BLOCKCHAIN IN THE ERA OF AUDITING & ASSURANCE

Suryachandra & Associates
Chartered Accountants

Authored by Anudeep Reddy

Disclaimer

This paper has been authored by Anudeep Reddy, representing Suryachandra & Associates (SCA), as non-authoritative guidance. The views, opinions, findings, and conclusions or recommendations expressed in these papers and articles are strictly those of the author. Anudeep Reddy nor Suryachandra & Associates accept any responsibility or liability for the correctness of, the information contained in papers and articles or for any errors or omissions in, or that might occur directly or indirectly as a consequence of the use, application or reliance on this material.

Table of Contents

What is Blockchain?

As the name suggests, Blockchain is nothing but a chain of blocks, where a block refers to any digital information and chain refers to a public database, where the information (Blocks) is stored. In other words, it is a digital ledger/record, distributed over the internet which captures digital transactions amongst various parties. It is a peer-peer oriented model where, all the transactions since their very inception are recorded, and together form a chain. Each peer holds a complete copy of the ledger. As transactions keep happening, block chain is a forever growing list of records, which are linked to each other using cryptography. Blocks store information about the transactions, such as date, time, amount transacted etc. Additionally, they store information about the parties to the transaction. But in order to secure the identity of the parties, the actual names are not stored. A party's identity is hidden via cryptography and represented only by their public address. A single block has the capacity to store up to 1 MB of data. Hence, a single block can house thousands of transactions under one roof.

To gain a better understanding of the Blockchain Technology, it is imperative to understand the underlying characteristics:

1. **Decentralized/ Distributed**: There exists no central authority to control the blockchain. Hence the transaction fees normally collected by corporations are no longer a factor. It is a peer-peer distributed network. It has been designed to be distributed and synchronized across all networks. A group of nodes maintain the network, making it decentralized.

2. **Consensus**: This is the most critical attribute of all. This gives blockchain the ability to update the ledger via consensus. This is what gives it the power of decentralization. No central authority is in control of updating the ledger. Instead, any update made to the blockchain is validated against strict criteria defined by the blockchain protocol and added to the blockchain only after a consensus has been reached among all participating peers/nodes on the network.[1]

3. **Immutable**: The literal meaning of Immutable is "*unchanging over time or unable to be changed.*" This means, once the data has been recorded on the block chain, it can never be changed or tampered with. As it is decentralized, each user has a copy of the chain. Moreover, the data is encrypted using complex algorithms. This combination makes hacking information on blockchain next to impossible. In fact, the larger the network grows and becomes increasingly decentralized, the more secure it becomes.

4. **Near Real Time Settlement**: A blockchain enables the near real-time settlement of transactions, thus reducing risk of non-payment by one party to the transaction.

5. **Transparency**: The transparency of blockchain stems from the fact that the holding and the transactions of each public address are open to viewing by everyone. Any individual with adequate measure can decrypt and access data. This coupled with the characteristic of being immutable, make the entire technology transparent.

[1] https://medium.com/coinmonks/what-the-hell-is-blockchain-and-how-does-it-works-simplified-b9372ecc26ef

How does Blockchain Technology Work?

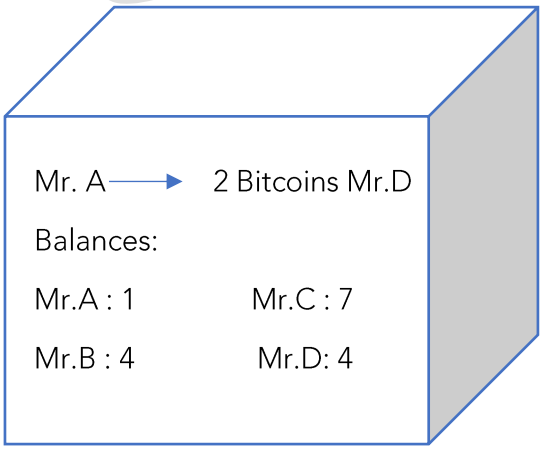
Overview

Blockchain technology has been the backbone for cryptocurrencies. All crypto currencies such as Bitcoin, Litecoin, Ethereum etc are transacted using blockchain technology. Blockchain had originally been devised for such transactions, but it has in turn has proved to be of potential use for other transactions, sectors and markets. But let's gain an understanding of how Blockchain technology work by taking a cryptocurrency transaction.

Let's assume 4 people Mr.A, Mr.B , Mr.C and Mr.D meet for dinner. The amount has been paid by Mr.D and all four of them decide to split the bill equally. Mr. A successfully transfers his share of amount to D. But the transactions of B & C do not go through due to some technical difficulties cited by the bank. They hence decide to use cryptocurrency. Let's assume A, B and C have to transfer 2 Bitcoins each to D. The following are the balances of Bitcoins with each individual:

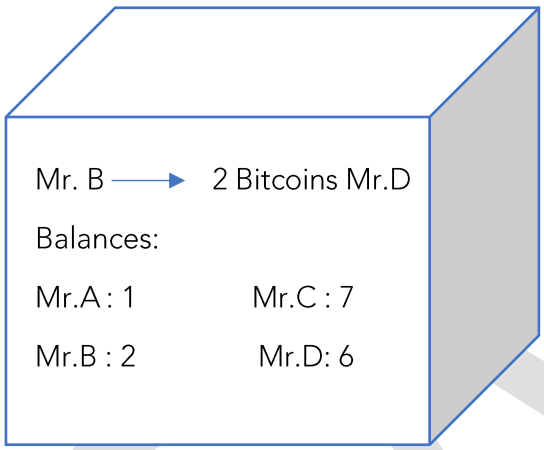
A	3 Bitcoins
B	4 Bitcoins
C	7 Bitcoins
D	2 Bitcoins

First, A transfers 2 Bitcoins to D. Here, a record of the transaction is created in the form of a block. The transaction details between A and D are permanently recorded in the block. Details such as amount transferred, parties to the transaction and the balance of Bitcoins available with each party. Hence after the first transaction, the block would look similar to this:

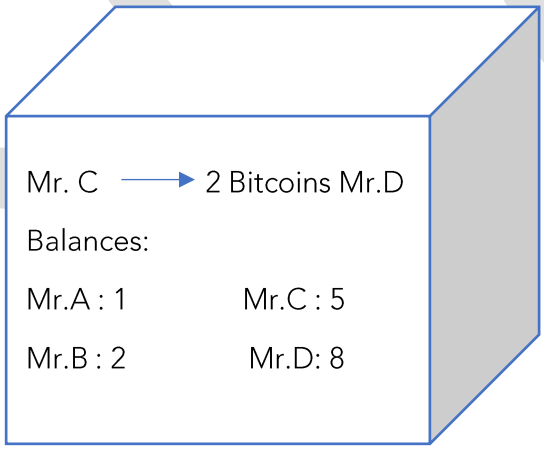


(This is not how the block actually appears. Also, as mentioned previously, the actual names of the parties aren't displayed on the block. The above representation is only for informative purposes.)

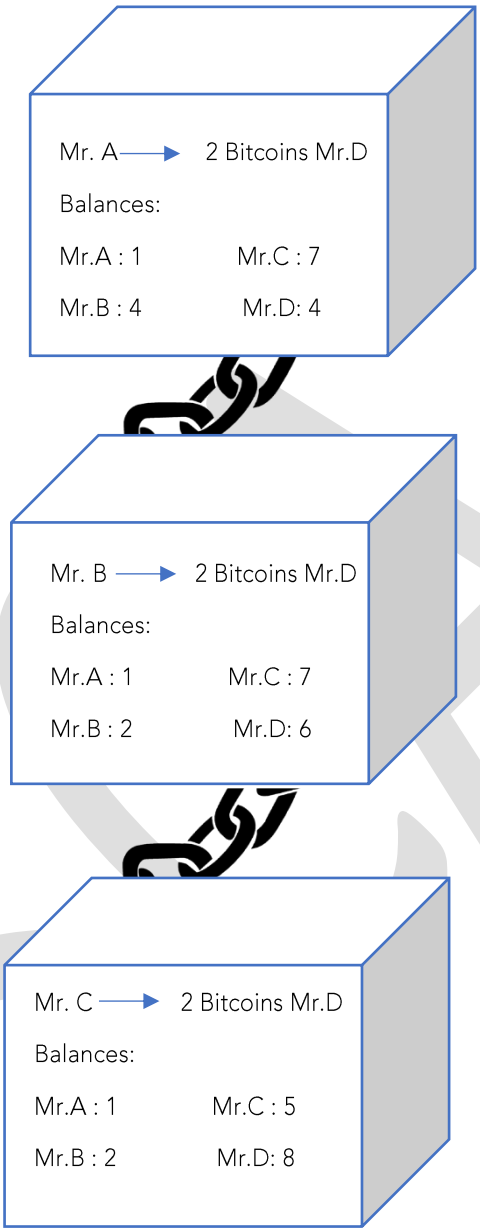
Next B transferred 2 Bitcoins to D. A new block is created for this transaction and stores the aforementioned information related to the transaction. Here is how the new block will appear after the second transaction:



Lastly, C transfers 2 Bitcoins to D and this is how the new block shall appear:



Hence it can be understood that all the blocks are linked to each other, as each of them takes into account the previous block, for the Bitcoin balances available with the parties. Hence the entire block chain appears as below:



As stated earlier, Blockchain is a public distributed ledger. Hence the above blockchain is shared among all the parties i.e. A,B,C and D and each of them has a copy of it. Hence, this is the framework of how the Blockchain technology works.

Let's assume that Mr. A now further tries to send 2 more Bitcoins to Mr. D. This transaction will not proceed as Mr. A has a balance of only 1 bitcoin. And this record is available with all the other parties namely B, C and D. Hence the others would not ratify this transaction. This where the characteristic of *"consensus"* comes into picture.

Therefore, it can be inferred that Blockchain is:

- Collection of distributed ledgers which are linked to each other (Decentralization)
- Available to everyone (Transparency)
- Strongly resistant to alteration (Immutable)
- And where the data is recorded in the block only after consensus (Consensus)

Public Cryptography and Blockchain

As mentioned above, the ultimate goal of a Blockchain system is to create a Digital Network, where the participants can transfer information and assets in a secure manner by eliminating third parties and the accompanying costs. Security over the network and in transactions is crucial to this process. In a traditional model, the third party usually provides the security – the bank protects the money or an asset, or maybe a lawyer helps execute a contract – so they can help verify a transaction. But in blockchain, without the existence of a third party, something needs to exist that ensures security.

All the above transactions are authorized using a "Public" cryptographic system consisting of Public & Private keys. Private and public keys are digital assets that, when combined, form a digital signature for an individual, thus enabling the secure transfer of data, money or information. Public keys are widely distributed, while private keys are kept secret and are proprietary to every individual on the blockchain network. The keys are nothing but a very long number sequences that are unique to an individual user.

Let's consider the first transaction where A transferred two bitcoins to D. Here, Mr. A will obtain Mr. D's public key. This public key shall be used to encrypt the transaction of transferring two bitcoins to Mr. D. Hence, this means that only Mr. D's private key can decrypt the information. So when the transaction is received by D , he uses his private key to create a digital signature and then accesses the information on the block. The above applies to all subsequent transactions in the block.

Cryptographic Hash Function

Hashing is the process of taking an input of any length and turning it into a cryptographic fixed output through a mathematical algorithm (Bitcoin uses SHA-256, for example). The primary function of hashing in Blockchain is to generate a "fixed-length" output data that acts as a shortened reference to the original data. The fixed-length output is called a hash. So basically, instead of remembering the input data which could be huge, you can just remember the hash and keep track. Hashing also requires the use of Digital Signatures as mentioned above. The hash code is generated by a "Hashing Algorithm". Hashing enhances security during the process of message transmission when the message is intended for a particular recipient only. An algorithm generates the hash, which helps to protect the security of the transmission against tampering.

In case of the first transaction, where Mr. A transferred two bitcoins to Mr. D, a hash is generated. Each block is identified by a unique hash. Hence, the block is not represented by the transaction but is represented by a hash. A hash somewhat looks like this:

"759831720aa978c890b11f62ae49d2417f600f26aaa51b3291a8d21a4216582a"

Each block in the block chain contains reference to the hash of the previous block that it is linked to. Now for example, the first block stores an additional transaction between Mr. D and Mr. A, the hash completely changes and looks somewhat like this:

"e320b6c2fffc8d750423db8b1eb942ae710e951ed797f7affc8892b0f1fc122b"

Hence even a minute addition to the block results in a new hash altogether. A block cannot be tampered with, as the hash totally changes hence resulting in a break in the chain. The key utility in the hashing process is that you can't reverse-engineer a hash. In other words, you won't be able to work backward from an output string to determine the input data.

Evolution of Blockchain- Permissioned Vs Permissionless

But just as any technology evolves, Blockchain has evolved too. Blockchain has evolved from being a public distributed ledger to a private distributed ledger. They are also known as "Permissioned Blockchains". Permissioned blockchains act as closed ecosystems, where users are not freely able to join the network, see the recorded history, or issue transactions of their own. Permissioned blockchains are preferred by centralized organizations, which leverage the power of the network for their own, internal business operations. Company consortiums are also likely to employ private blockchains to securely record transactions, and exchange information between one another. [2]

Moreover, any organization shifting to blockchain technology would prefer the use of a permissioned blockchain rather than a permissionless blockchain. A permissioned/private blockchain would retain the characteristics of a permissionless/ public blockchain, but only within the boundaries of the organization. Not everyone would have access to view the blockchain, unless they possess the private key of the organization. Hence, a private blockchain is still a public distributed ledger (within the organization), is still immutable and still runs on consensus, but is centrally managed by an organization.

Existing cryptocurrencies such as Bitcoin, Litecoin, Ethereum etc are examples of permissionless blockchains. There is no entry barrier to use it. Anyone can transact within the blockchain with anyone.

[2] https://blockonomi.com/permissioned-vs-permissionless-blockchains/

Blockchain in the world of Auditing & Assurance – Potential Impact, Challenges and Opportunities

Blockchain presents a challenge to the traditional audit approach. It is widely proclaimed by many publications and blockchain experts that the world of Auditing and Assurance will be revolutionized by blockchain. Indeed, Blockchain has also been recognized as *"digital era double-entry bookkeeping"* because of its similarity to old accountancy principles. Also, Blockchain, being a distributed ledger where the data is immutable, creates the perfect audit trial required for an audit.

As stated earlier, Blockchain provides for near real time settlement of transactions. And the record of the same is instantaneously available. This pseudo real-time verification blockchain characteristic could also impact the audit process. Instead of assessments at year end (or interim), audit firms will be in a position to perform continuous on-line assessments throughout the period under audit.[3]

As per SA 200, the objective of the auditor is to obtain reasonable assurance whether the financial statements are free from material misstatement and its prepared using applicable financial reporting framework. To support this, the audit evidence obtained by the auditor should be sufficient and appropriate. Hence, any audit involves an assessment that the recorded transactions are supported by evidence that is relevant, reliable, objective, accurate, and verifiable. Blockchain has the ability to meet the aforesaid criteria, solely due to its underlying characteristics of immutability and transparency, thereby maintaining integrity of the information.

Further, the days of sample based substantive testing will soon be challenged. With the use of blockchain technology, auditors would tend to rely less on audit sampling. Instead, auditors will exploit the possibilities provided by the technology which gives them the ability to test the whole or majority of the population. Hence, detection risk would reduce to an acceptably low level.

A blockchain solution, when combined with appropriate data analytics, could help with the assertions at the transaction level involved in an audit, and the auditor's skills would be better spent considering other strategic aspects. For example, auditing is not just checking the detail of whom a transaction was between and the monetary amount, but also how it is recorded and classified. If a transaction credits cash, is this outflow due to cost of sales or expenses, or is it paying a creditor, or creating an asset?[4].

During statutory audit, blockchain can be used to verify the reported transactions in the financial statements. For example, instead of asking banks to provide the bank statements or asking confirmation from third parties, auditors can verify the publicly available transactions on the blockchain. The transactions once recorded on the blocks, cannot be modified. This

[3] https://www2.deloitte.com/mt/en/pages/audit/articles/mt-blockchain-a-game-changer-for-audit.html

[4] https://www.icaew.com/technical/technology/blockchain/blockchain-articles/blockchain-and-the-accounting-perspective

integrity of data enhances the reliability of audit evidence. This also has it's disadvantage. If any transaction is recorded in error, it cannot be modified under any circumstance. The incorrect entry will be a part of the entire blockchain of the organization. For example, if an entity's employee accidentally or deliberately sends bitcoin to a wrong or unauthorized address (recipient), there is currently no way to reverse that transaction. It is therefore very crucial for the auditor to assess whether effective automated controls are in place to validate transactions before they are executed. Hence a fraud cannot occur by modifying the information on the block. But a fraud can occur by reporting an incorrect transaction in the first place. But due to the characteristic of consensus, it is an established fact that incorrect transactions will not be accepted and shall not form part of the block under any circumstance. Hence the need to obtain reasonable assurance about the reliability of the data on the blockchain, will make the auditor a bloodhound. In order to do this the auditor will have to gain an understanding of how the consensus protocol works and has to assess it's reliability for the specific blockchain. This assessment may need to include consideration of whether the protocol could be manipulated.

According to a study in 2011, hidden documents/information, altered documents, fake documents and collusion with third parties total 81% of evidence schemes, through which management creates or hides evidence to conceal the fraud. Premature revenue recognition, fictitious revenues, overvalued assets and understated expenses, omitted or understated expenses/liabilities total 78% of account schemes, through which management perpetrates fraud by manipulating account balances or disclosures. [5] Hence, having a blockchain system where accountants must input crucial documents and information in a secure manner, would have a considerable positive impact in the reduction of that kind of frauds.

In a traditional audit, any information requested from the client such as, reconciliations, trial balances, journals, ledgers etc are provided to an auditor in a variety of electronic and manual formats. The auditor has to then analyse the information in order to determine the level of materiality, areas to focus upon and ultimately draw up the audit plan.[6] This cycle is very time-consuming subject to the quantity of data that is provided. But blockchain technology offers an opportunity to streamline financial reporting and audit processes. In a blockchain world, the auditor could have near real-time data access via read-only nodes on blockchains. Hence, instead of assessments at year end (or interim), audit firms will be in a position to perform continuous on-line assessments throughout the period under audit. Real-time auditing and reporting will release CFOs and their teams from certain routine, time-consuming tasks so that they can play more strategic, creative roles – and focus on new ways to deliver future business value, rather than keeping track of past costs. And human interpretation of data and transaction patterns will still be needed to generate the new insights that can lead to business growth.[7]

In large organisations, an internal audit is carried out by a team of professionals in the organisation. Although not mandatory, it is generally conducted with the aim to evaluate the effectiveness of internal control, the soundness of the financial system, efficiency of business processes and so on. Internal audit is not required to provide assurance services but analyse

---

[5] **L. Gao and R. Srivastava, "The Anatomy of Management Fraud Schemes: Analyses and Implications," Indian Accounting Review, Jun-2011**

[6] https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf

[7] *https://www.ey.com/en_gl/digital/blockchain-why-finance-and-auditing-will-never-be-the-same*

and anticipate various risks and address these risks in an appropriate manner. In today's constantly evolving world, every organization is innovating and improving. This calls for the internal audit function also keep pace with the climate of constant disruption by employing advanced analytics and focusing on newer technologies. This automatically requires internal auditors to proactively acquaint themselves with the opportunities and risks emerging from the implementation of this technology. It is also imperative that Internal auditors must be involved at the planning stage of blockchain-based applications. All systems must have adequate governance, risk management, and controls, and it is much easier to build these right from the start than to retrofit them after a problem has been identified.

Last but not the least the relevant statutory bodies, within and outside India will need to come up with standards and guidelines with respect to auditing in a Blockchain environment. These standards and guidelines will have to keep with the ever-increasing pace of the technology and should be able to adequately address the risks and issues associated with the use of such technology. But importantly, the statutory bodies will have to cooperate with each other in determining the optimal approach and reporting standards while auditing in the blockchain environment, thereby making the work performed by the auditors internationally accepted.

Conclusion

It is undoubtful that the blockchain technology can have a profoundly positive impact on the auditing and environment and bring much-needed optimisation to the existing processes. But despite the level of automation and continuous audit, auditors will still have to use professional scepticism and apply professional judgement during the course of the audit. Indeed, blockchain may render many current risks related to financial statement opinions obsolete. Auditors should be aware of the new risks and their impact on traditional audit procedures. Identifying the risks associated with blockchain and learning how to use the technology for a competitive advantage can help auditors maintain and increase their relevance in the business environment. In a nutshell, Blockchain will change the way auditors operate, it will enhance the quality of the audit, but the objective of an auditor's job will continue to be relevant.