Rosary College of Commerce & Arts

Navelim, Salcete-Goa.

Department of Computer Applications

BITS N BYTES

Vol : XVIII August 2021 Issue : 2

Principal's Message

The world has moved from the traditional money concept to the digital currency which is used as a means of payment, a store of value and a unit of account. Digital Cryptocurrency is a digital payment maintained by a network of computers that uses cryptography to authenticate transactions. These currencies do not have a physical form and the transactions take place over the internet thereby removing the costs associated with distributing notes and coins. Digital Cryptocurrencies are not issued by a government body which makes them risky.

I am happy that our Department of Computer Applications is bringing up this new issue of Bits N Bytes focused on Cryptocurrencies. Through this electronic platform our students and teachers of Computer Applications can express their views and ideas in this emerging field that could benefit society at large.

I congratulate Asst. Prof Mildred Lemos and all who have contributed to Bits N Bytes.

I hope and wish Bits N Bytes will inspire and ignite many minds.

Dr. Helic Barretto

Acting Principal

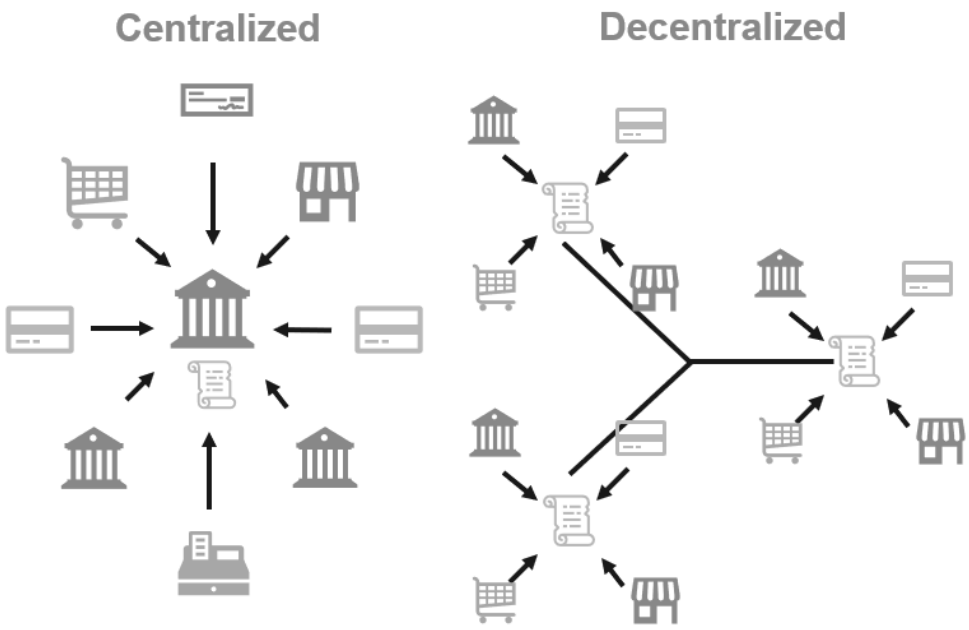
What is Cryptocurrency?

- Asst. Prof. Ramakrishna Reddy

A cryptocurrency or crypto is a digital currency and you can think of it as a digital dollar or digital INR as instead of paper money, it uses an online ledger for transactions. They provide a medium of exchange and allow individuals to directly make payments to each other.

How cryptocurrency works is on a technology called Blockchain which provides a peer-to-peer network and transactions are recorded on the blocks of the blockchain.

Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency. The interest in Blockchain technology has been increasing since the idea was coined in 2008. The reason for the interest in Blockchain is its central attributes that provide security, anonymity and data integrity without any third party organization in control of the transactions, and therefore it creates interesting research areas, especially from the perspective of technical challenges and limitations.



Blockchain technology has also some technical challenges and limitations that have been identified.:

- Throughput: The potential throughput of issues in the Bitcoin network is currently maximized to 7tps (transactions per second). Other transaction processing networks are VISA (2,000tps) and Twitter (5,000tps). When the frequency of transactions in Blockchain increases to similar levels, the throughput of the Blockchain network needs to be improved.

- Latency: To create sufficient security for a Bitcoin transaction block, it takes currently roughly 10 minutes to complete one transaction. To achieve efficiency in security, more time has to be spent on a block, because it has to outweigh the cost of double spending attacks. Double-spending is the result of successful spending of money more than once. Bitcoin protects against double spending by verifying each transaction added to the block chain, to ensure that the inputs for the transaction have not been spent previously. This makes latency a big issue in Blockchain currently. Making a block and confirming the transaction should happen in seconds, while maintaining security. To complete a transaction e.g. in VISA takes only a few seconds, which is a huge advantage compared to Blockchain.

- Size and bandwidth: At the moment, the size of a Blockchain in the Bitcoin network is over 50,000MB (February 2016). When the throughput increases to the levels of VISA, Blockchain could grow 214PB in each year. The Bitcoin community assumes that the size of one block is 1MB, and a block is created every ten minutes . Therefore, there is a limitation in the number of transactions that can be handled (on average 500 transactions in one block). If the Blockchain needs to control more transactions, the size and bandwidth issues have to be solved.

- Security: The current Blockchain has a possibility of a 51% attack. In a 51% attack a single entity would have full control of the majority of the network's mining hash-rate and would be able to manipulate Blockchain. To overcome this issue, more research on security is necessary.

- Wasted resources: Mining Bitcoin wastes huge amounts of energy ($15million/day). The waste in Bitcoin is caused by the Proof-of-Work effort. There are some alternatives in industry fields, such as proof-of-stake. With Proof-of-Work, the probability of mining a block depends on

the work done by the miner. However, in Proof-of-Stake, the resource that is compared is the amount of Bitcoin a miner holds. For example, someone holding 1% of the Bitcoin can mine 1% of the “Proof-of-Stake blocks”. The issue with wasted resources needs to be solved to have more efficient mining in Blockchain.

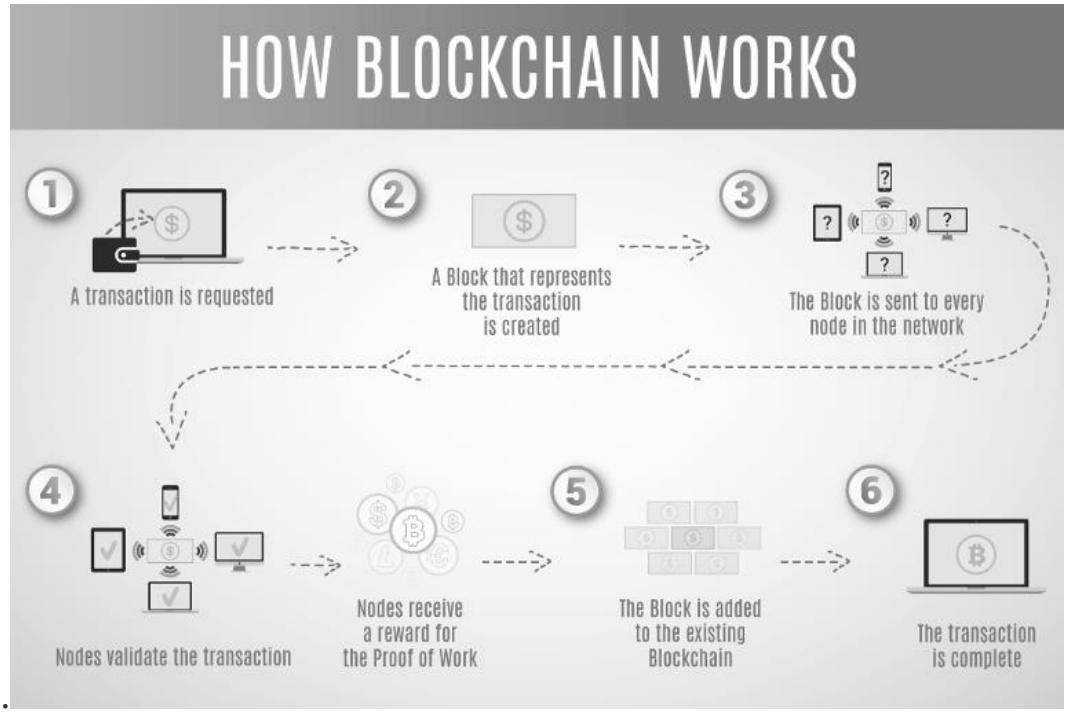
- Usability: The Bit coin API for developing services is difficult to use. There is a need to develop a more developer-friendly API for Blockchain. This could resemble REST APIs.

- Versioning, hard forks, multiple chains: A small chain that consists of a small number of nodes has a higher possibility of a 51% attack. Another issue emerges when chains are split for administrative or versioning purposes.

The decentralized nature of the blockchain makes cryptocurrencies immune to the old ways of government control and interference. Transactions are secured as the technology uses cryptography and are validated using a consensus mechanism such as Proof-of-stake

Various computers that are connected to a blockchain verify transactions on the network using these consensus mechanisms.

Upon successful verification of transactions, these transactions are grouped and chained together as blocks in the blockchain. This process of creating new blocks is known as mining and the people doing it are called miners. Miners are rewarded for their effort and resources spent on mining, in the form of crypto paybacks. Hence, the technology provides an incentive for people to maintain the blockchain and establish its authenticity.



Source: MLSDev

The technology is such that it provides:

- Transparency of transaction data
- Faster transfer of payments
- Lower transaction costs
- Secure payments

Why cryptos are a way to solve the digital cash problem is that they are creating a new path towards a cashless economy and apart from payments they provide several other use-cases. Bitcoin is the largest cryptocurrency and what makes Bitcoin so valuable is its limited supply of 21 million, unlike fiat currency.

Ethereum, the second-largest cryptocurrency provides various other use-cases such as Decentralised Finance (DeFi) and Non-Fungible Tokens (NFTs) which have grown in popularity as it empowers individuals, removes intermediaries such as banks and financial institutions and allows different parties to deal directly with each other.

Bitcoins – The Oldest Cryptocurrency

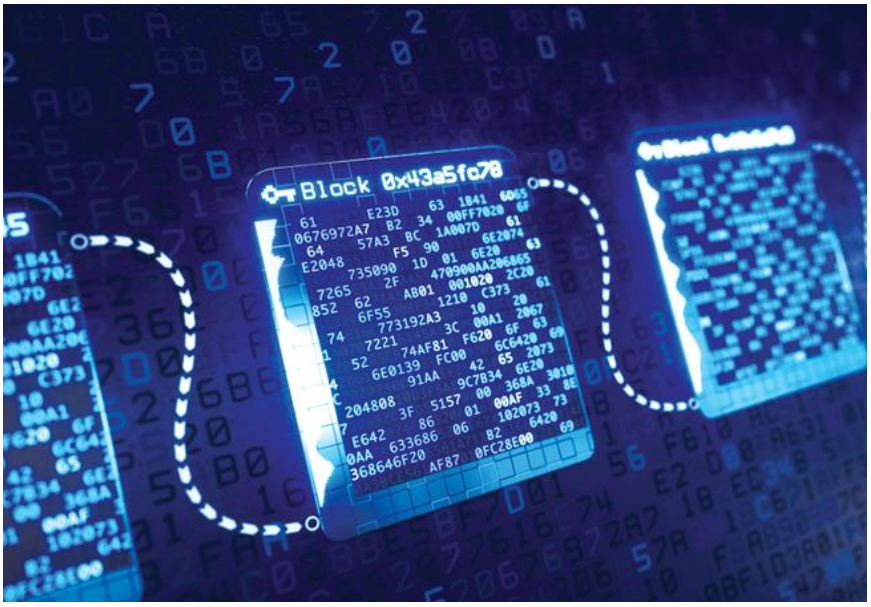
- Asst. Prof. Mildred Lemos

Cryptocurrency is a digital currency backed by encryption, and generated through complex mathematical equations. In 2009, the first decentralized cryptocurrency, bitcoin was created by presumably pseudonymous developer Satoshi Nakamoto. The identity of the person or persons who created the technology is still unknown. Bitcoin offers the promise of lower transaction fees compared to traditional online payment mechanisms and, unlike government-issued currencies, it is operated by a decentralized authority.

Bitcoins are not printed like paper money, coins or notes but are based on math and cryptography. The transactions are handled by a network of decentralized computers running the bitcoin software, all transactions are anonymous and no personal information is needed to buy or sell things with it.

There are no physical bitcoins, only balances kept on a public ledger that everyone has transparent access to. All bitcoin transactions are verified by a massive amount of computing power. Though it not consider legal tender in India and most parts of the world, bitcoin is very popular, it has given massive gains and has triggered the launch of numerous of other cryptocurrencies, collectively referred to as altcoins.

Bitcoins are based on the Blockchain technology. A blockchain is a growing list of records, called blocks, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Blockchains are typically managed by a peer-to-peer network for use as a publicly distributed digital ledger, where nodes collectively adhere to a protocol to communicate and validate new blocks.



Blocks in the Blockchain

The digital ledger stores every transaction that has ever occurred in bitcoin. These transaction records cannot be altered or reversed without the agreement of everyone on the bitcoin network. Unlike a bank's ledger which has a centralized network, blockchain protects the user's identity and is anonymous. Therefore, making it a more secure way to carry out a transaction.As the blockchain comprises of data containing blocks linking to the earlier blocks, an attempt to spending the same bitcoin twice would mean changing the entire link in the chain. Furthermore, as miners are competing with each other, each one checks the others work thoroughly at every stageand double spending of the same bitcoin can be easily detected.

The process of creating Bitcoin and other cryptocurrency is called mining.In this process, large, sophisticated computers are used to solve complex equations and the user earns Bitcoins as a reward for successfully doing that. It is then traded on dedicated exchanges. People can also buy cryptocurrency in a peer-to-peer exchange by investing actual money.

The real value of bitcoin is on the rate it can command i.e how much people are willing to pay for it and how many people want to buy it. With the volatility of bitcoin and other cryptocurrencies, it is difficult to predict whether or not these currencies will be widely accepted in the future. As a result, investors should plan for both outcomes by building up a diversification portfolio.