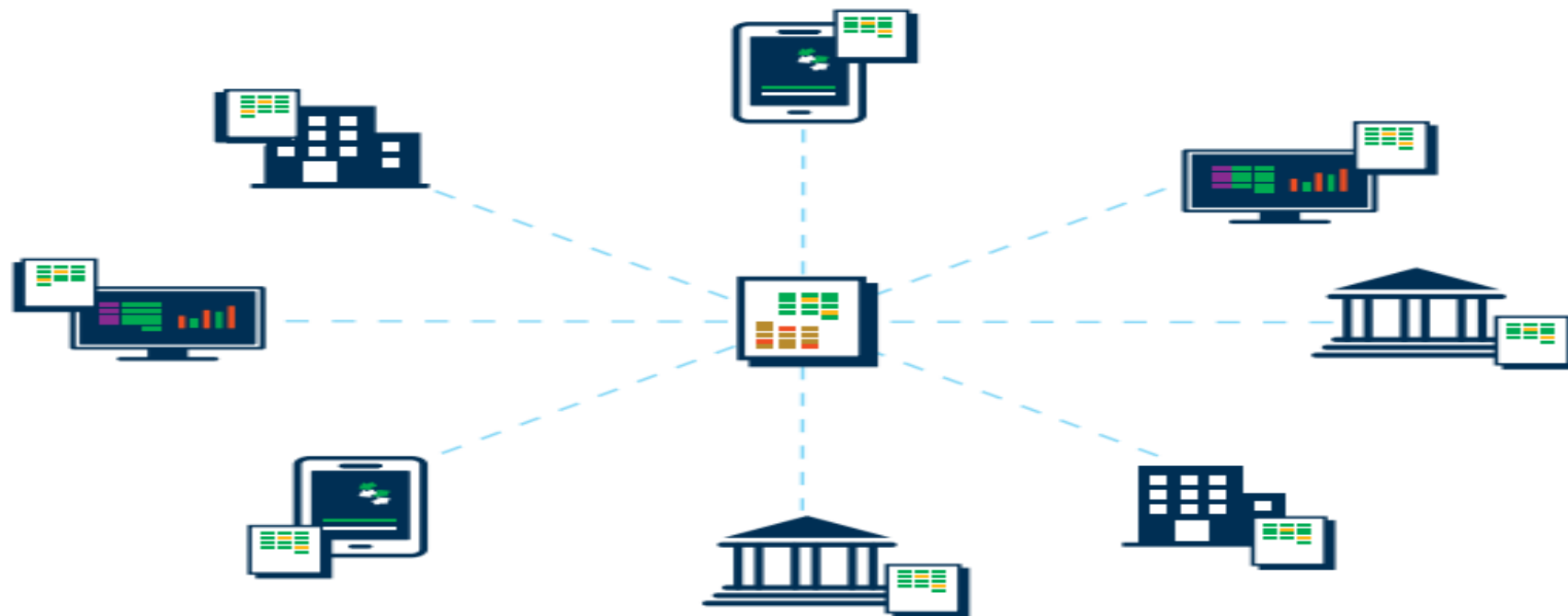
What is a Cryptocurrency?

- A cryptocurrency is a form of digital currency that can be used to verify the transfer of assets, control the addition of new units, and secure financial transactions using cryptography.
- One of cryptocurrencies' most important advantages over normal (fiat) currencies is that they are not controlled by any central authority. Without a central point of failure or a “vault,” the funds cannot be hacked or stolen.
- The shared and distributed nature of cryptocurrencies keeps everyone on the same page.
- Therefore, the transparency and distributed nature of Blockchain technology is what makes cryptocurrencies (at least those that use blockchain) secure.
- Some of the more popular cryptocurrencies are: Bitcoin, Litecoin, Ethereum, Stellar, Ripple, etc.

What is Distributed Ledger?...

A distributed ledger is a database that exists across several locations or among multiple participants.

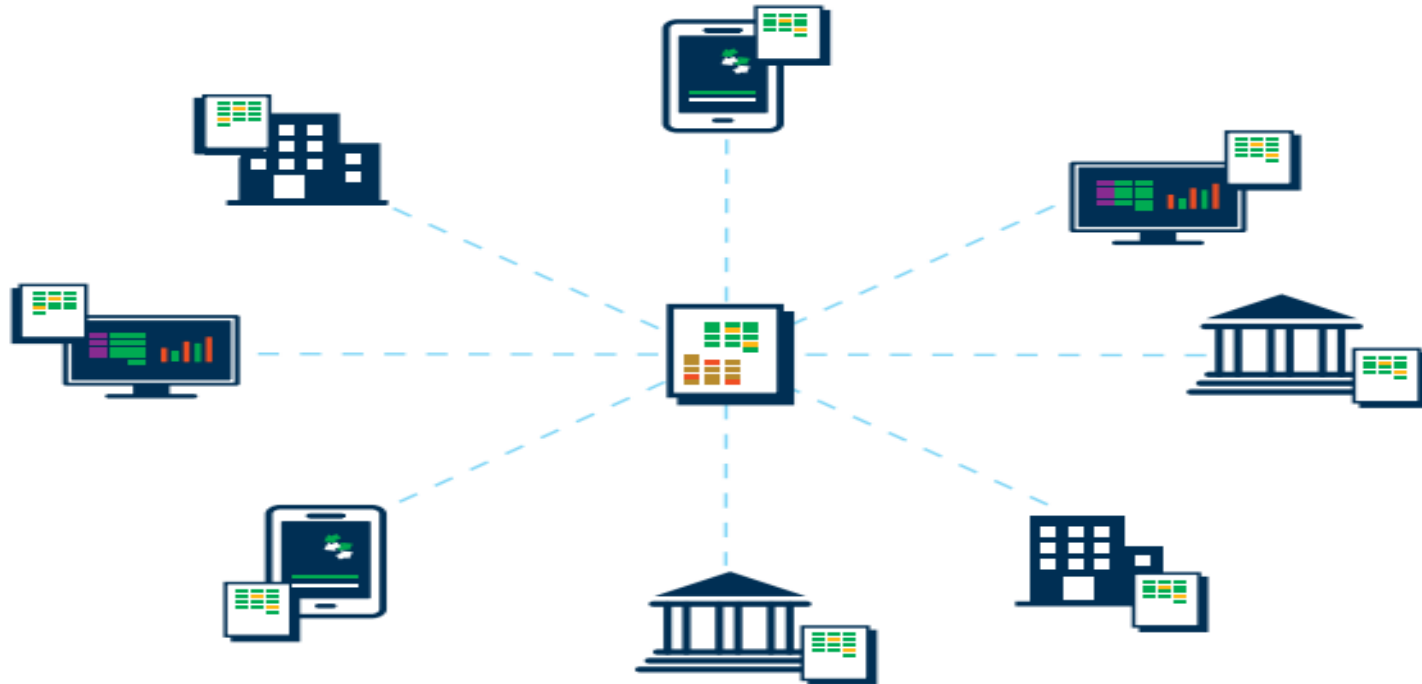
- **Centralized Ledger:** All parties reconcile their local databases with a centralized electronic ledger that is maintained and controlled by a trusted central party.



Centralized Ledger

What is Distributed Ledger?

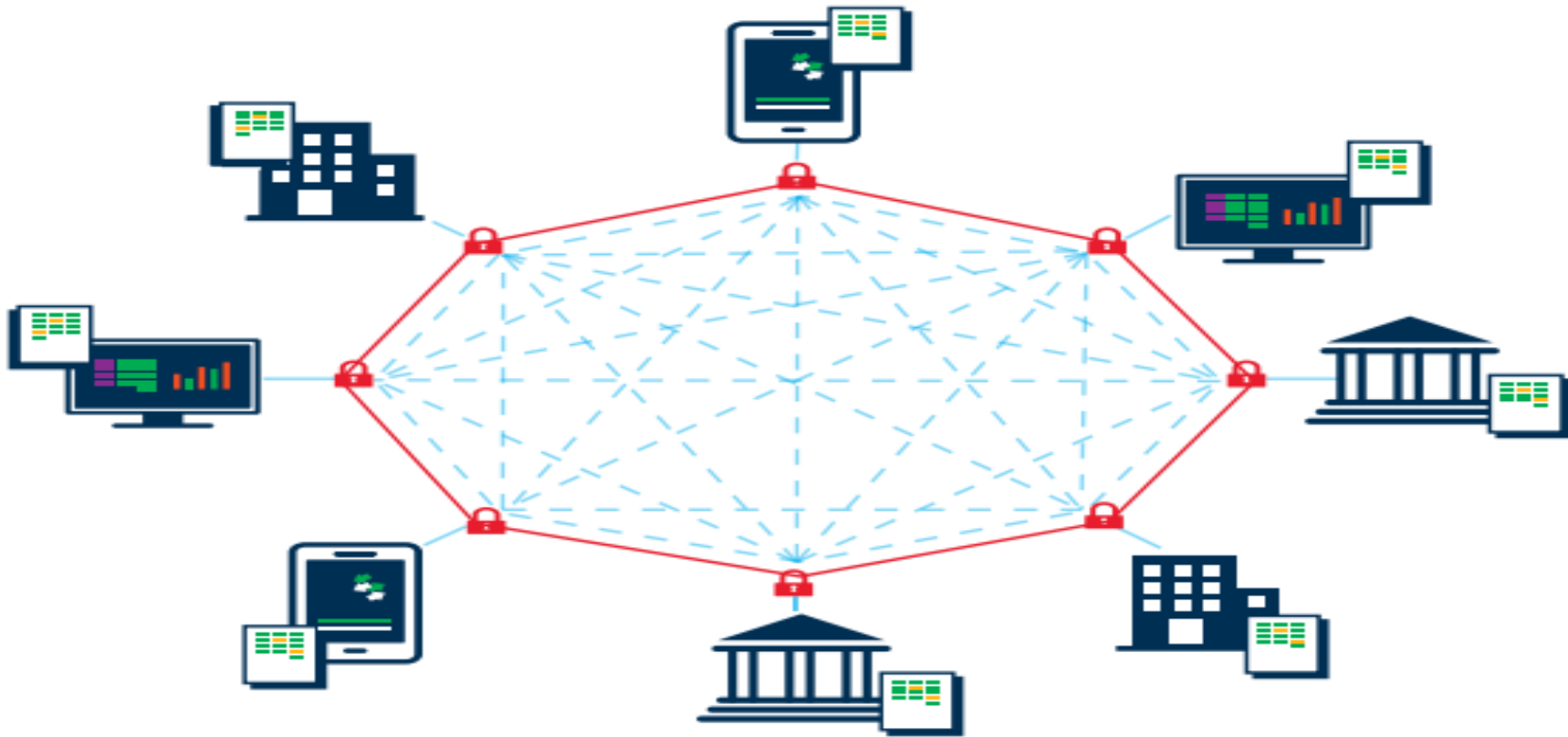
- **Distributed Ledger (Permissionless):** Each node in a P2P network owns a full and up-to-date copy of the entire ledger. Every proposed local addition to the ledger by a network participant is communicated across the network to all nodes. Nodes collectively validate the change through an algorithmic consensus mechanism. After validation is accepted, the new addition is added to all respective ledgers to ensure data consistency across the entire network.



Distributed Ledger (Permissionless)

What is Distributed Ledger?

- **Distributed Ledger (Permissioned):** In a permissioned system, nodes need permission from a central entity to access the network and make changes to the ledger. Access controls can include identity verification.



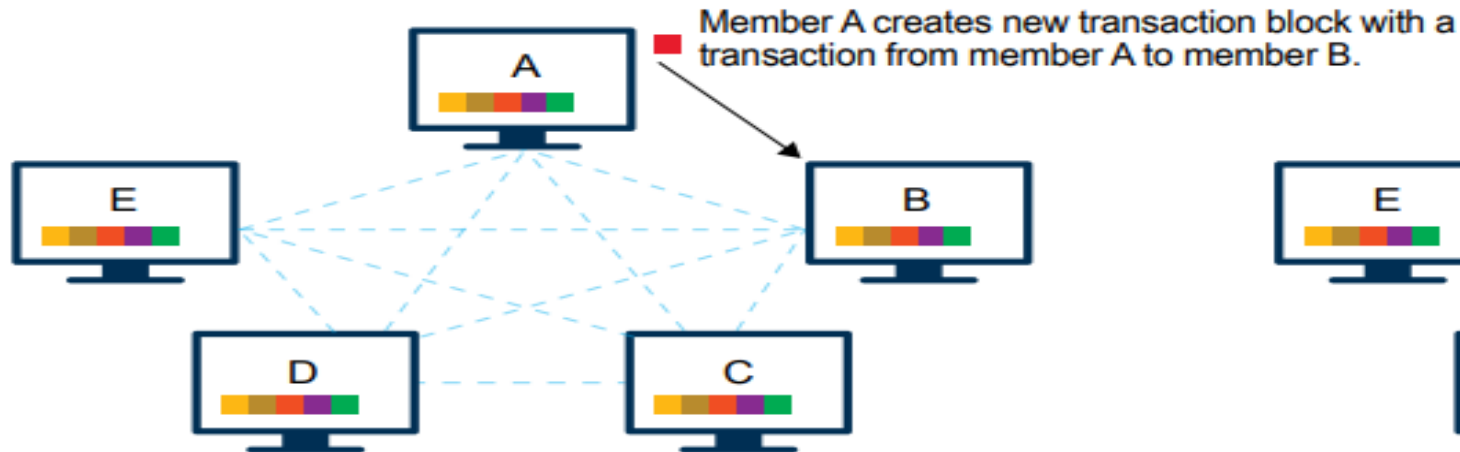
Distributed Ledger (Permissioned)

Features of Distributed Ledger

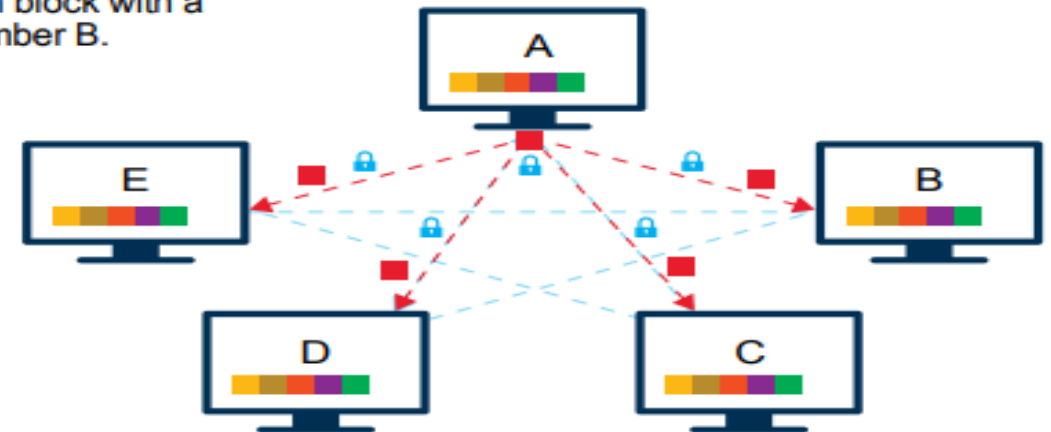
- The distributed feature of Distributed Ledger Technology (DLT) allows self-interested participants in a P2P network to collectively record verified data in a shared ledger without relying on a trusted central party.
- The removal of the central party can increase speed and remove costs and inefficiencies associated with maintaining the ledger and subsequent reconciliations.
- It can also enhance security because there is no longer a single point of attack in the entire network.
- Permissioned systems can fit more easily into existing legal & regulatory frameworks and institutional arrangements. However, to some degree, permissioned DLs remove key benefits of DLT's most critical innovation, such as the lack of need for a central party.

How does Blockchain-Based DLT Work?

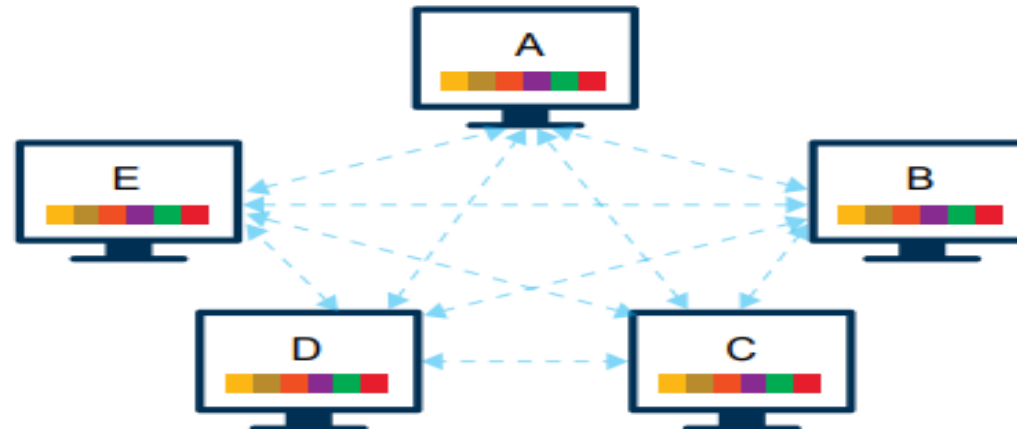
1. Blockchain-based DLT systems take the form of an append-only chain of data 'blocks'. New additions to the database are initiated by one of the members (nodes), who creates a new "block" of data containing several transaction records.



2. Information about this new data block is then shared across the entire network, containing encrypted data so transaction details are not made public.



3. All network participants collectively determine the block's validity according to a pre-defined algorithmic validation method ('consensus mechanism'). Only after validation, all participants add the new block to their respective ledgers. Through this mechanism each change to the ledger is replicated across the entire network and each network member has a full, identical copy of the entire ledger at any point in time.



Open/Permissionless Vs. Permissioned Distributed Ledgers

	'Public' (open) Blockchains	Permissioned Blockchains
Central party	No central owner or administrator	Has some degree of external administration or control
Access	Anyone can join	Only pre-selected participants can join the network
Level of Trust	Network members are not required to trust each other	Higher degree of trust among members required (as collaboration among members could alter the ledger)
Openness	Ledger is open & transparent - shared between all network members	Different degrees of openness and transparency of the ledger are possible
Security	Security through wide distribution in a large scale network	Security through access control combined with DLT in smaller scale networks
Speed	Slower transaction processing restricts transaction volume	Faster transaction processing allows for higher transaction volume
Identity	User identity anonymous or protected by pseudonyms	Identity verification typically required by owner/administrator
Consensus	Difficult proof-of-work required as consensus mechanism	Variety of consensus mechanisms possible (typically less difficult & less costly than proof-of-work in permissionless blockchains)
Asset	Typically: native cryptocurrencies. But implementations are possible where a token is used which can represent any asset.	Any asset
Legal ownership	Legal concerns over lack of ownership as no legal entity owns or controls the ledger	Greater legal clarity over ownership as owner/administrator is typically a legal entity
Examples	Bitcoin, Ethereum	R3's Corda, Hyperledger Fabric

How Does Blockchain Work?...

Blockchain consists of three important concepts: Blocks, Nodes and Miners.

Blocks

Every chain consists of multiple blocks and each block has three basic elements:

- The data in the block.
- A 32-bit whole number called a NONCE. The nonce is randomly generated when a block is created, which then generates a block header hash.
- The hash is a 256-bit number wedded to the nonce. It must start with a huge number of zeroes (i.e., be extremely small).

When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

How Does Blockchain Work?...

Nodes

- One of the most important concepts in blockchain technology is decentralization. No one computer or organization can own the chain. Instead, it is a distributed ledger via the nodes connected to the chain.
- Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning.
- Every node has its own copy of the blockchain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified.
- Each participant is given a unique alphanumeric identification number that shows their transactions.
- Combining public information with a system of checks-and-balances helps the blockchain maintain integrity and creates trust among users.
- Essentially, blockchains can be thought of as the scalability of trust via technology.

How Does Blockchain Work?

Miners

- Miners create new blocks on the chain through a process called mining.
- In a blockchain, every block has its own unique nonce and hash, but also references the hash of the previous block in the chain.
- Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found.
- Making a change to any block earlier in the chain requires re-mining not just the block with the change, but all of the blocks that come after. This is why it's extremely difficult to manipulate blockchain technology.
- When a block is successfully mined, the change is accepted by all of the nodes on the network and the miner is rewarded financially.

Public Vs. Private Blockchains

Public vs Private Blockchain Network



Public Blockchain: Permissionless

An open network system where all the devices can freely access without any kind of permission. The ledger is shared and transparent.



Private Blockchain: Permissioned

A user has to be permitted by the blockchain authority before he/she could access the network. The user might join only if he/she gets an invitation.

What is Blockchain good for?

Web 3.0 and blockchain give users the ability to **create value and authenticate digital information**.
What new business applications will arise as a result?



Smart Contracts

Distributed ledgers enable the coding of simple contracts that will execute when specified conditions are met.



Sharing Economy

By enabling peer-to-peer payments, the blockchain opens the door to direct interactions between parties.



Crowd Funding

Blockchains take this to the next level, potentially creating crowd sourced venture capital funds.



Governance

By making vote results fully publicly accessible, distributed database technology could bring full transparency to elections.



Supply Chain Auditing

Blockchains provide an easy way to certify the origin of products. Blockchain timestamping of dates and locations would correspond with product numbers.



File Storage

Decentralizing file storage on the internet brings clear benefits. Distributed data prevents hacked and lost files.



Prediction Markets

Prediction markets pay out according to event outcomes. Blockchains are a "wisdom of the crowd" technology that will no doubt find new applications for years.



Intellectual Property

Smart contracts can protect copyright and automate the sale of creative work online. This eliminates the risk of file copying and redistribution.



Internet of Things

Smart contracts can automate remote systems through a combination of software, sensors, and network facilities.



Microgrids

Blockchains enable markets for renewable energy within local areas like neighbourhoods.



Identity Management

Distributed ledgers offer enhanced methods to prove who you are. Having a secure, digitized identity will be important as online services continue to evolve.



AML and KYC

Improving anti-money laundering and know your customer practices can have huge potential. Cross-institution client verification and stronger analysis is possible with blockchain.



Private Data Management

Users will have the ability to manage and sell their online activity profiles in small, fractured amounts if they see fit.



Land Title Registry

Publically accessible ledgers can make all types of record keeping more efficient. Property titles are susceptible to fraud, and can be secured on chain.



Stock Trading

When peer-to-peer trade confirmations become instant, intermediaries like auditors and custodians get removed from the process.



Blockgeeks

Blockchain Issues

Legal Issues

- Ownership of a decentralized ledger
- Privacy

Security Issues

- Blockchain can be hacked

Standardization Issues

- Process Management
- Data Retention
- Provenance of Information Stored in the Blockchain
- Authenticity of Information

Blockchain for Enterprise Application Developer

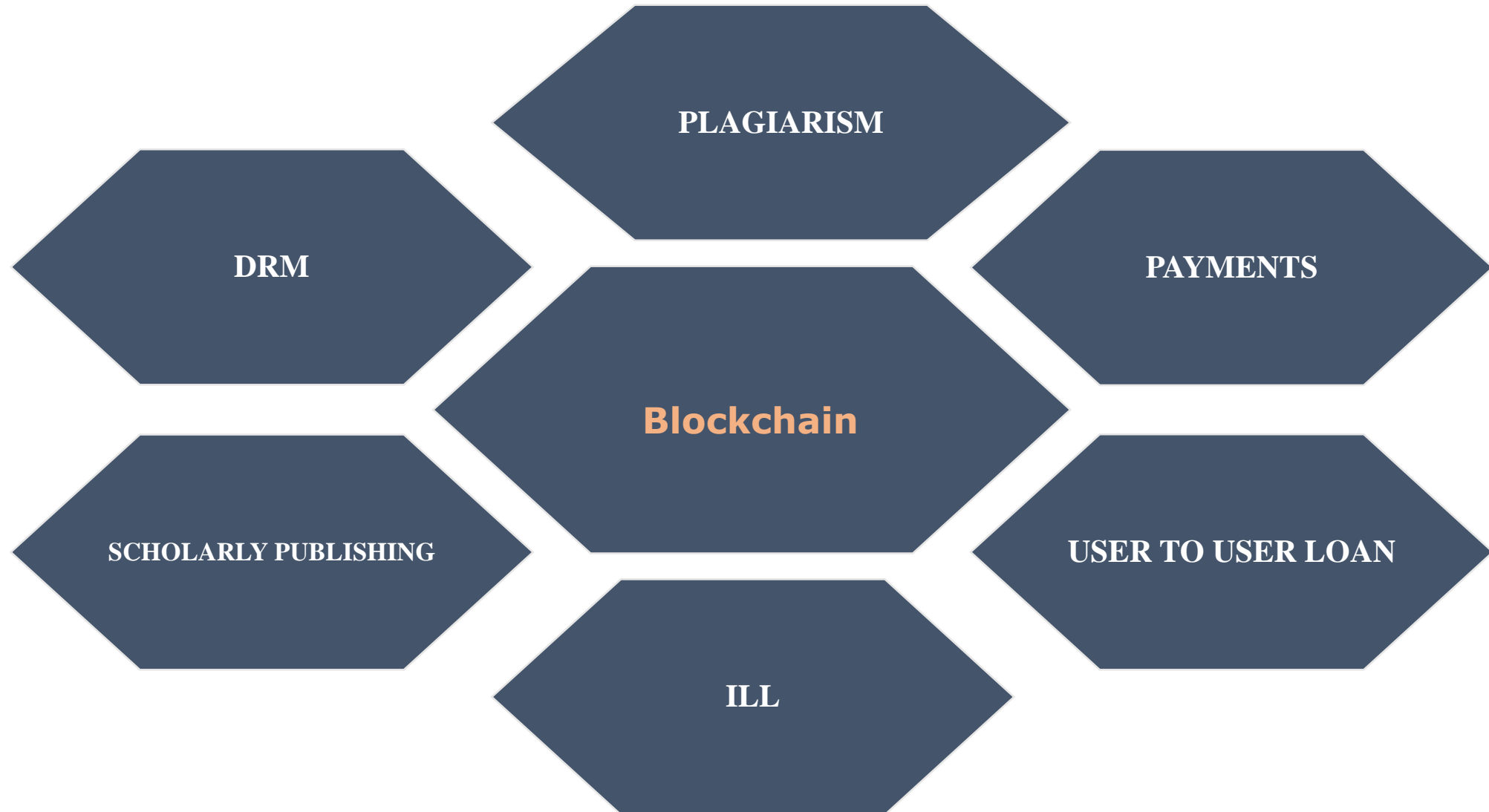
Audience	Managers	Software Developers	Instructors
	Architects	Business Analysts	Students
Topics Covered	<ul style="list-style-type: none">• Key Concepts• Architecture for blockchain solutions• Assignments		<ul style="list-style-type: none">• Development tools• Advance concepts like IPFS, BaaS, ZKP etc• Mindmaps
Hands-On	Developing solutions on Hyperledger	Solution Examples	
	Structured Approach to arrive at solutions	Developing solutions on Ethereum	
Key Features	How to Videos for easy walkthrough	Interview Questions to understand what industry is looking for	
	Supporting materials for chapter summaries and further reading	Introduction to Toolset for developers	
Buy At:	Physical Books		E-book
	<ul style="list-style-type: none">• Amazon• Flipkart• Brick and Mortar stores		<ul style="list-style-type: none">• Amazon Kindle• Impulsys

The Librarians can help Blockchain Education reach to All. Here, the Role of the Librarian is Important, like

Librarian's Role

- ⑩ In Need to understand blockchain
- ⑩ Use of Blockchain in various applications
- ⑩ To Provide Blockchain education to users

Areas of Implementation of Blockchain Technology in Libraries

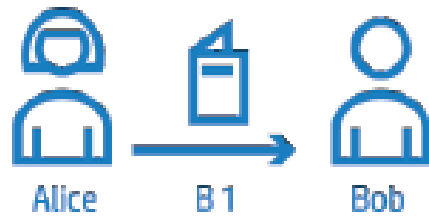


Blockchain for Libraries

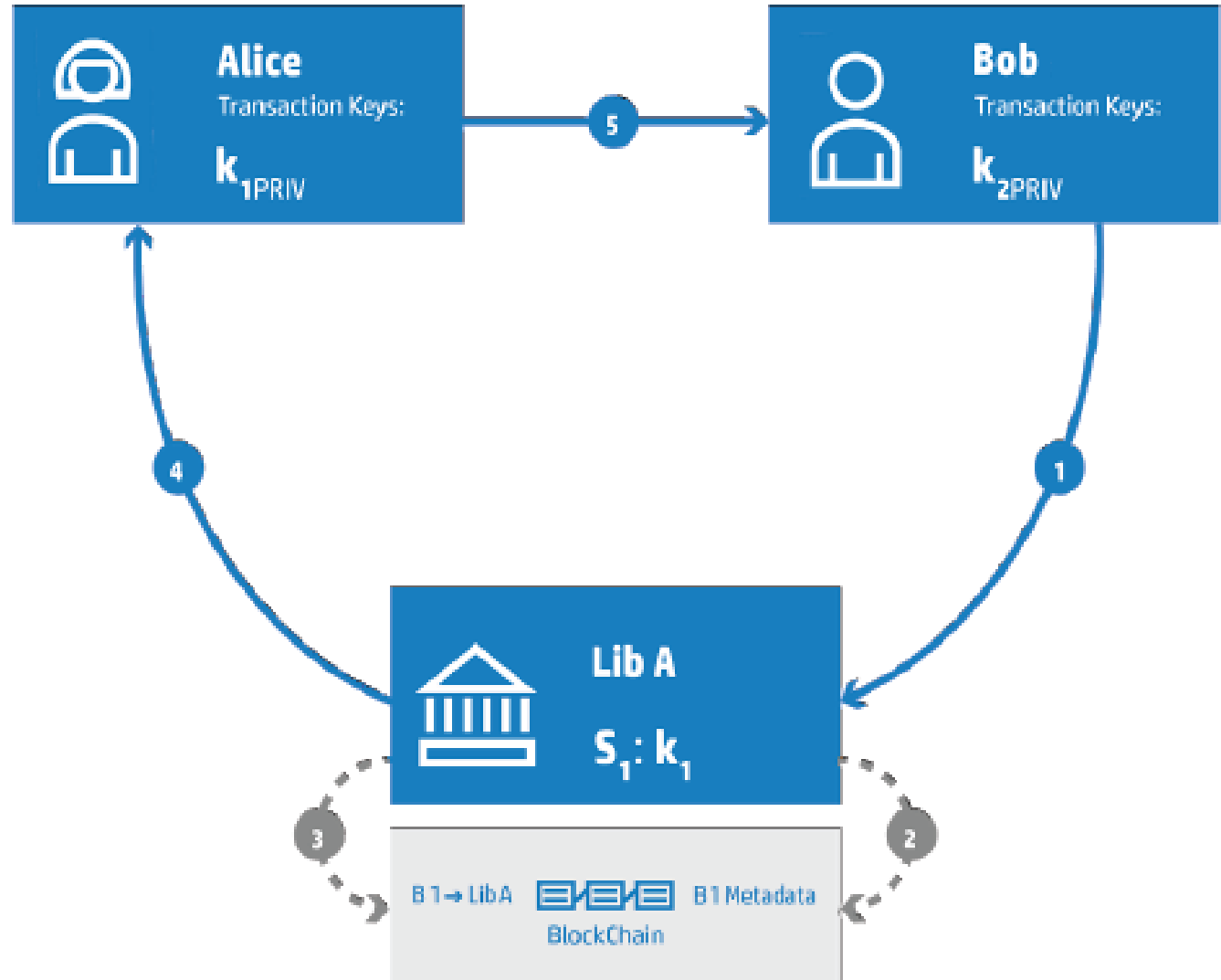
Blockchain technology is opening new opportunities. Apart from its application in financial services, blockchain-based systems may be implemented in other fields related to Libraries, like.

- Digital preservation and tracking
- Community-based collections to share objects, tools, and services
- Blockchain-based currencies for international financial transactions (IFLA)
- Inter Library Loan and Voucher System
- Library verification of credentials (information literacy)
- Library card
- Archives/special collections where provenance and authenticity are essential
- Corporate library records keeping
- Organizational data management
- Intellectual property for R&D, etc.

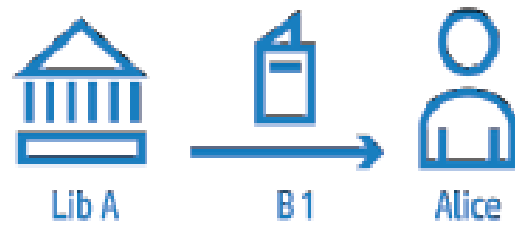
User to User Loan



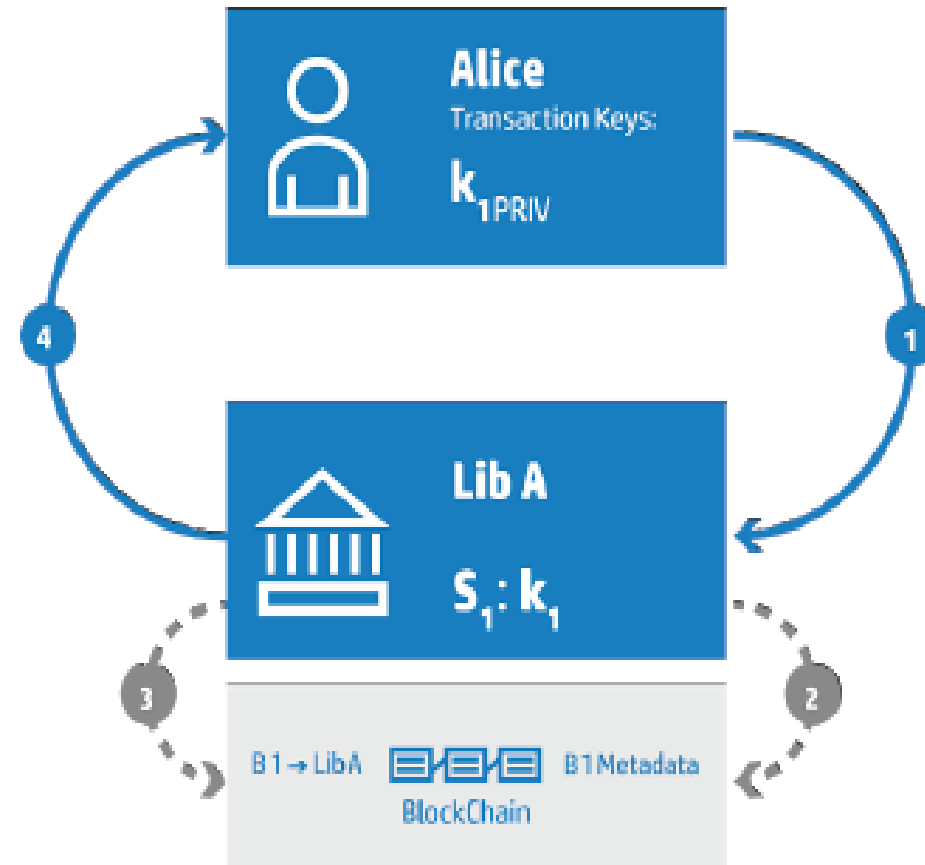
- 1 requestBook()
- 2 lookUpBookLibrary()
- 3 lookUpBookConditions()
- 4 pingHolder()
- 5 authorizeTransaction()



Library to User Loan



- 1 requestBook()
- 2 lookUpBookLibrary()
- 3 lookUpBookConditions()
- 4 authorizeTransaction()



Scholarly Publishing

- Basically, the Blockchain is about storing information in a distributed, tamper-resistant setting. This fits well with the work, librarians have always been doing, that is, gathering, preserving, and sharing authoritative information.
- The Blockchain can help librarians achieve that work, especially in the world of scientific publications.
- One potential use for the blockchain could be to create timestamped, verifiable versions of journal articles.
- Irving and Holden successfully tested the use of the Bitcoin blockchain “as a low cost, independently verifiable method that could be widely and readily used to audit and confirm the reliability of scientific studies.”
- They did this by creating a cryptographic hash of the plaintext of a trial protocol document and using that hash to create a new private Bitcoin key.
- This creates a time-stamped record in the blockchain, which other researchers can quickly verify in the future. If the document is changed, the hash of the new document will not match the one stored in the blockchain.

Digital Rights Management

- Like as DRM Tool.
- Digital resources are inherently reproducible, and this creates issues for libraries and publishers. Publishers have imposed draconian, often unworkable DRM tools on libraries and consumers in order to prevent copying of their materials. Because the blockchain creates a unique, verifiable record that can be accessed by anyone, it could be tied to digital materials and used as a method to show “proveable scarcity” of that resource.
- This would allow digital materials to be uniquely identified, controlled, and transferred.
- Publishers could be reassured that no copies were being made, but whether prices would decrease accordingly is debatable.

Summing Up

- Blockchain Technology is increasingly being adopted in libraries in various ways like for creating an enhanced metadata system, protecting digital first sale right, peer to peer sharing and so on.
- The technology is the best fit for academia and to get potential pace in libraries, apart from those already explained.
- It can be used to secure user records in libraries, document library acquisitions, and improve collections maintenance.
- Applications for special collections could allow for identification and discovery of unique holdings.
- The scholarly record is another use case that lends itself to blockchain by allowing researchers to record and timestamp their ideas and disseminate knowledge.
- Libraries have a major opportunity to use blockchain technology to advance privacy for users, increase collaboration, and transform the way they work with each other and their communities.
- San Jose University, Toronto Reference Library, Suffolk Cooperative Library System, etc. are already exploring this Technology and we can see a great scope for other libraries to follow.

References

- https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-ethereum?source=sl_frns_nav_playlist_video_clicked
- www.ala.org/tools/future/trends/blockchain
- <https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html>
- <https://blockgeeks.com/guides/what-is-blockchain-technology/>
- Enis, M. (2017), “SJSU-Led team explores blockchain in libraries”, Library Journal,(blogpost), available at: www.libraryjournal.com/?detailStory=sjsu-led-team-explores-blockchain-in-libraries,
- Frederick, Donna Ellen. (2019), “Blockchain, Libraries and the Data Deluge.” Library Hi Tech News, vol. 36, no. 10, 2019, pp. 1–7., doi:10.1108/lhtn-09-2019-0059.
- Coghill, J.G. (2018), “Blockchain and its implications for libraries”, Journal of Electronic Resources in Medical Libraries. 15 No. 2, pp. 66-70, available at: [HTTPs://doi.org/10.1080/15424065.2018.1483218](http://doi.org/10.1080/15424065.2018.1483218)
- Oyelude, Adetoun A. “What's Trending in Blockchain Technology and Its Potential Uses in Libraries.” Library Hi Tech News, vol. 36, no. 9, 2019, pp. 17–18, doi:10.1108/lhtn-09-2019-0062.
- Sanjay and Hasan, Nabi. (2020), “Blockchain Technology and its Application in Libraries”, Library Herald, Vol. 58 No. 4, pp. 118-125.

Disclaimer/Acknowledgements

- The Presentation/Lecture has been prepared from different resources to help the learners to understand the topic for academic and research use.
- I duly acknowledge the scholars and the website content providers whose materials has been used in my presentation/lecture.



THANK YOU

