TELECOMMUNICATION ENGINEERING CENTRE
दूरसंचार अभियांत्रिक केन्द्र
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
संचार एवं सूचना प्रोधोगिकी मंत्रालय
DEPARTMENT OF TELECOMMUNICATIONS
दूरसंचार विभाग
GOVERNMENT OF INDIA
भारत सरकार
ISO 9001:2008

STUDY PAPER ON

SECURITY ASPECTS OF BLOCKHAIN

……………………….TS Division, TEC

Contents

1. INTRODUCTION:

Distributed ledger technologies or Block chains are immutable digital ledger systems implemented in a distributed fashion (i.e. without a central repository) and usually without a central authority. This technology became widely known in the beginning of 2008 when it was applied to enable the emergence of electronic currencies where digital transfers of money take place in distributed systems. Various digital currency systems such as Bitcoin, Ethereum, Ripple, and Litecoin are only an example of this technology. Infact, this technology is broadly useful and can be used for variety of applications.
Block chains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify. New blocks are replicated across all copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

Presently, there are mainly two types of block chain: Public Blockchain and Private blockchain. Public blockchains use computers connected to the public internet to validate transactions and bundle them into blocks to add to the ledger. Any computer connected to the internet can join the party. Private blockchains, on the other hand, typically only permit known organizations to join. Together, they form a private, members-only "business network." This difference has significant implications in terms of where the (potentially confidential) information moving through the network is stored and who has access to it. Bitcoin is probably the most well-known example of a public blockchain and it achieves consensus through "mining." In Bitcoin mining, computers on the network (or 'miners') try to solve a complex cryptographic problem to create a proof of work.

This paper mainly focusses on the introduction of blockchain technology, its models and also various security threats along with countermeasures to addresses those threats in Blockchain environment.

2. Terminologies in block chain technologies:

i. Node: Any computer running block chain software is called nodes.
ii. Mining nodes: Subset of nodes and set of computers running block chain software
iii. Full nodes: The job of a full node is to store the blockchain data, pass along the data to other nodes, and ensure newly added blocks are valid.
iv. Lightweight nodes: Lightweight nodes do not need to store full copies of the blockchain and often pass their data on to full nodes to be processed. Lightweight nodes are generally found on smartphones and Internet of Things (IoT) devices i.e. devices with limited computational and/or storage capability
v. Miner: A miner is a participant in a Blockchain that participates in securing the network and validating new transactions. The mining and validation process happens via either competitive, voting or luck-based methods dependant on the consensus protocol chosen.
vi. Cryptographic Nonce: An arbitrary number (usually randomly selected) that is used once.

3. Blockchain Architecture:

At a high level, blockchains utilize well-known computer science mechanisms (linked lists, distributed networking) as well as cryptographic primitives (hashing, digital signatures, public/private keys) mixed with financial concepts (such as ledgers). Blockchain usually comprises of following components:

3.1. Hashes:

An important component of the blockchain technology is the use of cryptographic hash functions for many operations, such as hashing the content of a block. Hashing is a method of calculating a relatively unique fixed-size output (called a message digest, or just digest) for an input of nearly any size (e.g., a file, some text, or an image). Even the smallest change of input (e.g., a single bit) will result in a completely different output digest.

A hashing algorithm used in many blockchain technologies is the Secure Hash Algorithm (SHA) with an output size of 256 bits (SHA-256).

3.2. Transactions:

A transaction is a recording of a transfer of assets (digital currency, units of inventory, etc.) between parties. Each block in a blockchain contains multiple transactions. A single transaction typically requires at least the following information fields:

- Amount – The total amount of the digital asset to transfer.
- Inputs – A list of the digital assets to be transferred (their total value equals the amount).
- Outputs – The accounts that will be the recipients of the digital assets. Each output specifies the value to be transferred to the new owner(s), the identity of the new owner(s), and a set of conditions the new owners must meet to receive that value.
- Transaction ID/Hash – A unique identifier for each transaction. Some blockchains use an ID, and others take a hash of the specific transaction as a unique identifier.

3.3. Ledgers:

A *ledger* is a collection of transactions. Usually, ledgers have been stored digitally, often in large databases owned and operated solely by centralized “trusted” third parties on behalf of a community of users. A ledger implemented using a blockchain will be copied and distributed amongst every node within the system instead of ‘centralized’ mechanism.

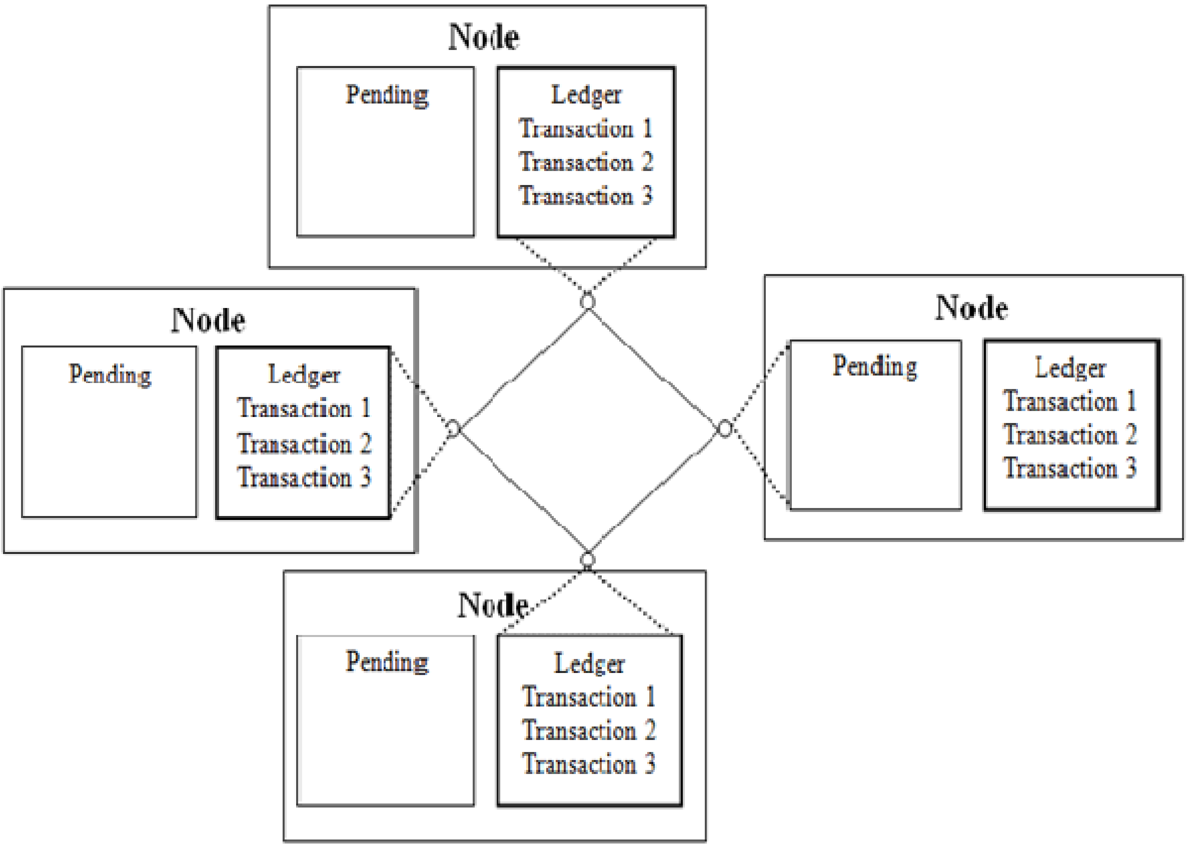

Fig 1: A Simple network maintaining a copy of ledger across nodes (Ref: Draft NISTIR 8202)

3.4. BLOCKS:

A block contains a set of validated transactions. Validity' is ensured by checking that the providers of funds in each transaction (listed in the transaction's 'input' values) have each cryptographically signed the transaction. This verifies that the providers of funds for a transaction had access to the private key which could sign over the available funds. After creation, each block is hashed thereby creating a digest that represents the block

Transaction are added to blockchain when mining nodes publishes a block.

3.5. Addresses:

A user's address is a short, alphanumeric string derived from the user's public key using a hash function, along with some additional data (used to detect errors). Addresses are used to send and receive digital assets.
There are two keys which are used in this technology namely public key and private key.

Private Key is essentially a randomly generated number which is analogous to a password. Private keys help in accessing the unspent money associated with the corresponding public key. Public Key is the 'To Address' in the transaction. Every address on the bitcoin blockchain comes attached with a Private key and a Public key. These together form the pillars of security in the Blockchain network. Private and Public keys always work in a pair. The private key is a string that is unique to the owner of a particular Bitcoin address. The owner of this Bitcoin address uses his private key to digitally sign any transaction that he makes. The public key is a long alphanumeric string that is generated with the private key to an account and this can be publicly shared so that miners can verify digitally signed transactions. As the name suggests, a user's private key is private (known only to the owner) to the user and the public key is known to everyone.

Every time a transaction occurs, it has to be signed by both public key and private key of person authorizing the transaction. It also includes public key of receiving party. After signing it gets added to ledger of that blockchain and also includes timestamp and a unique ID number. When this transaction occurs, it's broadcasted to a peer-to-peer network of nodes to other digital entities that acknowledge that this transaction has occurred and adds it to the ledger.

4. Operation of blockchain:

Blockchain are maintained through the consensus of set of computers (mining nodes) running blockchain software. There is no central authority determining which node publishes the next block on the blockchain. Each node maintains a copy of the blockchain and may propose a new block to the other mining nodes. Any node may propose

new transactions, and these proposed transactions are propagated between nodes until they are eventually added to a block.

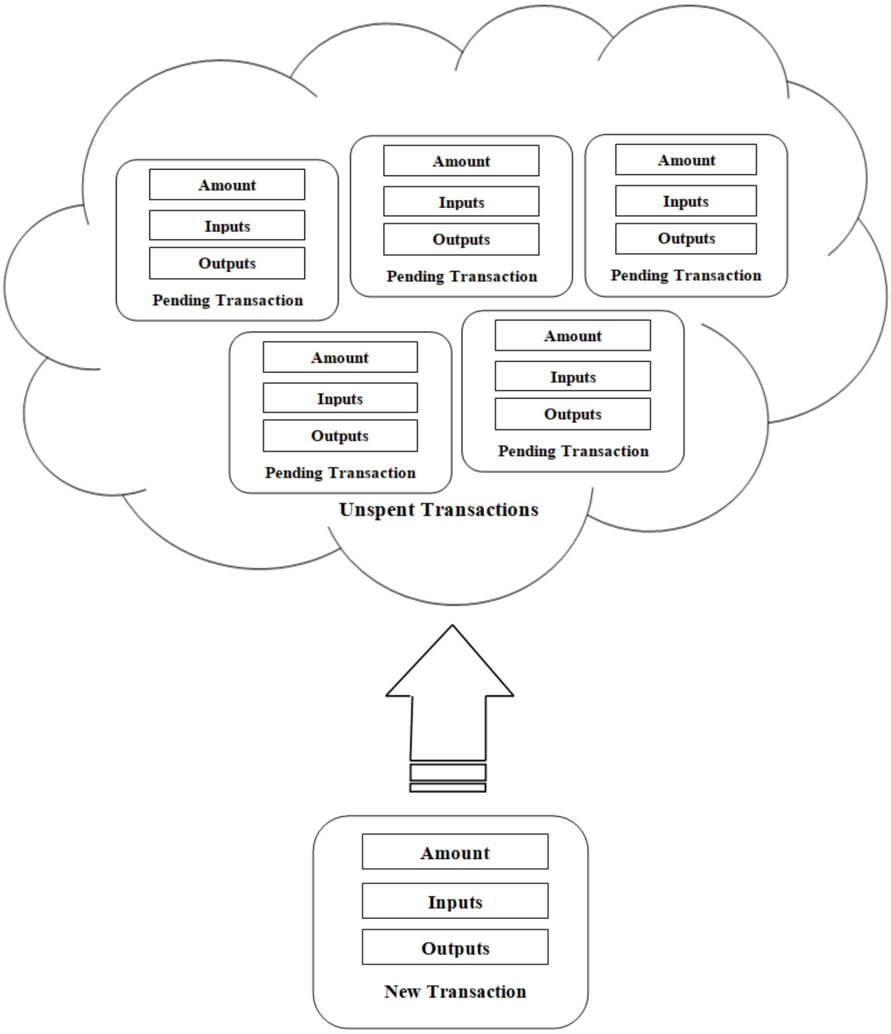

Figure 2: Transaction Being Added to Unspent Transaction Pool (Ref: Draft NISTIR 8202)

When mining nodes put together a new candidate block, they include a set of unspent transactions. They may take a combination of older transactions that have been waiting for some time and newer transactions that offer a higher payment (in the form of a transaction fee paid by the user who submitted the transaction). The mining node checks that each transaction is itself valid since the other nodes would reject the block if it included invalid transactions.

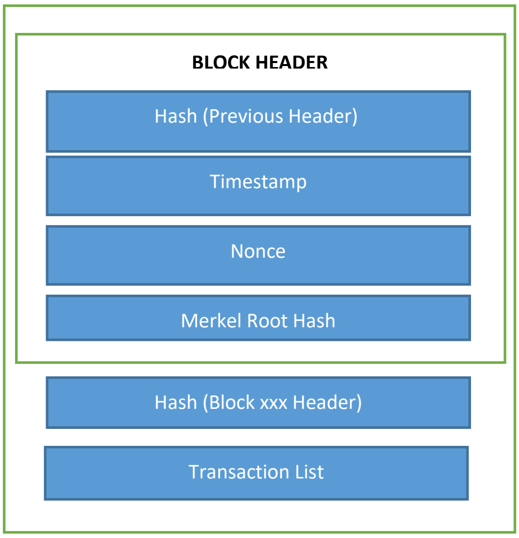

Fig 3: Finalised Block (Ref: Draft NISTIR 8202)

5. Consensus:

Block chains use a variety of consensus models that enable a group of mutually distrusting users to work together. When a user joins the block chain system, it has to agree to the initial state of system which is recorded only preconfigured block, the genesis block. After genesis block, every block must be added to block chain only after mutually agreed consensus method.

In a blockchain there is no need to have a trusted third party to give the state of the system instead every user within system can verify the system integrity. To add a new block to the blockchain, all participating nodes must come to a common agreement over time, however, so some temporary disagreement is permitted. The method of agreement (or consensus) must work even in the presence of possibly malicious users attempting to disrupt or take over the blockchain. The different consensus models as adopted by blockchain technology are as follows:

5.1. Proof of work Consensus Model:

In this model, every user gets right to publish the block only after solving a computationally intensive puzzle. The solution to this puzzle is the "proof" they have performed work. The puzzle is designed such that solving the puzzle is difficult, but checking that a solution is valid is easy. This enables all other mining nodes to easily validate any proposed next blocks, and any proposed block that did not satisfy the puzzle would be rejected.

An important aspect of this model is that the past work put into a puzzle does not influence one's likelihood of solving future puzzles. Hashing a candidate block one thousand or one million times (with different nonce values) only increases the likelihood of solving the current puzzle (as the nonce input space is being reduced with each hash calculation), it does not increase the user's likelihood of solving any future puzzles, and therefore each puzzle to solve for a block is independent and requires the same amount of work. This means that when a user receives a completed block from another user, they are incentivized to include the new block because the know the other mining nodes will include it and start building off it. If they refuse to accept the new block, they will be building off a shorter chain of blocks and (as mentioned previously) by default, the longest valid chain is adopted.

The proof of work consensus model is designed for the case where there is little to no trust amongst users of the system. It ensures mining nodes cannot game the system by always being able to solve the puzzles and thereby control the blockchain and the transactions added to it. However, a major pitfall of the proof of work consensus model is its excessive use of energy in solving the puzzles.

Bitcoin is an example where this consensus model is being adopted.

5.2. Proof of Stake:

This model is based on concept of stakes of user in the system. i.e The more the amount of stakes in the system, the more likely the system will succeed in putting the blocks in the system. Mainly there are three ways through which system can use the stakes such as random selection of staked users, to multi-round voting, to a coin aging system.

In random selection of staked users, the blockchain system will look at all users with stake and choose amongst them based on their stake to overall system stake ratio. So, if a user had 45% of the stake they would be chosen 45% of the time; those with 1% would be chosen 1% of the time.

In multi round voting system, blockchain system will select several staked users to create proposed blocks. The system will then ask all staked users to vote for the next block. After several rounds of this voting, a new block is decided upon. This method allows all staked users to have a voice in the block selection process for every new block.

On coin aging system, user is allowed to create blocks by "spending" age cryptocurrency. In this method, the user's staked cryptocurrency has an additional "age" property, and after a certain amount of time (such as 30 days) the staked cryptocurrency can be "spent" and allow the user to create a new block on the blockchain. The "spent" cryptocurrency then has its "age" reset to 0, and it cannot be used again until after the requisite time has passed. This method allows for users with more stake to create more blocks, without dominating the system.

5.3. Round Robin Consensus Model:

In this case, there is no need for a complicated consensus mechanism to determine which participant adds the next block to the chain. This consensus model is often used for private blockchains and is called round robin, where nodes take turns in creating blocks. To handle situations where a mining node is not available when it is their turn, these systems may include an element of randomness to enable available nodes to publish blocks so that unavailable nodes will not cause halt in block production. This model ensures no one node creates the majority of the blocks, it benefits from a straightforward approach, it lacks cryptographic puzzles, and has low power requirements**.**

6. Forking:

Forking is updation in blockchain technology. Since blockchains systems are decentralised system, updation is an extremely difficult task. Changes in blockchain software and implementation is called forking.

6.1. Soft Fork:

A soft fork is a change to the technology that will not completely prevent users who do not adopt the change (e.g., an update to the latest version) from using the changed blockchain system. Since non-updated nodes will recognize the new blocks as valid, a soft fork can be backwards compatible, only requiring that a majority of nodes upgrade to enforce the new soft fork rules.

6.2. Hard Fork:

A hard fork is a change to the technology that will completely prevent users who do not adopt it from using the changed blockchain system. Under a hard fork, the blockchain protocol will change in a manner that requires users to either upgrade to stay with the developer's "main fork" or to continue on the original path without the upgrades. Users on different hard forks cannot interact with one another. Any change to the block structure, such as the hashing algorithm choice, will require a hard fork**.**

7. Categorization of blockchain:

Blockchain are categorized on basis of permission of accessing the blockchain. There are two types of blockchain model namely permissionless and permissioned.

7.1. Permissioned Blockchain:

In Permissioned blockchain everyone can read and write to the blockchain, and the ledger is transparent/public. Organizations that wish to work together, but do not fully trust one another, can establish a permissioned blockchain and invite business partners to record their transactions on a shared distributed ledger. These organizations can determine the consensus mechanism to be used, based on how much they trust one another. Permissioned blockchains can be set up so anyone can read them, but only selected members can record transactions on them. This type of blockchain would provide full insight into the internal interactions of the organization by anyone who has an interest, but the public at large would not be able to interfere with the data.

7.2 Permissionless Blockchain:

Permissionless blockchains are decentralized platforms with no central authority and are open to participation without users requesting access. Permissionless blockchains often utilize a consensus method that requires more than a trivial effort in order to prevent bad users from easily subverting the system. Such consensus methods include proof of work and proof of stake methods.

8. BLOCKCHAIN USE CASES:

As the blockchain technology is maturing the number of use cases are increasing and every industry is exploring new options for implementing this technology. Some of use cases developed till now is mentioned below:

8.1. Banking:

During the scenarios when multiple banks want to join together and want to share a selective private data or any other transaction details to participating banks, this technology provide the ability to record transactions from each bank in a way that is visible to the participants, but not the public. However, to do this as a private blockchain (to avoid having to use an expensive proof of work algorithm), each bank takes turns signing the blocks under a distributed consensus algorithm. If there was some major disaster or exception situation, the banks could coordinate to roll back the blockchain and write a different transaction. Additionally, the transactions would not be anonymous because a banking ID would be required to join.

"ICICI Bank successfully executed its first two transactions using Blockchain technology in October 2016. Yes Bank has implemented a multi-nodal Blockchain transaction in January 2017 to provide efficient services to customers. Kotak Mahindra Bank and Axis Bank have announced interest and started conducting pilot transactions.

8.2. Insurance and Healthcare

Whenever someone visits a care provider, a myriad of transactions take place behind the scenes. Administrative transactions from nurses, doctors, staff, medical providers, insurance companies, and pharmacies could all be written to a blockchain. Transactions (such as checking benefits, eligibility, coverage, and the available medicine supply) could be read from the blockchain. Currently, records of these transactions reside in disparate systems, sharing results at the end of an (often manual) process.

8.3. Energy Industry

One of use cases in energy industry of blockchain usage is in recording certificates in mainly in smart grids. There are different power plants generating energy and creating certificates that attest to the amount of energy produced for subsequent exchange. Currently, there are problems such as emission certificates being spent twice, as well as the need to address regulatory challenges and provide more uniform access for everybody in the market. A blockchain can effectively track the issuance and spending of these energy certificates.

Another example of applicability of blockchain in the energy industry is in the trading of excess renewable energy. Buildings can be wired with devices measuring energy usage and recording it to a blockchain, enabling excess energy to be sold and bought on a market.

8.4. E-voting:

Another application for blockchain technology is voting. By casting votes as transactions, a blockchain is created which keeps track of the tallies of the votes. This way, everyone can agree on the final count because they can count the votes themselves, and because of the blockchain audit trail, they can verify that no votes were changed or removed, and no illegitimate votes were added. By using a blockchain code, votes can be casted via smartphone, tablet or computer resulting in immediately verifiable results.

9. BLOCKCHAIN IN TELECOM:

Service providers (SPs) have traditionally owned the end-to-end telecoms value chain for both consumers and businesses – spanning network infrastructure, provision of core voice and data connectivity, and related consumer services. However, in an environment of heightened competition in an increasingly digital world from infrastructure light over the top (OTT) players, together with decreasing revenues from voice and increasing costs due to the high band-width demands, there is a need to both reduce costs and find new sources of revenue. Following are the cases or scenarios where this technology can be used:

9.1. Fraud Prevention:

Blockchain can be a good solution for significantly decreasing the cost of fraud e.g. in roaming and in identity management. Identity fraud can occur when a person uses false identification to obtain services such as a physical SIM card. Blockchains inherent public key cryptography capability can be used to link a mobile device to the owner's identity. Instead of broadcasting the IMSI to the network to identify the device, the phone generated public key can be broadcasted. The device generates this public key from the private key that is stored securely on it. Neither the carrier nor any other third party needs to know the private key.

Meanwhile, roaming fraud could be mitigated by implementing a permissioned blockchain between every pair of operators that have a roaming agreement. Every time a subscriber triggers an event in a visiting network, a micro contract and the terms of the agreement between the roaming partners are executed. Automatic triggering of a roaming contract based on call/event data enables near instantaneous charging and reduction in roaming fraud.

9.2. Identity as a service:

Service providers can create new sources of revenue by providing identity and authentication as well as data management solutions to partners, enabled by a blockchain.

Currently, every time during signing up, proof of identity or credentials are required. PII (Personal Identity Information) is required even though most of the information would not be needed by every vendor; the vendor would only need a subset of that information. Also, signing up online either requires creating many username/password combinations or utilizing the services of third party providers (such as Google and Facebook) to use their SSO (Single Sign On) functionalities. This leads to many challenges such as lack of convenience (many username/ password combinations) and security (personal data shared with third parties) in current identity and authentication services.

A blockchain can be used as the shared ledger that stores identity transactions. The SP'S (service provider) can provide identity-as-a-service to partners, thus allowing for additional revenue generation by negotiating appropriate agreements. When a subscriber opens an account with a SP, it creates a digital identity. The private key associated with this identity is stored safely on the eSIM. The SP creates a virtual identity, using the public key from the digital identity and adds a set of standard fields (name, address, etc.) as required. It then adds a digital signature using its own private key. A pointer to this virtual identity along with necessary descriptors is then added to the blockchain. If the subscriber now visits a partner website, say an e-commerce site, the site will need to know their identity, so the merchant site starts running the corresponding app on the phone to provide the identity. A copy of the ledger entry is sent to the e-commerce site app. Now the e-commerce app can look at all entries for that same virtual identity. Once the virtual identity is established, the e-commerce site needs to know that the virtual identity belongs to the subscriber so its app takes the public key from the virtual identity, encrypts a challenge and sends it to their app which decrypts it (because it has the associated private key) and responds. Now the e-commerce site generates an e-commerce virtual identity which is then stored in the ledger itself. The next time the subscriber visits the same e-commerce site, he can be authenticated using the same mechanism. Also, the ledger already holds his transaction history and hence knows his preferences. The e-commerce site can use related insights for a recommendation engine. The subscriber can also use the same e-commerce virtual identity to login to a completely different e-commerce site using the same mechanism.

The SP virtual identity can be used to help create further virtual identities similar to thee-commerce one (such as a travel virtual identity). This identity need not know all of the details from the subscriber's digital identity, only the ones that are relevant (such as his home location) and add other attributes (such as his preferred mode of travel) to create a travel virtual identity. The possibilities of such identity management are limited only by the number of partner service providers that the SP can sign on to the blockchain-based system.

9.3. **IOT Connectivity**:

A blockchain can enable secure and error free peer-to-peer connectivity for thousands of IoT devices with cost-efficient self-managed networks. For example, machines within a manufacturing plant will be able to communicate and authenticate themselves via the blockchain to steer production processes. Active manual intervention by the workforce will for example only be needed if individual machines require service on the basis of predictive maintenance indicators. In addition, the risk of a production shut-down owing to corrupted or hacked machines could be limited, due to the distributed and consensus-based authentication of data in the blockchain network.

9.4. Enablement of 5G:

5G technology implementation is another example to potentially benefit from the blockchain to streamline processes. To realize the 5G promise of ubiquitous access across various networks, SPs will need to handle heterogeneous access nodes and diverse access mechanisms. Selecting the fastest access node for every user or machine will be a central challenge in the future. Blockchain can enable a new generation of access technology selection mechanisms to build sustainable solutions.

ANDSF, which stands for Access Network Discovery and Selection Function, is an entity within the EPC (Evolved Packet Core) which helps in the discovery/selection of access networks, such as Wi-Fi, WiMAX, and LTE, in the device vicinity, providing them with rules policing the connection to these networks. It consists of a list of access networks, such as Wi-Fi, that may be available in the vicinity of a device. This information is received in response to a device request which contains its location and capability, such as types of supported interfaces, among others. The received information assists the device in expediting connection to these networks. The ANDSF response the type of access technology (Wi-Fi, WiMAX, etc.), the access network identifier, and technology-specific information (such as one or more carrier frequencies). It mainly works on client server model.

The 3GPP (LTE, GPRS) and non-3GPP (WiMAX, WLAN, Wi-Fi) access networks in a given area can be networked via a blockchain where each access point (Wi-Fi router, SP cell tower, etc.) can serve as a node in the network monitoring the devices. Rules and agreements between the various access providing networks can be coded as smart contracts. These contracts can be dynamic in nature wherein any time a policy needs to be changed, only the contract code needs to be changed. When a device broadcasts its identity, it is accepted into the network by the corresponding SP cell. Once the device broadcasts its location, the access node that can best provide service to the device is called upon to do so. This also allows for seamless rating and charging of all services between the various access nodes.

10. Block Chain Security:

Blockchain is very complex system and comprises of distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Blockchain has the following security features:

i. Blockchain technology relies on a ledger to keep track of all financial transactions. Ordinarily, this kind of “master” ledger would be a glaring point of vulnerability. If the ledger was compromised, then it could lead to a system breakdown. For example, if someone altered a record, then they could steal a limitless amount of money. Or, if they merely read all the transactions, then they could gain access to sensitive private information. In the blockchain, the ledger is decentralized. This means no single computer or single system has control over the ledger at any one time. It would take an incredibly sophisticated, coordinated attack on thousands of devices, simultaneously, to gain this type of access to the main ledger.

ii. Another tenet of security is the chain itself. The ledger exists as a long chain of cryptographically encrypted sequential blocks. Each chain represents another piece of the overall puzzle. Structurally, these records date back all the way to the system’s launch. This means anyone who tries to alter a transaction would first have to alter all transactions leading up to that transaction, and do so accurately. This makes the hypothetical tampering process much more complicated. Also, it greatly increases the overall security of the system.

iii. Unlike present payment systems, in a block chain model here are hundreds to thousands of distinct nodes. Each node has a complete copy of the digital ledger. These can independently work to verify the transaction. If the nodes don’t agree, then the transaction is cancelled. This system keeps the ledger tidy. Additionally, due to its complex mechanisms it is very difficult to commit a fraudulent transaction.

iv. The cryptographic keys along with two keys system used in block chain exchanges are very long, complex and difficult to decipher unless one has authorization to view the keys.

11. Block Chain Security Issues and challenges:

Blockchain has got very complex and rugged structure. In spite of this, in this technology there exists following problems and challenges w.r.t to security. Apart from double spending, which will always be possible in Bitcoin, the attack space includes a range of wallet attacks (i.e., client-side security), network attacks (such as DDoS, sybil, and eclipse) and mining attacks (such as 50%, block withholding, and bribery).

11.1. Traditional Challenges:

The use of a distributed ledger implies that data is shared between all counterparties on the network. On one side this could potentially have a negative impact on the confidentiality; while on the other, it has a positive impact on availability with many nodes participating in the Blockchain, making it more robust and resilient.

Some of traditional security challenges are:

a. Key Management:

Private keys are the direct means of authorizing activities from an account, which in the event they get accessed by an adversary, will compromise any wallets or assets secured by these keys.

Potentially different private keys could be used for signing and encrypting messages across the distributed ledger. An attacker who obtained encryption keys to a dataset would be able to read the underlying data. A private key is usually generated using a secure random function, meaning that reconstructing it is difficult, if not impossible. If a user loses a private key, then any asset associated with that key is lost. If a private key is stolen, the attacker will have full access to all assets controlled by that private key and once a criminal steals the key and transfer funds to another account, it cannot be undone.

b. Cryptography:

Blockchain implementations always operate on the cryptographically generated public and private keys. In case of cryptography, stringent policies and procedures always be followed when managing keys, including people, processes and technology.

The software which is used to generate cryptographic keys should generate strong keys which could not be decrypted easily.

c. Privacy:

Privacy is an additional issue that emerges from the use of Blockchain technology. In a permissionless ledger, all counterparties are able to download the ledger, which implies that they might be able to explore the entire history of transactions, including those to which they are not members. In a permissioned ledger, exploitation of authorised agent' or smart contract capabilities could lead severe exposure of privacy, according to the access right of the agent or smart contract authors.

11.2. The Majority Attack (51% Attacks):

With Proof of Work, the probability of mining a block depends on the work done by the miner (e.g. CPU/GPU cycles spent checking hashes). Because of this mechanism, people will want to join together in order to mining more blocks, and become "mining pools", a place where holding most computing power. Once it holds 51% computing power, it can take control of this blockchain. This may create security issue in a chain.

If someone has more than 51% computing power, then he/she can find Nonce value quicker than others, means he/she has authority to decide which block is permissible. After this attacker can:

i. Modify the transaction data, it may cause doublespending attack.
ii. To stop the block verifying transaction.
iii. To stop miner mining any available block.

11.3. Distributed denial of service:

Distributed Denial of Service attacks coming out of the nature of the distribute ledger remain a concern. For example, if rogue wallets decide to push large numbers of spam transactions to the network it could create potentially a denial of service and increase the processing time, as the nodes will be checking the validity of the fraudulent transactions.

In March 2016, the Bitcoin network was slowed to a near halt. The cause was a Bitcoin wallet pushing large volumes of spam transactions with a higher than average transaction fee. This caused miners to prioritise these transactions when computing new blocks.

Within a permissioned ledger, it would be possible for nodes to agree to ignore or even block the issuer of such spam transactions. However, if an attacker is able to control a large number of clients, they might be able to severely disrupt the network by pushing large volumes of irrelevant transactions.

The distributed nature of Blockchain architecture introduces the prospect that it would be difficult to shut down a malicious program.

11.4. Wallet Management:

Wallet management represents the process and technology used with which a wallet software operates with the keys assigned to it. The wallet software would need to protect the keys from being accessed without authorization, in both cases while stored, but also while in operation with the software.

Losing access to a given wallet might preclude a financial institution from authorising transactions or moving assets. It might be difficult for an entity to be aware that a malicious user has access to the wallet, because copying or stealing the keys might not leave any trace on a computer.

11.5. Eclipse Attack:

An eclipse attack is when majority of peers are malicious and they prevent the user from being connected to the network to obtain information about interested transactions. An eclipse attack is particular useful when a user has sent some bitcoins to other user in some transaction, then decides to also double spend the same bitcoins. The double spender (or user) will use the eclipse attack to prevent the other user from knowing that there is also a double spend transaction out in the open, so other user gets misled into believing that there's only the original transaction.

This attacks mainly targets a single party.

11.6. Sybil Attack:

This attack effects whole network. A Sybil attack is an attack where a single adversary is controlling multiple nodes on a network. It is unknown to the network that the nodes are controlled by the same adversarial entity. For example, an adversary can spawn up multiple computers, virtual machines, and IP addresses. They can create multiple accounts with different usernames and e-mail addresses and pretend that they all exist in different countries.

11.7. Double Spending:

A client in the Bitcoin network achieves a double spend (i.e., send two conflicting transactions in rapid succession) if she is able to simultaneously spend the same set of bitcoins in two different transactions. Mainly, Double-Spending within BTC is the act of using the same bitcoins (digital money files) more than once. somehow an attacker captures 51% of the hash power of the network, double spending can happen. "Hash power" means the computational power which verifies transactions and blocks. If an attacker has this control, he/she can reverse any transaction and make a private blockchain which everyone will consider as real. But so far, no such attack has happened because controlling 51% of the network is highly cost intensive. It depends on the present difficulty of mining, the hardware price, and the electricity cost, all of which is infeasible to acquire.

Blockchain network usually have the mechanism to prevent double spending. Suppose a user have 1 BTC which he tries try to spend twice. He made the 1 BTC transaction to a merchant. Now, he again signs and send the same 1 BTC on another Bitcoin address to try and trick the merchant. Both transactions go into the unconfirmed pool of transactions. But only his first transaction got confirmations and was verified by miners in the next block. His second transaction could not get enough confirmations because the miners judged it as invalid, so it was pulled from the network. But if both the transactions are taken simultaneously by the miners? When miners pull the transactions simultaneously from the pool, then whichever transaction gets the maximum number of confirmations from the network will be included in the blockchain, and the other one will be discarded.

However, there is a possibility of unfair for the merchant, as the transaction might fail in getting confirmations. That's why it is recommended for merchants to wait for a minimum of 6 confirmations. Here, "6 confirmations" simply means that after a transaction was added to the blockchain, 6 more blocks containing several other transactions were added after it. "Confirmations" are nothing but more blocks containing more transactions being added to the blockchain. Each transaction and blocks are mathematically related to the previous one. All these confirmations and transactions are time-stamped on the blockchain, making them irreversible and impossible to tamper with. So if a merchant receives his/her minimum number of confirmations, he/she can be positive it was not a double spend by the sender.

11.8. Routing attacks:

In this attack, set of nodes are isolated from the Bitcoin network, delaying block propagation. In this attack, the adversary delays the delivery of a block by modifying the content of specific messages. This is possible due to the lack of encryption and of secure integrity checks of Bitcoin messages. In addition to these, the attacker leverages the fact that nodes send block requests to the first peer that advertised each block and wait 20 minutes for its delivery, before requesting it from another peer.

12. Real attack incidents:

In this section, we briefly present the existing real-world security breaches/incidents that have affected adversely to Bitcoin and its associated technologies, such as blockchain and PoW based consensus protocol.

a. One of the biggest attacks in the history of Bitcoin have targeted Mt. Gox, the largest Bitcoin exchange, in which a year's long hacking effort to get into Mt. Gox culminated in the loss of 744,408 bitcoins. However, the legitimacy of attack was not completely confirmed, but it was enough to make Mt. Gox to shut down and the value of bitcoins to slide to a three-month low.

b. **Silk Road:** In 2013, another attack called Silk Road, the world's largest online anonymous market famous for its wide collection of illicit drugs and its use of Tor and Bitcoin to protect its user's privacy, reports that it is currently being subjected to what may be the most powerful distributed denial-of-service attack against the site to date. As per initial investigations it was indicated that a vendor exploited a recently discovered vulnerability in the Bitcoin protocol known as "transaction malleability" to repeatedly withdraw coins from system until it was completely empty.

c. In August 2016, BitFinex, which a popular cryptocurrency exchange suffered a hack due to their wallet vulnerability, and as a result around 120000 bitcoins were stolen.

13. Countermeasures:

In this section, the state of art security solutions that provide possible countermeasures for the array of attacks as explained above on blockchain or its different applications:

13.1. No more double spending:

The transaction propagation and mining processes in Bitcoin provide an inherently high level of protection against double spending. This is achieved by enforcing a simple rule that only unspent outputs from the previous transaction may be used in the input of a next transaction, and the order of transactions is specified by their chronological order in the blockchain which is enforced using strong cryptography techniques. This boils down to a distributed consensus algorithm and timestamping. The most effective yet simple way to prevent a double spend is to wait for a multiple numbers of confirmations before delivering goods or services to the payee. In particular, the possibility of a successful double spend decreases with increase in the number of confirmations received.

13.2. Securing wallets:

A wallet contains private keys, one for each account. These private keys are encrypted using the master key which is a random key, and it is encrypted using AES-256-CBC with a key derived from a passphrase using SHA-512 and OpenSSLs EVP BytesToKey. Private key combined with the public key generates a digital signature which is used to transact from peer-to-peer. Bitcoin already has a built-in function to increase the security of its wallets called "multi-signature", which tightens the security by employing the splitting control technique. For instance, BitGo - an online wallet which provides 2-of-3 multisignature transactions to its clients. However, the drawback of using the multi-signature transactions is that it greatly compromises the privacy and anonymity of the user.

A manual method of wallet protection was proposed by called "cold wallet". A cold wallet is another account that holds the excess of an amount by the user. This method uses two computers (the second computer has to be disconnected from the Internet) and using the Bitcoin wallet software a new private key is generated. The excess amount is sent to this new wallet using the private key of a user. Authors in claim that if the computer is not connected to the Internet, the hackers will not get to know the keys, hence the wallet safety can be achieved.

13.3. Security of Networks:

In this section, we will discuss various existing countermeasures proposed for securing the core protocols and its peer-to-peer networking infrastructure functionalities Trust Zone is a technology that is used as an extension of processors and system architectures to increase their security against an array of security threats.

a. **Countermeasures against DDoS Attacks**:

To mitigate DDoS Attacks a Proof of Activity (PoA) Protocol was proposed which is robust against a DDoS attack that could be launched by broadcasting a large number of invalid blocks in the network. In PoA, each block header is stored with a crypt value and the user that stores the first transaction places this value. These users are called "stakeholders" in the network and they are assumed, to be honest. Any subsequent storage of transactions in this block is done if there are valid stakeholders associated with the block. Storage of crypt value is random and more transactions are stored, only if more stake users are associated with the chain. If the length of the chain is more, trustworthiness among other peers increases and more miners get attracted towards the chain. Hence, an adversary cannot place a malicious block or transaction since all the nodes in the network are governed by stakeholders.

One more possible way to mitigate DDoS attacks is by continuous monitoring of network traffic by using browsers like Tor or any user-defined web service. Applying machine-learning techniques like SVM and clustering will identify which part of the network is behaving ill. Hence that part can be isolated from the network until debugged. Other possible methods to protect against DDoS attacks include: (i) configure the network in a way that malicious packets and requests from unnecessary ports will be prohibited, (ii) implement a third party DoS protection scheme which carefully monitors the network and identify variations in the pattern.

b. **Countermeasures against Eclipse Attacks:**

To combat eclipse attack an additional procedure is adopted to store the IP addresses that are trustworthy. If the users are connected to other peers in the network, these peers are stored in “tried” variable. The connection of the user with the peers is dependent on the threshold of the trust factor, which varies from time to time. The users can have special intrusion detection system to check the misbehaving nodes in the network. The addresses which misbehave in the network could be banned from connections. These features can prevent the users from an eclipse attack. In particular, having a check on the incoming and outgoing connections from the node can reduce the effect of an eclipse attack.

c. **Countermeasures against Sybil Attacks**:

Sybil attacks are avoided in Bitcoin by requiring block generation ability to be proportional to computational power available through the proof-of-work mechanism. That way, an adversary is limited in how many blocks they can produce. This provides strong cryptographic guarantees of Sybil resilience.

14. Action items:

a. Dot can study this technology in detail and its implementation in telecom sector should be analysed. Guidelines may be issued for implementation of blockchain in service provider networks for identity management, database management. This also provide a perfect use case for prevention of roaming fraud as it was already an issue amongst service providers. Hence service providers may be directed by DoT to implement blockchain in their network.

b. Blockchain has its one of main application is in field of financial services in banking domains. DoT can work in collaboration with different financial institutions and work out in the security threats of this technology and can help in creating a more secure solution. IRDBT will work and develop different use cases for applications in financial domain. DoT can work in collaboration with them for developing use cases with proper security.

c. Meity has developed a centre of excellence of blockchain. DoT can work in collaboration with Meity to develop security guidelines for use cases developed by them.

d. DoT is developing Central Equipment Identity register A Central Equipment Identity Register is a database of the IMEI numbers of blacklisted mobile handsets, while list numbers including genuine IMEI shipped by vendors/OEMs, suspect list including IMEI numbers reported in theft cases. It connects the IMEI database of all mobile network operators. It acts as a central system for all the network operators to share the black listed mobile terminals so that devices blacklisted in one network will not work on other networks even if the Subscriber Identity Module (SIM) in the device is changed. The CEIR shall be operated and maintained by DoT or any other agency designated by Government and shall be accessible to all the stakeholders including citizens to find out whether mobile device purchased by them is genuine one. TEC can work in collaboration with DoT for study implementation of blockchain in CEIR and create a distributed network.

15. Conclusion:

DLT or blockchain has become one of disruptive technologies with great potential to change our economy, culture and society. DLT enables innovative financial/non-financial decentralized applications that eliminate the need for third party intermediaries. This technology is introducing new data management infrastructure that will accelerate a services revolution in industries (for example, banking and finance, government, healthcare and super logistics) based on telecommunications. These are a significant new avenue for technological advancements, enabling secure transactions without the need for a central authority.

This technology will have a profound impact for telecom users and industries including telecom service providers. This can be major source in increasing the revenue of service providers. Hence, there is a need for identifying the roles and responsibilities of telecom users, operators and service provider with regards to security aspects in the DLT environment.

16. ABBREVIATIONS:

ANDSF	Access Network Discovery and Selection Function
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technologies
eSIM	Embedded Sim
EPC	Evolved Packet Core
IoT	Internet of Things
OTT	Over The Top
POA	Proof of Activity
SHA	Secure Hash Algorithm
SP	Service provider
SSO	Single Sign Off
SVM	Support Vector Machine
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

17. References:

a. Draft NISTIR 8202 Blockchain Technology Overview

b. A Survey on Security and Privacy Issues of Bitcoin by IEEE-Mauro Conti, Senior Member, IEEE, Sandeep Kumar E, Member, IEEE, Chhagan Lal, Member, IEEE, Sushmita Ruj, Senior Member, IEE

c. Paper on Distributed Ledger Technology & Cybersecurity Improving information security in the financial sector by ENISA

d. Paper on Security of Blockchain Technologies by Federal Institute of technology Zurich

e. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin

f. https://due.com/blog/issues-blockchain-security/

g. https://www.telecomstechnews.com/news/2017/nov/17/blockchain-telecoms-it-still-all-hype-or-are-we-moving-towards-reality/

h. Blockchain @ Telco | How Blockchain can impact the telecommunications industry (paper by deloitte)

i. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A Kroll, and E. W. Felten, \Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in IEEE Symposium on Security and Privacy