Rosary College of Commerce & Arts

Navelim, Salcete-Goa.

Department of Computer Applications

BITS N BYTES

DECEMBER 2022

From the Principal's Desk

The rapidly evolving education system in our Country focuses on critical thinking, life skills, analytical skills, value education and decision-making skills. It enables students to understand complex issues with ease and face varied situations with confidence.
Technology plays an important role in education today. The availability of video lectures, recordings and digital resources enables students to choose when and where to learn, at their own pace.

The implementation of the National Education Policy (NEP) 2020 in our country will provide an opportunity to students to learn skill-based courses of their choice and give multiple exit options to students pursuing their under graduates studies. It also encourages foreign universities to set up their campuses in India. The concepts of resource sharing, cooperative and collaborative learning emphasized in NEP 2020 will contribute substantially to the improvement of education in our country.

The current issue of the newsletter *‘Bits and Bytes’* published by the Department of Computer Applications has interesting contributions from faculty and students on Blockchain Technology and its importance in education as well as business. I am sure *‘Bits and Bytes’* will make an engrossing reading.

Congratulations to the Department of Computer Applications and the editorial board for their hard work and contributions.

Prof. Helic M. Barretto
Principal

Blockchain: A Primer

- Asst . Prof. Anusree Sadanand

Introduction

In the last few years, we might have heard about Blockchain technology and mostly as a technology that is used to power cryptocurrencies like bitcoin, ether. While Bitcoin is used widely as a successful decentralized financial transaction system, other proposed platforms are trying to cover other use cases more than just the cryptocurrency. It could revolutionize the internet of today

“...I have a dream for the Web [in which computers] become capable of analysing all the data on the Web: the content, links, and transactions between people and computers. A ‘Semantic Web’, which should make this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled by machines talking to machines. The ‘intelligent agents’ people have touted for ages will finally materialize...” --Tim Berners-Lee.

Blockchain technology is a step towards ‘Sematic Web’

So, what is Blockchain?

Blockchain a sentence can be mentioned as decentralized storage of data in the form of blocks in which blocks are connected. Now let us analyse the above sentences little more;

The first important concept here is decentralization

What is decentralization? traditionally data is stored centrally in single system or servers which has all the data (there can be clones of the servers, which also have the same data)and any system requiring data from that system has to send a request to it and the server replies with a response. In decentralized scenario the data is stored in many systems and are connected securely with each another. No centralized "official" copy exists and no user is "trusted" more than any other. Hence it is also called trust-less network, which also implies that such networks can be used to collaborate within a group of people who do not trust each but have to work together to achieve a common goal.

The next important concept here is blocks. Block is a basically a data structure which are connected using cryptographic functions or hash function. These functions take a raw data and encodes it to make it in unintelligible. Blocks hold batches of valid transactions that are hashed. Each block includes the hash value of the prior block, linking the two. The linked blocks form a chain. This process confirms the integrity of the previous block, all the way back to the initial block, which is known as the *genesis block* (Block 0).

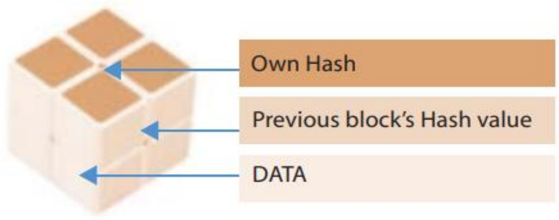
So blockchain is a distributed ledger that provides a way for information tobe recorded and shared by any group of people. The information could represent transactions, contracts, assets, identities, or practically anything else that can be described in digital form.

Entries are permanent, transparent, and searchable, which makes it possible to view transaction histories in their entirety.

Structure of Blockchain

A blockchain consists of blocks, each block containing the data, its own hash value (a unique cryptographic value containing characters and numbers generated through a complex computational algorithm) and a pointer to the hash of the previous block.

The fig below shows the basic structure of the block:



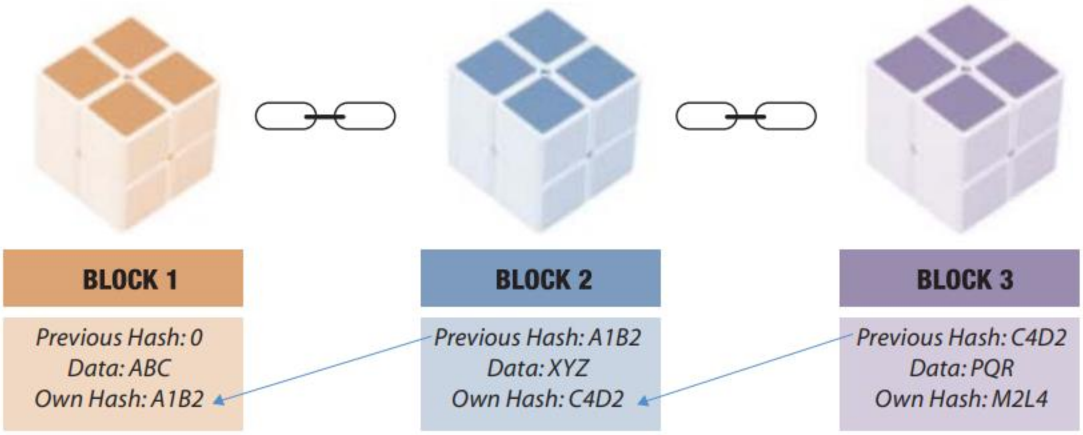
Here the **hash** is calculated using SHA 256 algorithm, which is an advanced algorithm for calculating the hash value.

Example, the hash value for ‘hello world’ is b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

And the hash value for hello world! is 7509e5bda0c762d2bac7f90d758b5b2263fa01ccbc542ab5e3df163be08e6ca9

Note the huge difference the single character makes and also note the both the hash values are of the same size.

The figure below depicts blockchain having different blocks looks like.



As seen in the figure the chaining of the blockchain happens because the previous hash is stored in each block. The immediate implication of this is that any change to the data changes the whole block which in turn disrupts the chain. In such cases the changed data is not accepted.

types of data can be the following types:

Blockchains are typically used to store records of:

- Asset Transactions: Asset Transactions are mostly money, expressed in units of a currency or Documentary evidence of ownership rights, commonly used to represent immovable property such as land, or intangible property such as intellectual property rights.
- Smart contracts: Smart contracts are effectively small computer programmes stored on a blockchain, which will perform a transaction under specified conditions. A smart contract is self-executing - that is, once the instructions are written to a blockchain, the transaction will take place automatically when the appropriate conditions are detected, with no further actions required by the parties to the transaction or other third parties.
- Digital signatures and certificates: Blockchains can be used to either store cryptographic hashes ("digital fingerprints") of the certificates, or to store the claims themselves. Thus, a blockchain can take on the function of a public certificate registry.

Consensus Mechanism

Since blockchain is an open network, it is important to form an agreement on who creates the blocks. Blocks are mostly of 1 MB size and the people who creates the blocks are called miners. These miners compete on different criteria to able to create the blocks and the those who create these blocks are awarded with a cryptocurrency.

let us look into the different criteria on which the miners are selected to create the blocks:

Proof of work (PoW): PoW requires the initiator to solve a puzzle, a mathematical or cryptographic operation by brute forcing and to produce a value (also called wining value), which is less than a defined one as set forth by the network.
The miner who solves the puzzle first will be allowed to create the new block and add the block to the chain .This method usually requires the miners to invest a huge amount in computing power, So as to be able to create the block and get the reward.

Proof-of-Stake (PoS): PoS method uses already existing cryptocurrency. The miner is selected in proportion to the number of cryptocurrencies he owns. This method uses much less energy than PoW and is preferred than PoW for many modern blockchain networks.

Proof of Burn (PoB): In PoB miners 'burn' coins by sending them to an address from where they are irretrievable. By sending the coins to an unreachable address, miners earn a privilege to mine on the system based on a random selection process. The more coins they burn, the better are their chances of being selected to mine the next block.

Proof of Elapsed Time: PoET is one of the fairest consensus algorithms. Here the miners wait for a random amount of time, proof has to be submitted that it had shortest-wait-time before it is allowed to start mining the next block. Since it relies on specialized hardware, it is the main drawback of utilizing this consensus mechanism. The block from the winning miner node gets appended to the Blockchain.

Apart from the above consensus method there are many more like, Byzantine Fault Tolerance, Practical Byzantine Fault Tolerance (PBFT) which are also widely used.

Types of blockchain

Public blockchain.

A public, or permission-less, blockchain network is one where anyone can participate without restrictions. Most types of cryptocurrencies run on a public blockchain that is governed by rules or consensus algorithms. E.g. Bitcoin, Ethereum all are public network

Permissioned or private blockchain.

A private, or permissioned, blockchain allows organizations to set controls on who can access blockchain data. Only users who are granted permissions can access specific sets of data. Oracle Blockchain, Hyperledger fabricare a permissioned blockchain. If any organisation wants to use a blockchain to solve any of their problems they mostly use permissioned blockchain

Federated or consortium blockchain.

Consortium blockchains are permissioned blockchains supervised by a group of organizations, unlike a private blockchain that is governed by a single entity or an organization.These blockchains are more decentralized as the authority is shared among a few organizations.

Hybrid blockchains

A hybrid blockchain has a combination of centralized and decentralized features. It is the mixed content of the private and public blockchain, where some part is controlled by some organization and other makes are made visible as a public blockchain.

Use cases of Blockchain

There are many applications and domains in which blockchain can be used for the benefit of all the stakeholders. Cryptocurrency is the most well known ,but blockchain as a technology can used for solving wide range of problems, specifically when we need a security ,integrity and cooperation among parties who do not trust each other but have to work together

Cryptocurrencies

Most cryptocurrencies use blockchain technology to record transactions. For example, the bitcoin network and Ethereum network are both based on blockchain. Miners are paid in cryptocurrencies to create blocks in the blockchains of bitcoin and Ethereum.

Governments have mixed policies on the legality of their citizens or banks owning cryptocurrencies, many countries, including India are launching their own central bank cryptocurrency (CBDC) so as not be left out and keep the citizen’s money in formal economy.

Financial services

Using blockchain for exchanges allows for faster and less expensive transactions. Moreover, it doesn't require investors to deposit their assets with the centralized authority, which means they maintain greater control and security. Banks are interested in this technology not least because it has the potential to speed up back-office settlement systems. Money transfers using blockchain can be less expensive and faster than using existing money transfer services. This is especially true of cross-border transactions, which are often slow and expensive. Even in the modern U.S. financial system, money transfers between accounts can take days, while a blockchain transaction takes minutes.

Supply chain: Supply chain is another domain, where keeping track of all the goods involved is very complicated process. When goods travel from one place to another a lot of documentation is involved. Blockchain can make all these tracking very easy and transparent. The paperwork involved can also be reduced tremendously since the verified data will always be available .example in Shipping industry blockchain-based platform ecosystem that would create value across the global shipping supply chains.

Blockchain Healthcare: Individual Health records could be encoded and placed with a private key on the blockchain which would allow the admittance only to the authorized people. Medicine records, Surgery receipts could be kept on a blockchain and be accessed as required and keeping data on blockchain is more secure, as the data is decentralized. These days health records often fall prey to ransomware.

Food Safety: One more important domain where blockchain could be used for tracking the food right from farm to plate. Since the block chain data is changeless; you can verify the claims made by the food retailers and suppliers.

Web3:Blockchain will power the next generation of internet where instead of transferring data in the form of documents, the internet itself will become intelligent enough to analyse the data and dissipate knowledge instead of just raw information. Web3 protocol enable the direct exchange of value between users, removing the need for trusted intermediaries. The peer-to-peer character of web3 means it represents a more democratic vision for the web than its current iteration, Web 2.0, which is dominated by powerful intermediary platforms (Facebook, Amazon, Apple, Google and other big tech companies).

Apart from the above applications it can also used for many other applications like Blockchain is also being used in peer-to-peer energy trading.

In conclusion blockchain is a technology that can cause major disruption in the way we process, transfer and use information.

Top Applications of Blockchain in the Real World

- Asst . Prof. Mildred Lemos

Blockchain Technology was first created to enable crypto currency but has been slowly gaining momentum and is being increasingly used in various other industries. Blockchain could solve the anti-trust problems through greater transparency. The biggest advantage for blockchain in cyber security is that it provides end-to-end encryption and privacy and removes the risk of a single point of failure.

Blockchain has applications in healthcare, finance, government, Capital markets, Insurance etc

Some of the major contributions of Blockchain are as follows :

Healthcare

With blockchain applications in healthcare, medical records can be safely published and only authorized persons would be able to can access it anywhere in the world. Blockchain is used for health record-keeping, clinical trial, patient monitoring It can be used to maintain the financial statements in hospitals and minimize the data transformation time and cost.

Health-care systems may use blockchain to securely store medical records and update patient data across different facilities and regions in real-time. By concealing the identity of any individual with complex and secure codes that can protect the sensitivity of medical data. The decentralized nature of the technology also allows patients, doctors and healthcare providers to share the same information quickly and safely. This would allow healthcare facilities to devote more time and money to patient care and innovation rather than administration.

Copyright and Royalties

Copyright and royalties are a big issue in creative sectors like music, films, etc. and Blockchain can be important in ensuring security and transparency in the creative industries where there are many instances of music, films, art being plagiarized and original artists not getting their due credit . This can be rectified using Blockchain which has a detailed ledger of artist rights. Blockchain is also transparent and can provide a secure record of artist royalties and deals with big production companies. The payment of royalties can also be managed using digital currencies like Bitcoin.

Insurance

Smart contracts can be used in the Insurance Industry. These contracts allow customers and insurers to manage claims in a transparent and secure manner. Unlike physical contracts, smart contracts can track insurance claims and hold both parties accountable. Insurance policies could be written as coded, decentralized smart contracts in which an individual agrees to pay the insurance company money in return for the company’s promise to help cover that person’s future medical costs.

Blockchain smart contracts will create immutable data based on an insurance policy owner’s records that can immediately accept or refute any insurance claims made to the company. All contracts and claims can be recorded on the blockchain and validated by the network, which would eliminate invalid claims, since the blockchain would reject multiple claims on the same accident or life.

Birth and Death Certificates

There are many people in the world who don’t have a legitimate birth certificate while the problem is similar to death certificates as well. Blockchain can help in solving this problem by creating a secure repository of birth and death certificates that are verified and can only be accessed by the authorized people.

Providing fair Elections

Fake voting has been increasingly becoming an issue in many countries leading to a distrust among voters in the electoral process. Blockchain technology has the ability to make the voting process easily accessible while improving security. Hackers would be no match to blockchain technology, because even if someone were to access the terminal, they wouldn’t be able to affect all nodes. Each vote would be attributed to one ID, and with the ability to create a fake ID being impossible, government officials could tally votes more efficiently and effectively