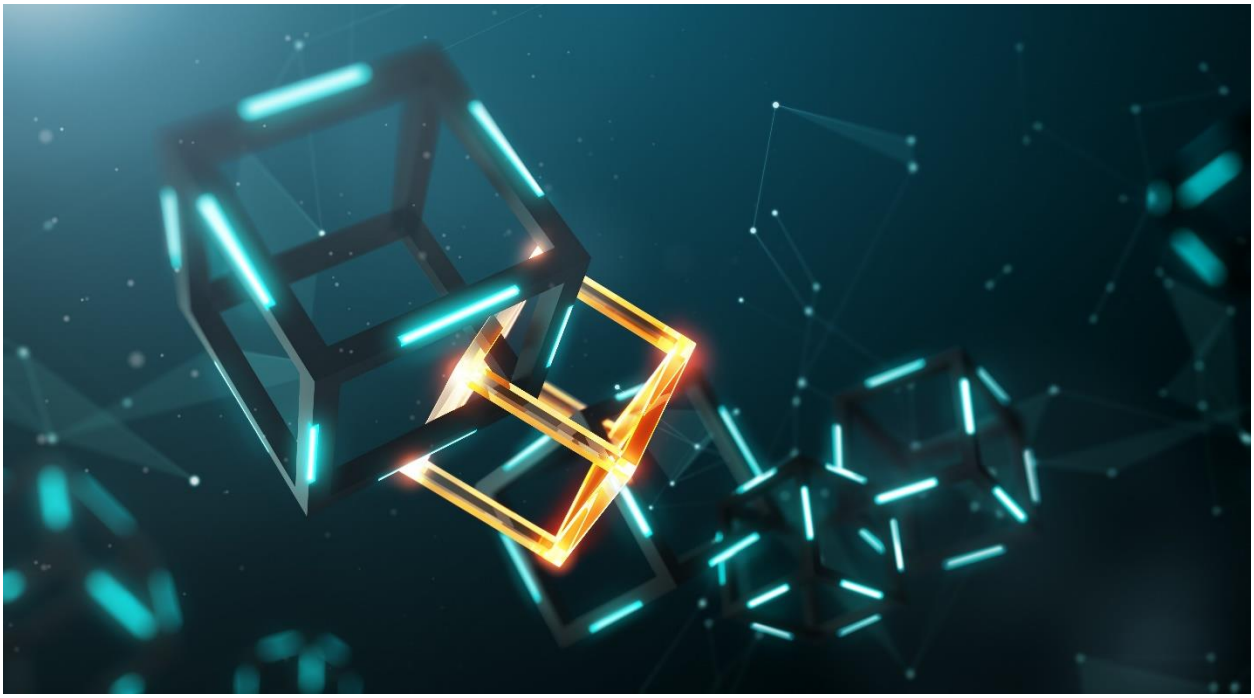
Blockchain – An Electrosoft Whitepaper

Faraaz Khan



What is a Blockchain?

A Blockchain, as the name suggests, is a chain of blocks (i.e., collection of information). The information is contained in blocks, which are linked with each other to form a Blockchain. It is essentially a digital ledger of transactions that is duplicated and distributed across an intended network of computer systems, also known as nodes on the blockchain. Each block has information about the block added to the chain immediately before it. This information includes a hash of the previously added block, a timestamp and transaction data.

To understand the concept, let us take an example of Google Docs. Upon creation of a Google document, the creator shares the link to the document with others. Unlike a paper document, each user gets their own copy to edit rather than getting the original. Users make changes to the document and all user updates are recorded with each user seeing the other's changes transparently. We can also think of Blockchain as something similar to a database, which is a collection of information that is stored electronically on a computer system. Of course, when we look at a database, we have an administrator who is in charge of changing, editing, adding, or deleting entries. This is where Blockchain is

different as there is no one person or administrator is in charge of making these modifications to a Blockchain ledger. Entries cannot be modified, money cannot be double spent, and everyone who is a part of the ledger has a copy of it and is notified of changes.

The Blockchain Architecture

Figure 1 illustrates the structure of a typical Blockchain. Blocks 1, 2 and 3 contain information including hashes, transaction data and timestamps.

There is another block known as the Genesis block, which is the 0^{th} Block or Block 0. The genesis block is the first block in any blockchain. It is the foundation on which the subsequent blocks (i.e., blocks 1,2,3, etc.) are added further to form a chain of blocks - hence the term blockchain. As mentioned before, every block in a blockchain stores a reference to the previous block. But in the case of Genesis Block, there is no previous block for reference. The genesis block has its previous hash value set to 0 and the genesis block is almost always hardcoded into the software of the applications that utilize its block chain.

Figure 1 -Blockchain Architecture

Source: https://www.researchgate.net/figure/A-simplified-example-of-how-blocks-are-chained-to-form-a-blockchain-Notice-that-each_fig1_332215097

Now, a question arises: why are there hashes of previous blocks in a block? This is to ensure there is transparency and blocks are in order. If there is a compromise and a threat actor has been able to tamper with the ledger, the hashes of the blocks would change which will render the ledger corrupt. This along with timestamping offers non-repudiation.

Blockchain Usage

Blockchain is often thought of as a technology that has a future in banking and monetary transactions but Blockchain is used in a variety of industries. For example, IBM has created a food trust blockchain to trace the journey of food products. This way, there is a track of all the locations and people the food product had to pass through to get to stores. In case of a disease outbreak, it would be much easier to track the product's journey and identify a source point that caused it. Blockchain also has great scope of usage in the real estate business to reduce property crime by having legitimate and easily accessible records that cannot be tampered with. In the healthcare industry, Blockchain can be used to secure Personal Health Records (PHR) preventing third parties from getting access to these records.

Securing the Blockchain

Proof of Work

Hashing is an excellent mechanism to prevent tampering but high-speed computers these days can calculate hundreds of thousands of hashes a second. In a few minutes, an attacker can tamper with a block, and then recalculate all the hashes of other blocks to make the blockchain valid again. To avoid this problem, blockchains use the Proof-of-Work mechanism. It is a computational problem which does not allow the blocks to be created at a rapid pace.

A proof-of-work is a computational problem that takes certain effort and time to solve. This is feasible as the time required to verify the results of this computational problem is relatively very less compared to solving the computational problem. In the case of Blockchain, it takes almost 10 minutes to calculate the required Proof-of-Work to add a new block to the ledger. So, if there were any changes to be made in blocks within a ledger, the threat actor would require at least 10 minutes to perform Proof-of-Work for each block.

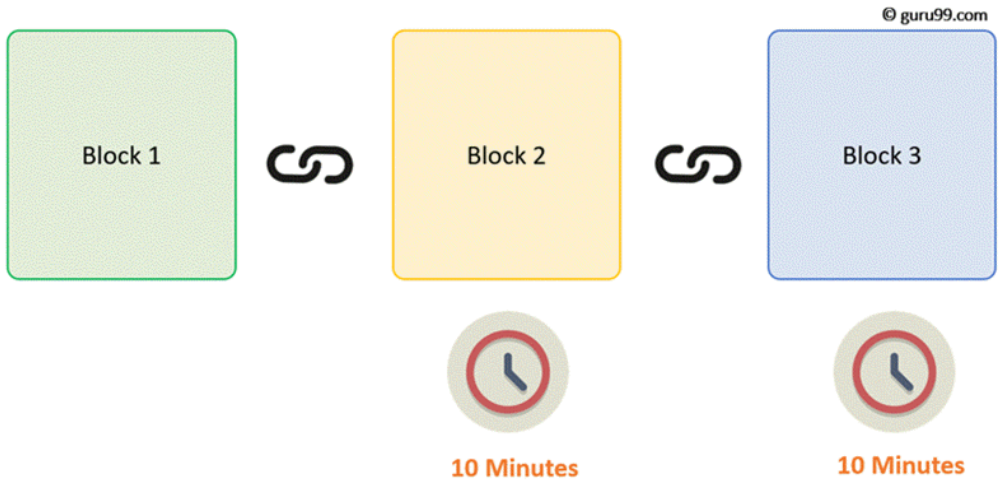


Figure 2 -Proof of Work

Source: https://www.guru99.com/blockchain-tutorial.html

The Proof-of-Work mechanism makes it tough to tamper with the blocks so even if there are modifications in a single block, the modifier will need to recalculate the proof-of-work for all the following blocks. Thus, hashing and proof-of-work mechanisms make a blockchain secure.

Smart Contracts

Smart contracts are computer programs that are stored on a Blockchain which are executed when predetermined conditions are satisfied. It is like an agreement between two parties that include Party A to do something for Party B and vice versa, which would trigger the

execution of the program. For example: Alice wants to buy a car from Bob for 2 BTC. Once, the amount is paid to Bob, Bob would complete the sales process and hand over the keys to Alice. Here, the predetermined conditions are the transfer of 2 BTC and handing over the keys which would ensure that the agreement has been honored. In technical terms, the transaction would reflect on the Blockchain ledger only if nodes in the Blockchain ledger approve of the transaction. If the agreement does not go through, there will not be any execution of the smart contract code and no blocks will be added to the Blockchain ledger. If we talk about monetary transactions, a smart contract is an essential property to avoid any dispute between two parties.

Implementation of the Blockchain

In this paper, we propose that a Blockchain be implemented with other technologies and protocols to enhance transparency and security of the workflow.

Asymmetric Encryption

Asymmetric Encryption uses 2 keys - a public key and a private key. Public keys are spread out and they can be used by anyone to encrypt data and convert it into an unreadable format. Private or a secret key, as the name suggests is confidential and is only known to the key generator. Let us take a mailbox for an example; a mailbox usually is an open public place for receiving mail. Now, any letter or mail placed in the mailbox could be accessed by a random person if left open. That is why there is a lock over the mailbox and the key is possessed by the owner to protect random people from gaining access to the mail. The key that the owner uses to open his mailbox is equivalent to a ‘private key’ in this system and people dropping mail in this mailbox use its address which is equivalent to a ‘public key’.

Encryption adds an extra layer of security to Blockchain, as there would be hashes of data present inside each Block rather than data. So, even if a threat actor compromises a Blockchain and get access to the Blocks, they would need the private keys to actually access the data in the compromised blocks. Digital signature algorithms like ECC and RSA and hashing algorithms like SHA-256 and Blowfish can be used with the system depending on the type of data and devices being dealt with i.e., whether the target devices are high-end computers, laptops or lightweight devices like smartwatches, odometers or other IoT devices.

Inter- Planetary File System

One of the major shortcomings of Blockchain is the efficiency of storing data on the ledger and the price it takes to do so. Inter-planetary file system (IPFS) is a file sharing system that aims to combat this problem. IPFS is a peer-to-peer protocol aimed at decentralizing and delivering faster, safer web content. It is based on a principle of content-based addressing. It means that if a user wants a file, they will ask for the file and not for its

location (which is how the centralized Internet works). Every file added to the IPFS network has a unique identity - its hash.

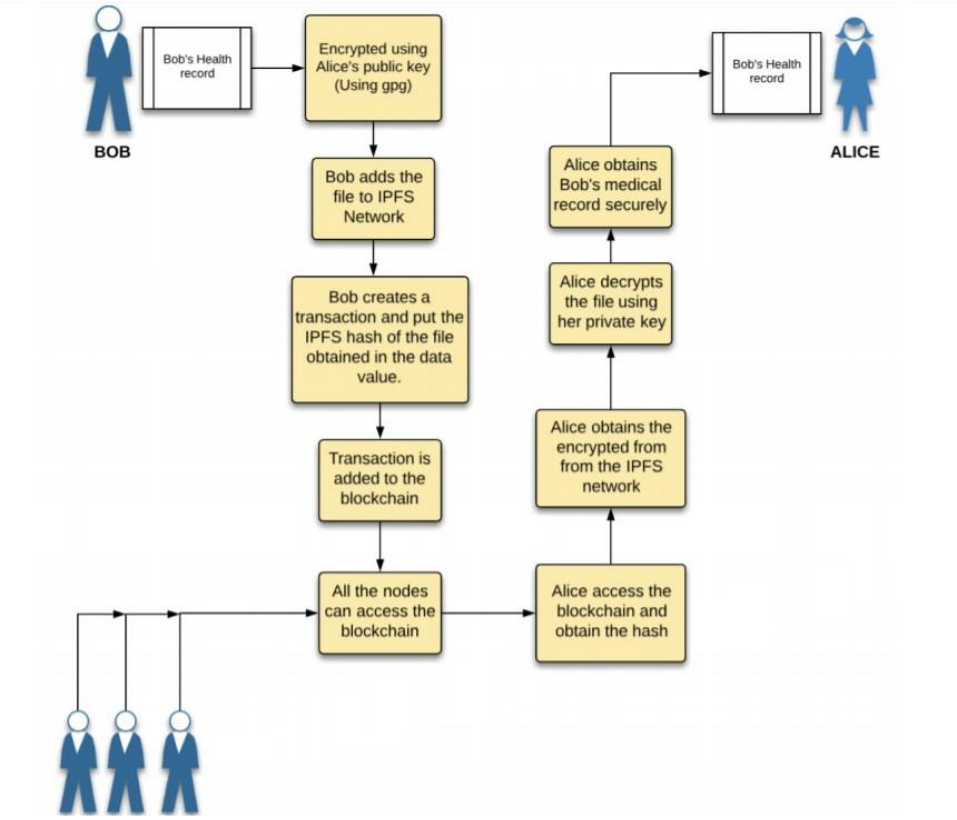


Figure 3: Example of use of IPFS

When you want to access a specific file, you just ask within the network who has the file with the specified hash. Anyone with a copy of that file on the network can provide you the file. The files added to the network cannot be changed or tampered with as changing a file would result in a different hash. This ensures integrity of the file shared on the network. The more you share a file, the more it will become accessible to a large group of people as each time a file is accessed it is stored in the cache of that user's storage and then he can provide the file to others if they need it. Duplication of files is reduced and the amount of data on the Blockchain reduces significantly as the system transfers hashes between nodes rather than an actual file which could be 100s of megabytes large.

Advantages

- **Decentralization**: One of the major attributes and advantages of using a Blockchain is decentralization. There is no central authority governing the Blockchain and the network is peer to peer (P2P). This means that the Blockchain itself does not store any information centrally, or on specific servers like the centralized internet we are familiar with. Every node of the network has an updated copy on the Blockchain which makes

it extremely difficult to tamper with, because it would require an attacker to tamper with not just one central Blockchain but with copies of the Blockchain on multiple nodes on the network. Ideally, an attacker would need to get control of 51% of the nodes on a network which would mean that the attacker would need to compromise 51 nodes on a network of 100, which seems very unrealistic and exponentially harder than getting control of one central node.

- **Cost Reduction**: We talked about how storing data on a Blockchain can be expensive and inefficient. But, once we use supporting protocols and are able to switch over to Blockchain, there is a huge margin of reducing costs. Since the system is decentralized, an institution could be saving up a lot on 3rd party vendor costs - which would help in keeping transactions transparent and data secure.

- **Transparency**: Conflicts and disputes across various industries could be avoided as mentioned previously in this paper. It would be easier to track the lifecycle of a product and the supply chain becomes a lot more efficient, saving up time on finding the source point of a problem and improving traceability.

Disadvantages

- **Scalability**: Decentralization brings with it the disadvantage of scalability. The current Blockchain systems is not nearly as scalable as a centralized system. Transactions depend on network congestion i.e., if there are more nodes on the network, there might be a delay in processing times. For example, Bitcoin can do around 7 transactions a second whereas Visa can do around 24000 transactions a second - so there is a need to address this problem which can be accomplished using architectural blockchain solutions.

- **Inefficiency in storage**: As addressed before, it would not be ideal to have a ledger with blocks of data that could be in the range of various hundred gigabytes. If we ignore additional protocols to use with Blockchain, data storage and transfer becomes an issue which comes with additional costs and inefficiency.

- **Users**: Users who are not unfamiliar with this technology and its use can be a potential vulnerability. In this system, each user has their private key and that is their only authentication method. If this key is compromised or lost, it would lock the user out so there is a need to introduce secure ways for the user to retrieve their key.

Conclusion

Blockchain is a revolutionary technology that is often thought of as something that could or is used with monetary transactions or the banking industry but as we discussed, it has

the potential to be used in numerous industries. The concept and theory of Blockchain indicates that it is a highly secure system, which it has the potential to be if we use architectural solutions, lightning networks and other protocols and technologies. It would be a challenge for users and institutions to switch to Blockchain and adapt to it but there is a huge potential of changing the way we operate on the internet and attempting to tackle security compromises and mismanagement within industries.

References

[1] https://www.forbes.com/sites/ilkerkoksal/2019/10/23/the-benefits-of-applying-blockchain-technology-in-any-industry/?sh=5670b12f49a5

[2] https://101blockchains.com/benefits-of-blockchain-technology/#:~:text=Advantages%20of%20Blockchai n%20Technology,-There%20are%20many&text=Enterprise%20blockchain%20technology%20enables%20organizations,and%20hence%2C%20easy%20to%20track

[3] https://101blockchains.com/disadvantages-of-blockchain/

[4] https://www.youtube.com/watch?v=SSo_EIwHSd4

[5] https://www.researchgate.net/figure/A-simplified-example-of-how-blocks-are-chained-to-form-a-blockchain-Notice-that-each_fig1_332215097

[6] https://ieeexplore.ieee.org/document/8726493

Contact Us

To learn more information about Electrosoft and our capabilities, contact us at info@electrosoft-inc.com.

About Electrosoft

Electrosoft delivers a diversified set of technology-based solutions and services differentiated by thought leadership and innovation. Fueling the success of our government and commercial customers since 2001 through outstanding value and trust, we couple our domain knowledge and experience with proven, mature management practices to deliver the right solutions on time and within budget. These practices include an ISO 9001:2015 registered Quality Management System (QMS) and Capability Maturity Model Integration (CMMI) Level 3 assessed processes. Headquartered in Reston, Virginia, Electrosoft is an 8(a) certified Small Disadvantaged Business (SDB) and an 8(m) certified Economically Disadvantaged Woman-Owned Small Business (EDWOSB). For more information about Electrosoft, visit our website at www.electrosoft-inc.com .