

BLOCKCHAIN

Athira Biju
MCA-B
Roll No:4

Blockchain

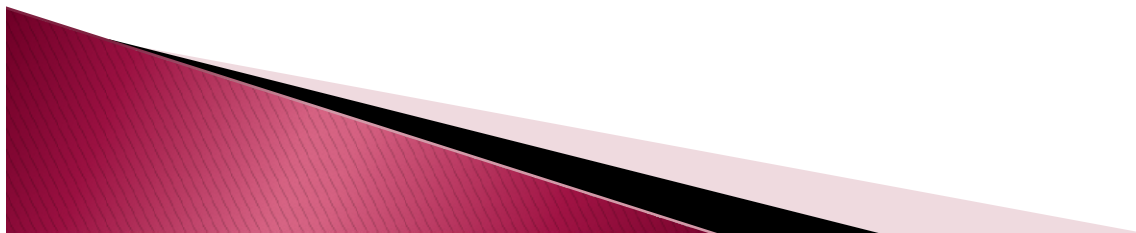
A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.



- ▶ One key difference between a typical database and a blockchain is how the data is structured.
- ▶ A blockchain collects information together in groups, known as blocks, that hold sets of information.
- ▶ Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain.
- ▶ All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled.

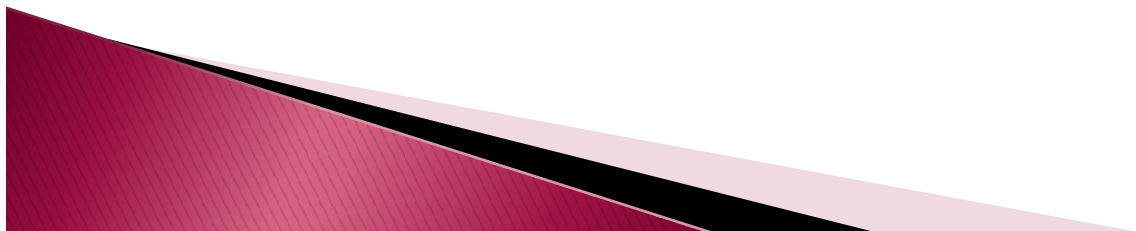


- ▶ As new data comes in, it is entered into a fresh block. Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in chronological order.
- ▶ In Bitcoin's case, blockchain is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control.
- ▶ Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.

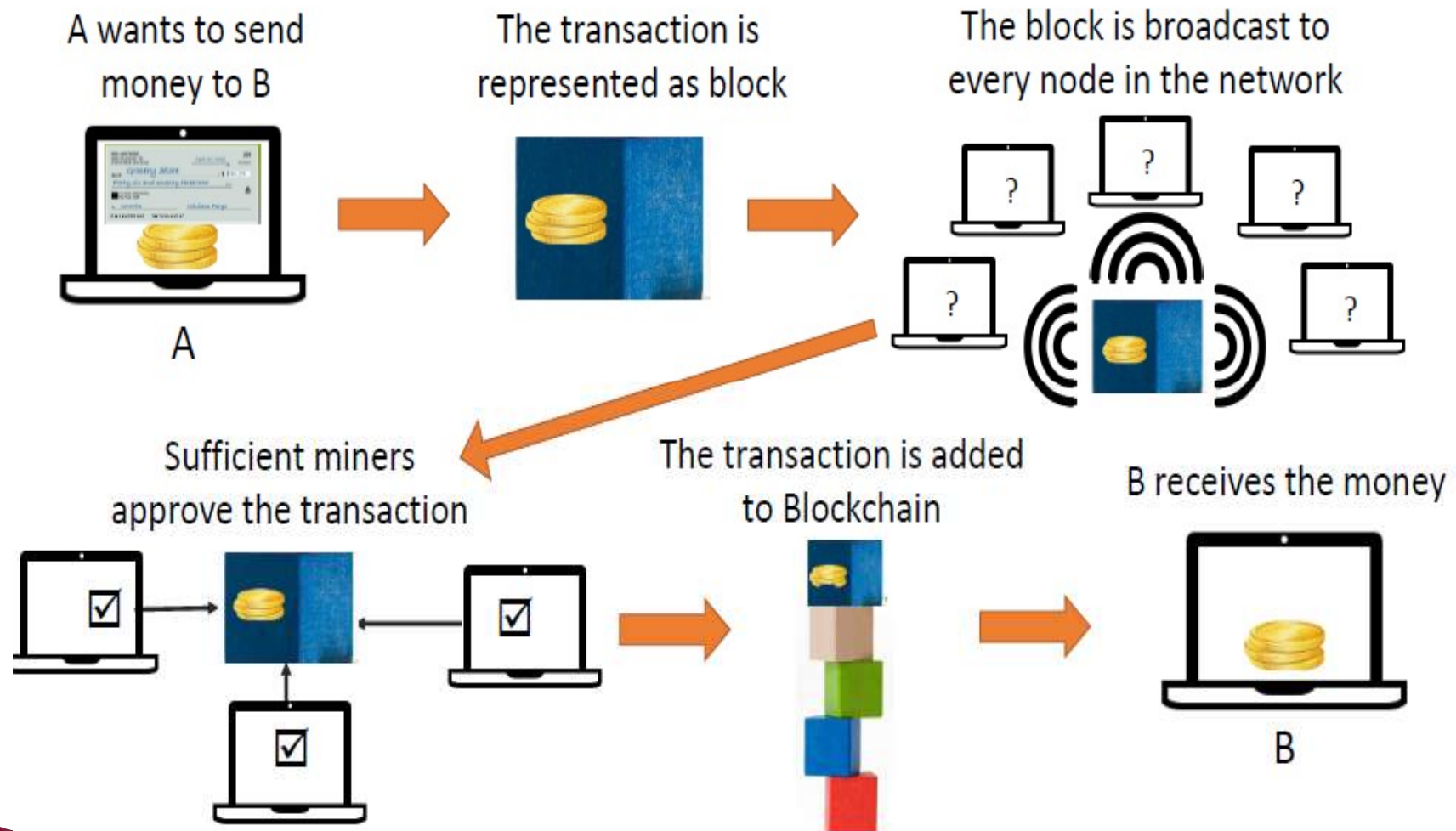


Bitcoin vs. Blockchain

- ▶ Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application.¹
- ▶ The Bitcoin protocol is built on a blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator, Satoshi Nakamoto, referred to it as “a new electronic cash system that's fully peer-to-peer, with no trusted third party.”



How Blockchain works?



Is Blockchain Secure?

- ▶ Blockchain technology achieves decentralized security and trust in several ways. To begin with, new blocks are always stored linearly and chronologically. That is, they are always added to the “end” of the blockchain. After a block has been added to the end of the blockchain, it is extremely difficult to go back and alter the contents of the block unless a majority of the network has reached a consensus to do so. That’s because each block contains its own hash, along with the hash of the block before it, as well as the previously mentioned timestamp. Hash codes are created by a mathematical function that turns digital information into a string of numbers and letters. If that information is edited in any way, then the hash code changes as well.



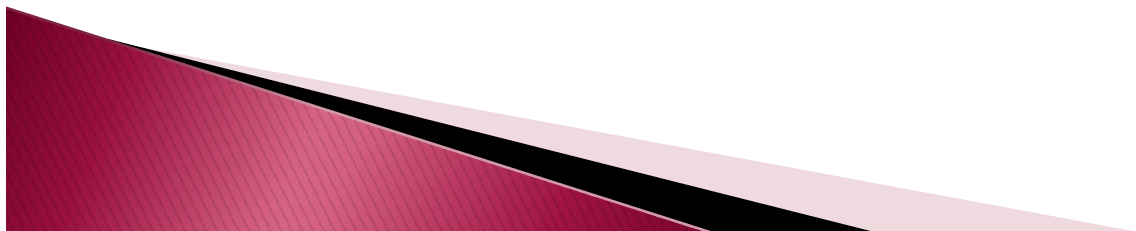
Types of blockchain networks

- ▶ **Public blockchain networks**

A public blockchain is one that anyone can join and participate in, such as Bitcoin. Drawbacks might include substantial computational power required, little or no privacy for transactions, and weak security. These are important considerations for enterprise use cases of blockchain.

- ▶ **Private blockchain networks**

A private blockchain network, similar to a public blockchain network, is a decentralized peer-to-peer network. However, one organization governs the network, controlling who is allowed to participate, execute a consensus protocol and maintain the shared ledger. Depending on the use case, this can significantly boost trust and confidence between participants. A private blockchain can be run behind a corporate firewall and even be hosted on premises.



- ▶ **Permissioned blockchain networks**

Businesses who set up a private blockchain will generally set up a permissioned blockchain network. It is important to note that public blockchain networks can also be permissioned. This places restrictions on who is allowed to participate in the network and in what transactions. Participants need to obtain an invitation or permission to join.

- ▶ **Consortium blockchains**

Multiple organizations can share the responsibilities of maintaining a blockchain. These pre-selected organizations determine who may submit transactions or access the data. A consortium blockchain is ideal for business when all participants need to be permissioned and have a shared responsibility for the blockchain.




Benefits

► **Cost Reductions**

Typically, consumers pay a bank to verify a transaction, a notary to sign a document, or a minister to perform a marriage. Blockchain eliminates the need for third-party verification—and, with it, their associated costs. For example, business owners incur a small fee whenever they accept payments using credit cards, because banks and payment-processing companies have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has limited transaction fees.

► **Decentralization**

Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes more difficult to tamper with. If a copy of the blockchain fell into the hands of a hacker, only a single copy of the information, rather than the entire network, would be compromised.

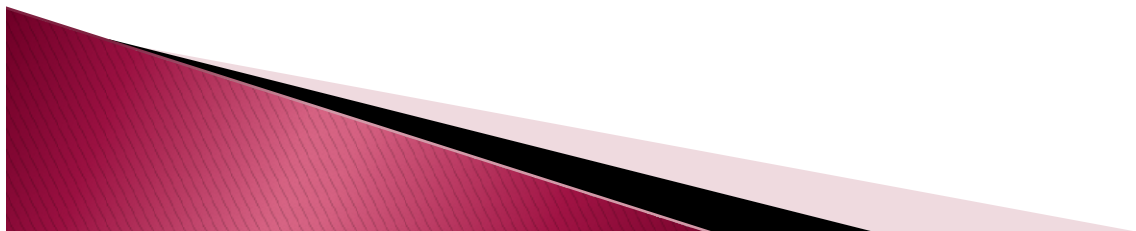


- ▶ **Secure Transactions**

Once a transaction is recorded, its authenticity must be verified by the blockchain network. Thousands of computers on the blockchain rush to confirm that the details of the purchase are correct. After a computer has validated the transaction, it is added to the blockchain block. Each block on the blockchain contains its own unique hash, along with the unique hash of the block before it. When the information on a block is edited in any way, that block's hash code changes—however, the hash code on the block after it would not. This discrepancy makes it extremely difficult for information on the blockchain to be changed without notice.

- ▶ **Transparency**

Most blockchains are entirely open-source software. This means that anyone and everyone can view its code. This gives auditors the ability to review cryptocurrencies like Bitcoin for security. This also means that there is no real authority on who controls Bitcoin's code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile, then Bitcoin can be updated.



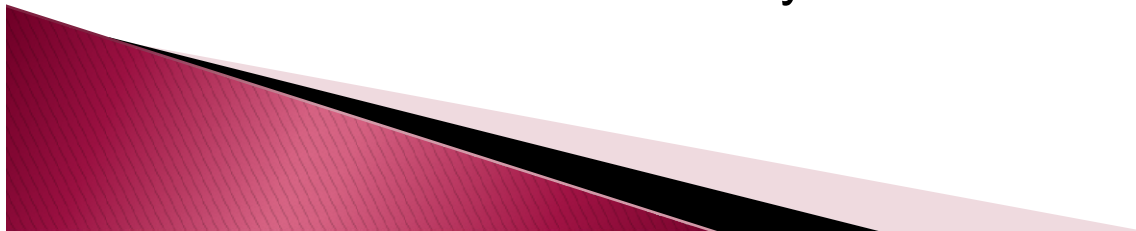
Drawbacks of Blockchains

- ▶ Speed and Data Inefficiency

Bitcoin is a perfect case study for the possible inefficiencies of blockchain. Bitcoin's PoW system takes about 10 minutes to add a new block to the blockchain. At that rate, it's estimated that the blockchain network can only manage about seven transactions per second (TPS). Although other cryptocurrencies such as Ethereum perform better than bitcoin, they are still limited by blockchain.

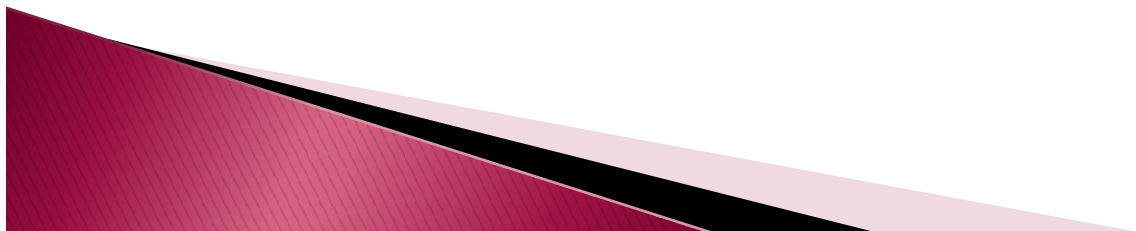
- ▶ Illegal Activity

While confidentiality on the blockchain network protects users from hacks and preserves privacy, it also allows for illegal trading and activity on the blockchain network. The most cited example of blockchain being used for illicit transactions is probably the [Silk Road](#), an online dark web illegal-drug and money laundering marketplace operating from February 2011 until October 2013, when it was shut down by the FBI.



How Many Blockchains Are There?

The number of live blockchains is growing every day at an ever-increasing pace. As of 2022, there are more than 10,000 active cryptocurrencies based on blockchain, with several hundred more non-cryptocurrency blockchains.



THANK YOU

