**Abstract:**

The digital transformation in the world introduced Blockchain technology which can solve the busiest sector i.e., Banking Sector. Blockchain technology which was introduced with the concept of cryptocurrency bitcoin, a form of cash that can be sent peer-to-peer without the need of central bank or any authority to maintain the ledger which was decentralized, faster, secure, cost effective, transparent and non -vulnerable. Through this Paper we are introducing, how blockchain Conesus algorithms, hashing techniques, salting techniques, time stamp algorithm and Hashing can be helpful to solve banking issues and make the overall banking procedure smooth and secure.

**Introduction:**

**1.About Blockchain**

A blockchain is a decentralized database that is shared across computer network nodes. A blockchain acts as a database, storing information in a digital format. Blockchains are well recognized for their critical function in keeping a secure and decentralized record of transactions in cryptocurrency systems like Bitcoin. The blockchain's novelty is that it ensures the accuracy and security of a data record while also generating trust without the requirement for a trusted third party.

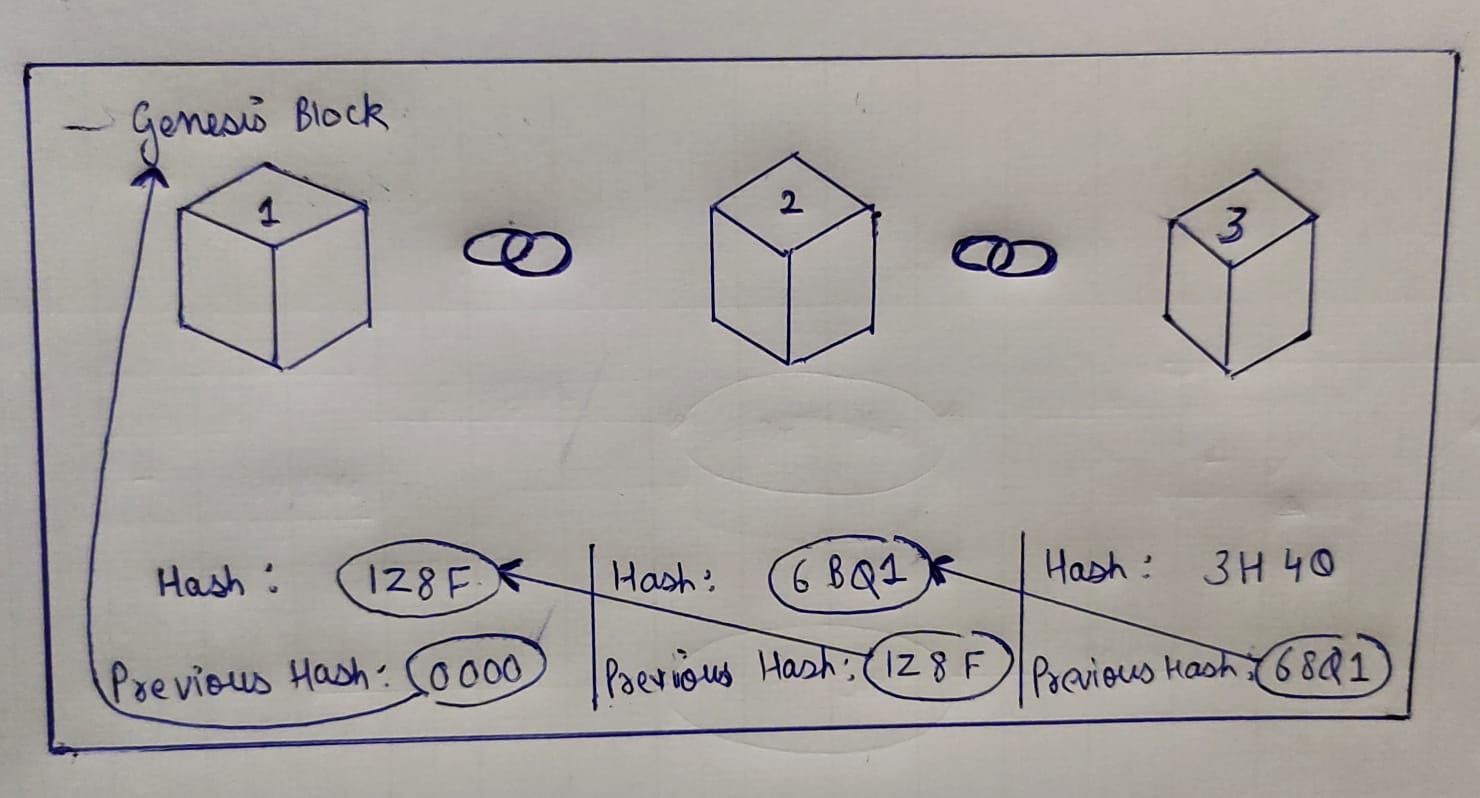
The structure of the data on a blockchain differs from that of a traditional database. A blockchain organizes data into groupings called blocks, each of which contains a collection of data. Blocks have specific storage capabilities, and when they're full, they're closed and connected to the preceding block, producing a data chain known as the blockchain. All additional data that comes after that newly inserted block is assembled into a new document.

Today, banks are continuously exploring new ways to do transactions quicker for enhanced customer services by assuring transparency to customers and regulators while ensuring cost efficiency. Blockchain is an essential technology with promising application scenarios in banking industry nowadays. It can transform banking industry and make process more democratic, transparent secure and efficient. Blockchain is a technology that combine several technologies like distributed data storage, consensus mechanism, point-to-point transmission and encryption algorithms. A Blockchain act as decentralized ledger that keeps track of transactions between two parties effectively. Although these parties have simultaneous access to update digital ledger constant and system virtually impossible to hack.

**2. Blockchain Architecture:**

A blockchain is a decentralized, immutable, and distributed digital ledger that records transactions in real time. Blockchain functions as a ledger or spreadsheet that enables a peer-to-peer (P2P) network to validate and verify transactions. This blockchain system consists of N nodes that are networked via a widely established protocol, resulting in a continuous process of error, manipulation, and data quality checking. This keeps track of an increasing number of records known as 'Blocks.'

The hash in the block header, which is created using the SHA256 algorithm (bitcoin), may be used to identify blocks in a blockchain. This hash function was created with the help of a mathematical procedure that converts data of any size into a 32-byte string. These blocks are data structures that aid in the inclusion of transactions in the public ledger. Index, Hash, previous hash, timestamp, and nonce make up the block's header. Complete summary of transactions stored as array in the body of the block. The figure below, illustrate how hash value and previous block hash value link to each other.



The genesis block is the initial block in a blockchain, and it contains all of the transactions that have a unique hash value. This hash, as well as any new transaction data, is utilized in the chain's following block. That is, each block's hash connects it to the preceding block. Transactions can be safely added in this manner. They're protected against manipulation and alteration. By employing the safe Hash Algorithm [3], each block has a timestamp and is linked to the preceding block. As a result, if the data of a block is altered, the hash value of that block is likewise updated. The following block is then affected since it contains the hash of the preceding value. As a result, no one can alter the block's transaction data.

The fundamental benefit of Blockchain is that it employs encryption, which allows users to alter transactions on a secure network. If a majority of nodes or participants agree that the transaction conducted seems to be valid, the transaction is said to be valid.

**3.Consensus Algorithms:**

Before Knowing Consensus Algorithms, we must know what is Consensus, it is a process in computer science used to achieve agreement on a single data value among distributed systems. In a distributed computing environment, a consensus algorithm is a technique that allows all participants in a blockchain network to reach a shared understanding (consensus) on the current data state of the ledger and trust unknown peers.

Therefore, Consensus Algorithms helps to achieve reliability in network of blockchain and build a trust between unknown peers, where the consensus protocol is added to blockchain which is the only version on which every other node agrees upon.

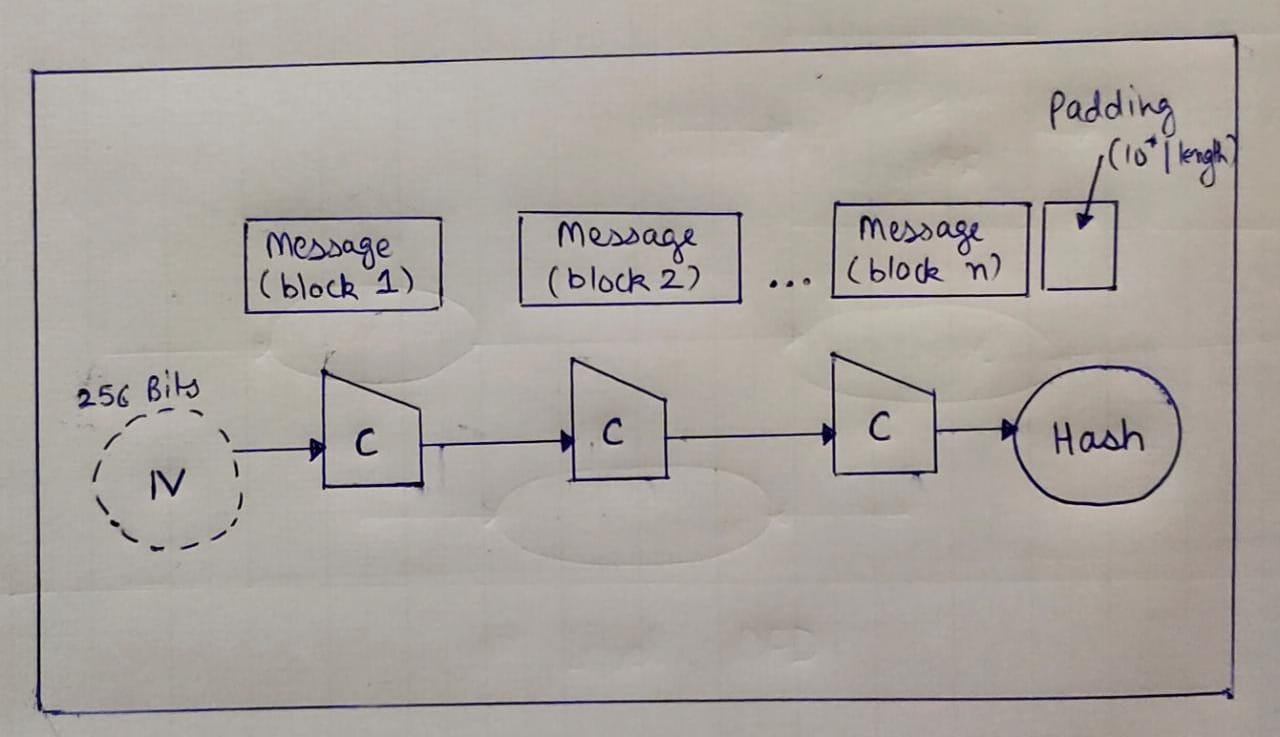
Consensus algorithms has some objectives to be clear before making an agreement that will be beneficial for whole network. Firstly, it agrees for an agreement, collaborate, equal right to nodes and compulsory participation of every node in the process.

We will be discussing 4 major types of consensus algorithms in details to get a better understanding over the topic:

1. ***Proof of Work (POW)***

This Algorithm was introduced with first cryptocurrency i.e., Bitcoin by Satoshi Nakamoto. It is the most known way of confirming transactions. Proof of work (PoW) is a form of cryptographic proof in which one party (the prover) proves to others (the verifiers) that a certain amount of a specific computational effort has been expended. The first node to complete all necessary calculations receives a reward from blockchain network. All nodes compete against each other by increasing capacity of computing resources. The goal of proof-of-work algorithms is not to prove that particular tasks were completed or that a computational challenge was "solved," but to discourage data modification by imposing high energy and hardware-control requirements.

We must define the hash function and the nonce throughout this step. In Bitcoin, a nonce is a random number that can range from 0 to 4294967296. Hash is a complicated method that converts data of any size into a string. Every Block has a unique Hash value, which we should copy and paste into the next block of transactions. After that, take the nonce value and append it to the end of the text block. We now have a large block of text including the previous block hash and nonce, as well as new transactions. The computer then spends around 10 minutes performing 10n21 calculations to discover the string value with the most zeroes in front of it. The SHA-256 Hash algorithm was utilized to execute the hash function in Bitcoin [2]. As an example, the hash value of the preceding block is 00000000000000000028c91a95cd6a5b6cbd913c203510eab26 9208df6c64091 with 18 zeros.



1. ***Proof of Stake (POS)***

Proof of stake (PoS) protocols are a type of blockchain consensus method that selects validators based on their bitcoin holdings. This is done to circumvent proof of work methods' high computing costs. Therefore, node with greater number of resources get chosen to generate next block in blockchain.

Just like in company, the one who has the highest number of shares has powers, node with greater number of resources is appointed to generate block in blockchain.

It can be further classified into two categories:

1. **Delegated POS (Proof of Stake)**

Delegated POS is a type of POS consensus algorithm, in which blocks are signed by selective representatives. Owners of the largest balances choose their representative and each of them receives right to sign blocks on blockchain network. If by any chance, if the representative missed turning a block, he gets deprived from delegated votes and leaves council. Its advantages are that balance owners have a opportunity to delegate their votes without delegating actual resources. Unlike POS, amount of unnecessary work is reduced during the process of choosing next voter.

**(b) Leased POS (Proof of Stake)**

Leased POS is another type of consensus algorithm user has a possibility to lease out their balance to mining nodes, in return mining nodes share a part of profit with users, which is only supported on waves platform.

1. ***Proof of Capacity (POC)***

POC, allows mining devices in network to use their hard drive space to decide mining rights. Proof-of-Capacity consensus is a step forward from the widely used Proof-of-Work consensus algorithm. Even before mining can begin, processor power and hard disc storage must be set aside. As a result, the system outperforms the Pow. Proof-of-Capacity produces a block in four minutes, whereas Proof-of-Work takes ten minutes. Supported by bitcoin. It tries to tackle the hashing problem in the PoW scheme. If there are more solutions or plots accessible on the computer, there is a better possibility of winning the mining dispute.

The PoC technique is as follows:

- each miner calculates a huge quantity of data, which is stored on a node's disc subsystem: hard drive, cloud storage, or other. Space is the name of the first dataset in the PoC.

- The miner reads a tiny data set equal to 1/4096, or around 0.024 percent of all stored data, for each new block on the blockchain. The miner can then generate a new block after receiving the result (deadline) as elapsed time since the last block was created.

- The miner who met the minimum deadline time signs the block and earns a transaction reward.

1. ***Proof of Importance***

The NEM blockchain platform employs this consensus mechanism. The quantity of resources available on a user's balance and the number of transactions in their wallet determine their importance in the NEM network. Unlike the more prevalent PoS method, which solely considers user balance, PoI considers both the number of resources and the amount of user activity in the blockchain network. This strategy encourages customers to not just maintain money in their accounts, but also to spend it. Line time is responsible for signing the block and receiving a payment for each transaction.

1. ***Proof of Activity***

Each miner in a blockchain network tries to construct an empty block header, which contains a previous block hash, a miner's public address, an index of a current block in the blockchain, and a nonce.

- The node delivers the empty block header to the blockchain network after producing one that fulfils the current difficulty criteria.

- The header of such a block is treated as data received from pseudo-random owners by all nodes in the network. A follow-the-Satoshi algorithm is used to pick stakeholders using a hash of the transmitted block header and a hash of the preceding block Plus N presets.

- Every stakeholder who is online at the moment verifies the validity of the empty block header. Everyone who got the header verifies whether they are one of the first N-1 lucky stakeholders in this block throughout the validation.

. If this is the case, they use a secret key to sign the empty block header and submit it to the blockchain network.

- When the Nth stakeholder notices that he is the one to sign the block, he adds a block with transactions, a number of which he chooses himself, as well as all N-1 signatures from other stakeholders, to the empty block header, and then signs the block.

- A new block is sent out by stakeholder N. This block is received by nodes, who verify its authenticity before adding it to the blockchain.

- The miner and N fortunate stakeholders split the transaction reward obtained by the N-stakeholders.

1. ***Proof of Authority***

The PoA consensus method differs from the others in that, unlike PoW and PoS, it does not require any mining. All transactions and blocks in a Po Authority-based blockchain network are verified by authorized accounts, commonly called as validators. The validator's computational capacity is used to automatically execute transactions and generate blocks.

1. ***Hashing Techniques***

Hashing is the process of scrambling raw data to the point that it can no longer be reproduced in its original form. It takes a chunk of data and runs it through a function that manipulates the plaintext with math. The hash function produces the hash value/digest, which is the result of the hash function.

Two main applications of Hashing are:

*Password Hashes*: In most website servers, it converts user passwords into a hash value before being stored on the server. It compares the hash value re-calculated during login to the one stored in the database for validation.

*Integrity Verification*: When it uploads a file to a website, it also shared its hash as a bundle. When a user downloads it, it can recalculate the hash and compare it to establish data integrity.

SHA 256 is a member of the SHA 2 algorithm family, with SHA standing for Secure Hash Algorithm. It was a cooperative effort between the National Security Agency and the National Institute of Standards and Technology to introduce a successor to the SHA 1 family, which was steadily losing power against brute force assaults. It was published in 2001.The 256 in the name refers to the final hash digest value, which means that regardless of the amount of plaintext or cleartext, the hash value will always be 256 bits. SHA 256 is more or less comparable to the other algorithms in the SHA family. Look into learning a little more about their policies immediately.

The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits.

You can divide the complete process into five different segments, as mentioned below:

### ***Padding Bits***

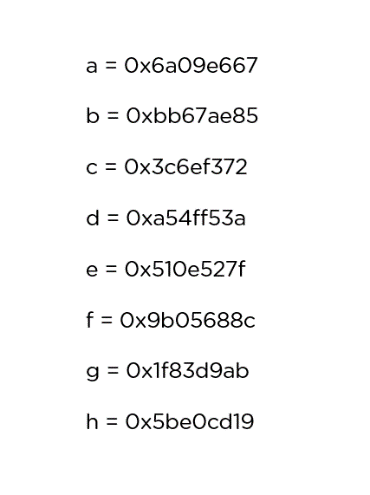
It adds some extra bits to the message, such that the length is exactly 64bits short of a multiple of 512. During the addition, the first bit should be one, and the rest of it should be filled with zeroes.

### ***Padding Length***

You can add 64 bits of data now to make the final plaintext a multiple of 512.You can calculate these 64 bits of characters by applying the modulus to your original cleartext without the padding.

### ***Initializing the Buffers:***

You need to initialize the default values for eight buffers to be used in the rounds as follows:



### ***Compression Functions***

### the entire message gets broken down into multiple blocks of 512 bits each. It puts each block through 64 rounds of operation, with the output of each block serving as the input for the following block

1. ***Salting Techniques***

In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage.

1. ***Time Stamp Algorithms***

The timestamp or timestamp is a small data stored in each block as a unique serial and whose main function is to determine the exact moment in which the block has been mined and validated by the blockchain network. In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage. One of the main uses of timestamp is to establish the parameters of the process of [mini](https://academy.bit2me.com/en/what-is-cryptocurrency-mining/)ng. This is because these timestamps allow nodes to correctly adjust the [mining difficulty](https://academy.bit2me.com/en/what-is-bitcoin-mining-difficulty/) to be used for each block generation period. Timestamps help the network determine how long it takes to extract blocks for a certain period, and from there adjust the mining difficulty parameter.

**Blockchain in Banking Service**

Blockchain technology promises huge opportunity to recover the challenges in banking industry. There are several use cases with advantages and limitations with blockchain technology.

1. *Payments*: Payments are the most common use of any financial or banking system. The blockchain technology will be used for payment processing by both commercial and central banks. These are crucial for cross-border payments, as they can be completed quickly without the use of a third party. Changes in exchange rates might pose issues with cryptocurrency conversion to local currency.

2. *Digital verification*: Using blockchain, all traditional verification mechanisms such as identification, face verification, and evidence of customer intent may be eliminated. Blockchain allows users to identify themselves and those who want to share their identities without having to register for each banking service again. Any participant can access information without authorization thanks to the shared ledger technology. As a result, private data should not be stored on the blockchain.

3.*Bookkeeping (Pass Book)*: Most traditional banks still rely on paperwork such as double entry transactions, which are gradually being digitalized after a lengthy process. Banks can submit transaction information directly into the shared ledger system . When utilizing blockchain, all records are visible and irrevocable. Smart contracts are a feature of this system that allows it to pay invoices automatically. Working at a bank requires previous understanding of blockchain, which is a significant constraint.

**Literature Review:**

Blockchain technology is reshaping the standard economies. individuals could have additional trust than ever before because the dealings is immutable and clear. Time Banking may be a generalized exchange economy not supported cash, however values everyone's contribution on identical scale, the time exhausted. Time banking may be a noble plan with nice potential, however the safety and trust problems don't seem to be well self-addressed. during this paper a Blockchain Enabled localized Time banking industry (Blends) is projected to make a trusting, dynamic and respectful community. individuals during this community area unit inspired to be engaged in mutual serving relationships. Hope this position paper could inspire additional interests within the roles that blockchain technology will play in trendy society. The processed info passes through the info of banks and payment systems, that doubtless makes it offered to the assaulter. The protection mechanisms of distributed databases, proposes an answer to the matter of maintaining the individuality of data in them supported Blockchain technology while not tokens and offers recommendations on the introduction of Blockchain technology into fashionable banking. we have a tendency to square measure exploitation block chain technology for the decentralized operating of banks and therefore the complete removal of authoritarian interception. The model that we have a tendency to square measure proposing includes block chain encapsulated within the method of NEFT (National Electronic Fund Transfer) exploitation IFSC (Indian national economy Code) incorporating the protocols set down by tally for secure and decentralized fund transfer. Our blocks can contain the method computed in java small services. The ledger is interconnected among themselves exploitation agreement algorithms. This platform can eliminate the presence of the sure third party that is that the third entity through that the assorted transactions and banking info should pass. to start with, our platform can eliminate third-party trust, promote user-user dealings so store bank transaction info within the blockchain. The paradigm of net of Things (IoT) is paving the means for a world, wherever several of our daily objects are interconnected and can move with their setting so as to gather data and modify sure tasks. Such a vision needs, among alternative things, seamless authentication, knowledge privacy, security, lustiness against attacks, straightforward readying, and self-maintenance. Such options is brought by blockchain, a technology born with a cryptocurrency known as Bitcoin.

**References:**

**[1] Bakaul, Masum & Das, Nipa & Moni, Madhabi Akter. (2020). The Implementation of Blockchain in Banking System using Ethereum. International Journal of Computer Applications. 177. 50-54. 10.5120/ijca2020919895.**

**[2] R. C. Merkle, "Protocols for Public Key Cryptosystems," 1980 IEEE Symposium on Security and Privacy, 1980, pp. 122-122, doi: 10.1109/SP.1980.10006.**

**[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *URL:*** [***http://www.bitcoin.org/bitcoin.pdf*,**](http://www.bitcoin.org/bitcoin.pdf) **2008.**

**[4] X. Lin, R. Xu, Y. Chen and J. K. Lum, "A Blockchain-Enabled Decentralized Time Banking for a New Social Value System," 2019 IEEE Conference on Communications and Network Security (CNS), 2019, pp. 1-5, doi: 10.1109/CNS.2019.8802734.**

**[5] Q. K. Nguyen, "Blockchain - A Financial Technology for Future Sustainable Development," 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD), 2016, pp. 51-54, doi: 10.1109/GTSD.2016.22.**

**[6] N. A. Popova and N. G. Butakova, "Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions," 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2019, pp. 1764-1768, doi: 10.1109/EIConRus.2019.8657279.**

**[7] V. Naik, R. Pejawar, R. Singh, A. Aher and S. Kanchan, "Expeditious banking using Blockchain Technology," 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), 2020, pp. 1-6, doi: 10.1109/CISPSSE49931.2020.9212253**

**[8] S. Sakho, Z. Jianbiao, F. Essaf and K. Badiss, "Improving Banking Transactions Using Blockchain Technology," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), 2019, pp. 1258-1263, doi: 10.1109/ICCC47050.2019.9064344.**

**[9] Chowdhury, M. , Suchana, K. , Alam, S. and Khan, M. (2021) Blockchain Application in Banking System. *Journal of Software EngineeringandApplications*,14,298-311.doi:**[**10.4236/jsea.2021.14701**](https://doi.org/10.4236/jsea.2021.147018)**8.**

**[10] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," in IEEE Access, vol. 6, pp. 32979-33001, 2018, doi: 10.1109/ACCESS.2018.2842685.**

**[11] Knezevic, Dusko. (2018). Impact of Blockchain Technology Platform in Changing the Financial Sector and Other Industries. Montenegrin Journal of Economics. 14. 109-120. 10.14254/1800-5845/2018.14-1.8.**

**[12] S. King, “Primecoin: Cryptocurrency with prime number proof-of- work,” July 7th, 2013.**

**[13] J. J. Kishigami, “Blockchain contract: A complete consensus using blockchain,” in Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on. IEEE, 2015, pp. 577–578.**

**[14] S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof- of-stake,” self-published paper, August, vol. 19, 2012.**

**[15] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, 2014.**

**[16] E. Dufﬁeld and K. Hagan, “Darkcoin: Peertopeer cryptocurrency with anonymous blockchain transactions and an improved proof\_of\_work\_system,” Mar-2014 [Online]. Available:https://www.dash.org/wpcontent/uploads/2014/09/DarkcoinWhitepaper.pdf, 2014.**

**[17] “A brief survey of cryptocurrency systems,” in 2016 14th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2016, pp. 745–752.**

**[18] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Sur- veys & Tutorials, vol. 18, no. 3, pp. 2084–2123, 2015.**