ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 11(A), pp. 29472-29493, November, 2018

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

A TECHNOLOGICAL PERSPECTIVE OF BLOCKCHAIN SECURITY

Yusuf Perwej[1]*., Nikhat Akhtar[2] and Firoj Parwej[3]

[1]Department of Information Technology, Al Baha University, Al Baha, Kingdom of Saudi Arabia (KSA)
[2]Department of Computer Science & Engineering, Babu Banarasi Das University, Lucknow, India
[3]Department of Computer Science & Engineering Singhania University, Pacheri Bari, Jhunjhunu, Rajasthan, India

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0911.2869

ARTICLE INFO

Article History:

Received 12th August, 2018
Received in revised form 23rd September, 2018
Accepted 7th October, 2018
Published online 28th November, 2018

Key Words:

Blockchain, Big Data, Distributed Ledger, Consensus Protocol, Bitcoin, Delegated Proof of Stake (DPoS), Consortium Blockchain, Blockchain Security, Forking.

ABSTRACT

Blockchain has swiftly become one of the most dominant and promising technologies of the past couple of years. The information security is the key to the development of contemporaneous Internet technology. The distributed mechanism, scripted mechanism, password mechanism and decentralized mechanism of the Blockchain present a perfectly new perspective for the development of Internet information security technology. Blockchain is a distributed database that maintains a successively increasingly list of records called blocks that are secured from any kind of interfere with and revision endeavor. A word that often emerges when talking about Blockchain is Bitcoin. The numerous people still confuse Blockchain with Bitcoinal though, they are not the same. Bitcoin is just one of several applications that use Blockchain technology. In Blockchain every block contains a time stamp and a link to the previous block. Blockchain extant level of security of a system and data perspective for both private and public ledgers. Alternatively, uploading data to a cloud server or storing it in a single location, as well as breaking everything into small chunks and distributes them across the whole network of computers. In this paper, we try to conduct a comprehensive survey on the Blockchain security as well as the challenges and opportunities for the prospective of security and privacy of data in Blockchain. In its present state, several leading companies and governments detect demonstrations of the Blockchain integrated intoidentity management, credential validation, finance, supply chain, property exchange recording, and other territory.

Copyright © Yusuf Perwej., Nikhat Akhtar and FirojParwej, 2018, this is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

INTRODUCTION

The amount of data in our world is swiftly increasing. According to a recent report, it is estimated that 89% of the data in the world today has been created in the last two years as well as current output of data is roughly 2.5 quintillion bytes a day [1]. This data comes from everywhere, such as posts to social media sites, sensors used to gather shopper information, cell phone, GPS signals and videos, purchase transaction, and digital pictures to name a few [2]. This data is called big data [3]. In the big data era, data are incessantly being collected and analyzed, leading to innovation and economic growth [4]. The organizations and companies use the data they collect to personalize services, predict future trends, optimize the corporate decision-making process and more. At present, data is a valuable asset in our economy [5]. There have been different attempts to address these privacy matters, both from a legislative perspective as well as from a technological viewpoint [6]. In recent years, a new class of responsible systems emerged. The first such system was Bitcoin [7], which permits users to transfer currency [8] securely without a centralized regulator, using a publicly verifiable open ledger such as Blockchain [9].

A Blockchain consists of blocks that hold batches of valid and avowed transactions. Every block includes the hash of the previous block in the Blockchain linking the two. The linked blocks form a chain [8], which is called a Blockchain. A Blockchain is factually an append-only data structure maintained by a set of nodes which do not fully believe each other. All nodes in a Blockchain network consent on an ordered set of blocks, each [9] containing multiple transactions, thus the Blockchain can be lookedat a log of ordering transactions. In a database reference, Blockchain can be looked as a solution to the distributed transaction management arduous nodes keep facsimile of the data and agree on [10] an execution order of transactions [11]. In spite of that, conventional database systems work in a trusted environment and employ well known

*Corresponding author: **Yusuf Perwej**
Department of Information Technology, Al Baha University, Al Baha, Kingdom of Saudi Arabia (KSA)

concurrency control techniques to [12] order transactions. The Blockchain superior position is that it does not presume nodes trust each other and consequently is designed to achieve Byzantine fault tolerance [13]. This potentially permits you to use the Blockchain ledger to make sure that the data you backed up and stored in the cloud with third-party vendors [9] has gone entirely unchanged even years, months, and weeks later. No one can deny that Blockchain offers authentic, independent data verification [14].

Related Work

The Blockchain technology enables distributed public ledgers that hold immutable data in aencrypted and secure way and make sure that transactions can never be changed. The condos *et al*. [15] define a Blockchain as an electronic ledger for digital records, transactions, phenomena managed by the participants of a distributed computer network. Earlier, most trade repositories, for lending or sale of securities, were not publicly accessible. In spite of, this does not necessarily indicate who carried out the transactions, e.g. in the case of Bitcoin, the users remain unidentified or pseudo-unidentified, since only the identification tag of the digital wallets is required for a transaction. The Glaser and Bezzenberger [16] and Tapscott and Tapscott [17] *et al* furthermore, a Blockchain is a distributed system without a pivotal control point or authority. The pivotal control points or authorities are not essential in a Blockchain because the distributed network verifies the transactions being performed. This is contemplatea key innovation of the Blockchain technology [18].

Nakamoto 2008 *et al* [19] said if a transaction between two sideis to be made in the network, the nodes in the distributed network compete to find a solution to mathematical puzzle and also store that transaction in the trade repository. A transaction can then no longer be destroyed from the trade repository or ever returned. Tapscott and Tapscott *et al* [17] said the expunction of a central instance in the distributed network implies a radical shift to direct transactions between non-intermediaries or intermediary services. The blocks hold a copy of the last transactions since the last block was added Bogart and Rice *et al* [20]. The Walport *et al* [21] said the data structure of a Blockchain correlate with a database that groups entries into blocks that are linked in chronological order via a cryptographic signature. The Glaser and Bezzenberger *et al* [16] for the verification of the Blockchain different consensus procedure can be used, which are based on peer-to-peer procedure and encryption. Blockchain was fundamentally created as an approach to cryptographic-based payment transactions to confer ansubstitute procedure of trust between two transaction parties. Nakamoto *et al* [22] in classical transactions, the parties have to rely on a faith third party, like as a bank. In the instance of Bitcoin, the essential faith is now completely substituted by the Blockchain, as it permitsfor a mass trade repository operated by many decentralized registers.

Next related to the vulnerability discovered in Ethereum that permits an attacker to eclipse a victim Gervais *et al*. [23] show that a resource constrained attacker can perform eclipse attacks on Bitcoin with only one TCP/IP connection. As long as MDP model does not capture such partial eclipse attacks, we do consider stronger full eclipse attacks. Nasdaq *et al* [24] said you need to have aabsolute ecosystem on the Blockchain for it to offer maximum value to all its stockholder. Yonatan Sompolinsky *et al*. [25] GHOST is an substitute to the longest chain rule for establishing consensus in PoW based Blockchains in which stale blocks also contribute to the security of the chain and in which stale blocks therefore do not influence the security. The Puschmann *et al* [26] define a literature does not provide a structured inter-organizational overview of the emerging Blockchain ecosystem. Mougayar *et al* [27] to imagine the Blockchain ecosystem, some Blockchain landscapes were developed for practitioners clustered companies that are besmeared in decentralized services, crypto-tech computing, or crypto currencies into four major categories with over 20 sub-categories.

There also exist many options to Proof of Work. In Proof of Stake [29], nodes “stake” some value and based on the staked amount get a share of the vote of whether a block is valid. Proof of Burn (POB) is a proposal to subsititute POW by burning coins, i.e. sending them to an address that is verifiably unspendable, such that they can no longer be spent. However, current POB based Blockchain rely on burning coins from POW Blockchain in order to create blocks and therefore can not stand on their own. From a security standpoint, researchers developed different techniques targeting privacy concerns focused on private data. The Yves-Alexandre *et al*. [30] contemporaneous research has demonstrated how anonymized datasets employing these methods can be de-anonymized given even a small amount of data points or high dimensionality data. Latanya Sweeney *et al* [31] said data anonymizationtechnique attempt to defend personally identifiable information. k-anonymity, a common property of anonymized datasets be in need of that sensitive information of each record is indistinguishable from at least k-1 other records. AshwinMachanavajjhala *et al* [32] is respective extensions to k-anonymity include l-diversity, which make sure that sensitive data is represented by a diverse enough set of presumable values. Ninghui Li *et al* [33] t-closeness, which looks at the distribution of sentient data.

Blockchain Architecture

Blockchain endue a shared ledger technology that participants in a business network can use to record the history of business transactions that cannot be modified. In view of the fact that, Blockchain uses consensus [8] to commit transactions to the ledger, the outcomeis final. Every member has a copy of the same ledger, so asset provenance and traceability are transparent and faith [14]. Blockchain systems can seem complex but, they can be comfortably understood by examining and it can be applied to any industry.

Hashes

An essential component of the Blockchain technology is the use of cryptographic hash functions for many operations, like as hashing the content of a block. Hashing is a procedure of calculating acomparatively unique fixed-size output (called a message digest) for an input of nearly any size (such as a file, text, an image) shown in figure 1. Even the smallest modification of input a single bit will outcome in a completely dissimilar output digest. Input the data into a hash function reason the output of a hash value with a few number of digits. This contrivance is characterized by the reality that the same hash value is obtained from the same data, but only an

inappreciable difference in the original [34] data outcome in a completely different hash value. It is extremely arduous to presuppose the original data based on a hash value. The taking mileage of such characteristics, this contrivance is used for the detection of falsification of data, and in the Bitcoin system, it is used for the verification and assurance of the continuity of Blockchain data and the creation of Blockchain through proof of work make use of the calculation of hash values. The Hash algorithms play an important role in security systems where they are used to assure that transmitted messages have not been interfered with [35]. A hashing algorithm makes use of many Blockchain technologies is the secure hash algorithm (SHA) with an output size of 256 bits (SHA-256). So many computers support this algorithm in hardware, making it rapidly to compute.

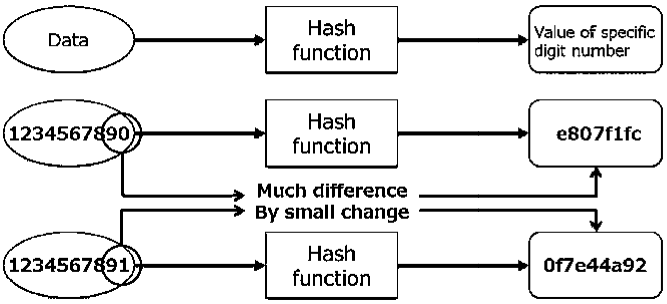

Figure 1 The Hash Functionality

Transactions

A transactionis a recording of a shifting of assets between parties. An analog to this would be a record in a examine account for each time money[36] was deposited or withdrawn. Every block in a Blockchain contains multiple transactions. A single transaction typically need sat least the following information fields.

Transaction ID

A unique identifier for every transaction. The certain Blockchain use an ID, and others take a hash of the distinguished transaction as a unique identifier.

Inputs

A list of the digital assets to be relocated. The each digital asset is uniquely identified and may have different values from other assets [8]. However, assets cannot be added or delete from existing digital assets. Alternatively, digital assets can be divided into multiple new digital assets are combined to form fewer new digital assets.

Outputs

The accounts that will be the receiver of the digital assets. Every output specifies the value to be relocated to the new owner, the identity of the new owner, and a set of conditions the new owners must meet to obtain that value. If the digital assets provided are more than need, the superfluous funds are returned to the sender.

Amount

The total amount of the digital asset to transposition.

Ledgers

Throughout history, pen and paper ledgers have been used to keep track of the interchange of goods and services. A ledger is a collection of transactions. Not long ago, ledgers have been stored digitally, often in huge databases owned and operated solely by centralizing faith third parties on behalf of a community of users [37]. A ledger implemented using a Blockchain can mitigate these matters through the use of a distributed consensus contrivance. The Block chain ledger will be imitated and distributed amongst every node within the system. In figure 2 shown illustratea simple network with four nodes, where each has a copy of a ledger of transactions. New transactions are submitted to a node, which will then caveat the rest of the network that a new transaction has arrived.

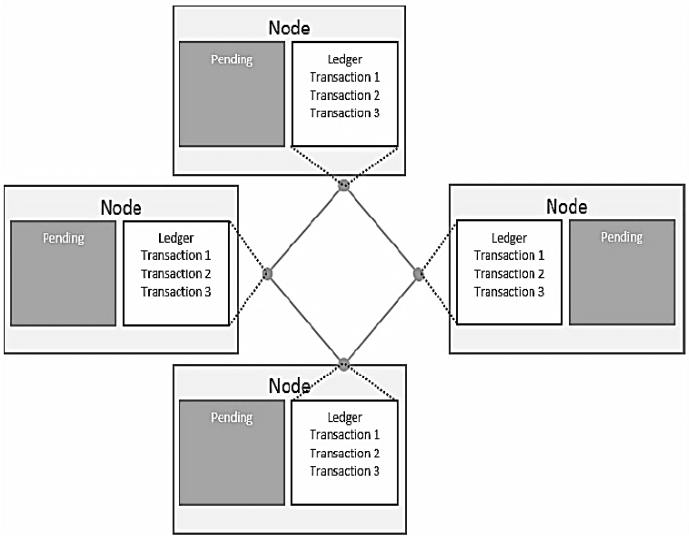

Figure 2 A network maintaining a ledger across nodes

Asymmetric-Key Cryptography

A basic technology utilized by Blockchain technologies is asymmetric-key cryptography (also referred to as public/private key cryptography) [38]. Asymmetric-key cryptography uses a pair of keys a public key and a private key that are mathematically belonging to each other [39]. The public key may be made public without deficiency the security of the process, but the private key must abide secret if the data is to retain its cryptographic protection. Even though there is a connection between the two keys, the private key cannot proficient be determined based on knowledge of the public key. The asymmetric key cryptography uses the various keys of the key pair for specific functions, dependent on which service is to be endured. Asymmetric-key cryptography endue the ability to verify that the user transferring value to another user is in possession of the private key competent of signing the value.

Addressin Blockchain

An address is just like an account number in the bank and it signifies your unique identity on the Blockchainfrom which you can transfer out cryptocurrency and to which you can receive cryptocurrency [8]. Addresses are used to send and receive digital assets shown in figure 3.Each address on the bitcoinBlockchain comes attached with a public key and a private key [15]. These together form the backbone of security in the Blockchain network. The public and private keys always

work in a couple. The public key is a long alphanumeric string that is originated by the private key to an account and this can be publicly shared so that miners can confirm digitally signed transactions. The private key is a string that looks the way the address does and is unique to the owner of a specific Bitcoin address. The proprietor of this Bitcoin address utilization his private key to digitally sign any transaction that he makes. As the name proposes, a user private key is private to the user and the public key is known to every person.

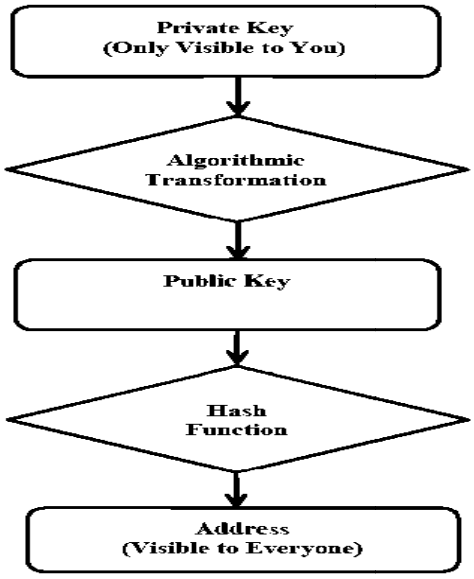

Figure 3 The Address in Blockchain

Firstly, any wallet collects entropy and uses it to generate an Elliptic Curve Digital Signature Algorithm (ECDSA) private key and ECDSA is the cryptographic algorithm in the core of Bitcoin addresses [40]. It is an asymmetric signature algorithm, which means that you can sign piece of information with the private key and calibrate the signature with the public key. This means that anyone can generate the corresponding public key if they are being aware the private key. But, it is not possible to generate the private key from the public key. The Elliptic Curve Digital Signature Algorithm on the private key to get the public key. However, it is a one-way function, there is no route to derive the private key from the public key. It is a derivative of the public key. The various cryptographic algorithms run on the public key to generate the address. The software hashes the public key with SHA 256 and the outcome with RIPEMD-160. Then it adds the bytes 00 as a prefix in the beginning of the consequence of string.

Blocks

The transaction data for all time recorded in files called blocks. Every block records transaction for that time period, and once the block are computed with hashes, it is intaglio, and that will never be changed after that. The participant may submit candidate transactions to [41] the ledger by sending these transactions to some of the nodes engage in the Blockchain. The presented transactions are propagated to the additional nodes in the network. The distributed transactions, then wait in a queue, or transactionpool, so long as they are added to the Blockchain by a mining node. The mining nodes are the subset of nodes that preserve the Blockchain by publishing new blocks.

The transaction is added to the Blockchain when a mining node publishes a block and block containsa set of validated transactions. The calibrate that the providers of funds in a transaction had access to the private key which could sign over the attainable funds. The other mining nodes will investigate the validity [15] of all transactions in a published block and will not accept a block if it contains any invalid transactions. Subsequently, creation each block is hashed thereby creating a digest that represents the block. The transformation of even a single bit in the block would completely change the hash value. The block's hash digest is used to help protect the block from transformation since all nodes will have a copy of the block's hash and can then check to make sure that the block has not been transformed. The block header hash is calculated by running the block header through the SHA256 algorithm two times. A block header hash is not sent through the network, but as an alternative is calculated by each node as part of the verification process of every block.

The version number is used to keep track of upgrades and modification in the protocol. The previous block header hash is the linkage into the foregoing block and secures the chain. The timestamp is the number of seconds since the first of January 1972 and the trouble target of the block is the number of zeroes that must be found when hashing the block header in order to meet the required level of proof of work to retain the block time at 10 minutes. The nonce is the value that is changed by the miners to try disparate permutations to achieve the hassle level required the nonce has been appended by the superfluous nonce function which sits in the coinbase transaction or the first transaction of the Merkle root, indicate who to pay the block reward to a superfluous counter to add permutations to as the nonce number can be used well within a second by the modern mining apparatus.

Table 1 The Block Header Format Data

Field	Description	Size
Version	Block version number	4 bytes
Hash of Previous Block	Hash of prior block header	32 bytes
Time	Unix timestamp	4 bytes
Merkle Root Hash	Merkle root hashtransaction	32 bytes
Nonce	Assents miners to explore a block	4 bytes
nBits	Current difficulty of the network	4 bytes

The storing the hash of every transaction within the header of a block, a data structure known as a Merkle treeis utilized. A Merkle tree likens the hash values of the data together until there is a singular root. The root is an efficient contrivance used to summarize the transactions in a block and make sure the presence of a transaction within a block. This structure bears out that the data sent in a distributed network are valid, since any transformation to the underlying data would be detected and can be thrown away.

Chaining Blocks

The Blocks are chained together through each block containing the hash of the prior block's header, [8] thus forming the Blockchain shown in figure 4. If a prior published block were altered, it would have a dissimilar hash.

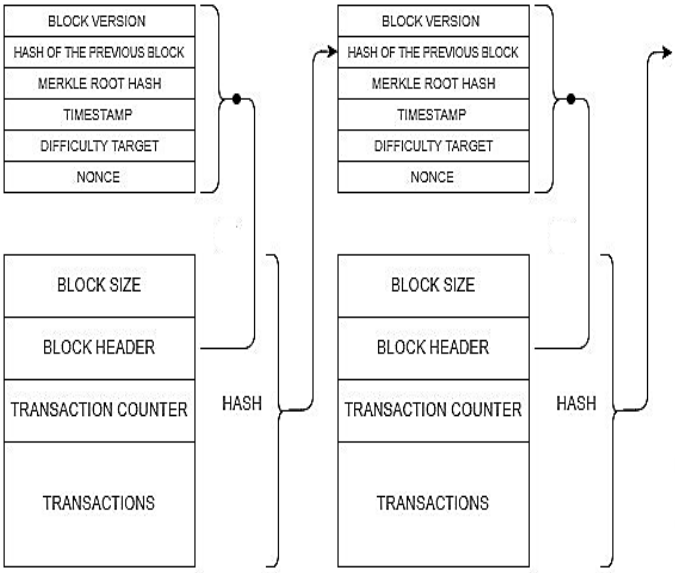

Figure 4 The Chain of Blocks

This in turn would reason all ensuing blocks to also have dissimilar hashes since they include the hash of the prior block. This makes it possible to comfortably detect and denial any modification to prior published blocks. Example for, an electronic coin as a [42] chain of digital signatures. Every owner transfers the coin to the next by digitally signing a hash of the prior transaction and the public key of the next owner and concatenate these to the end of the coin [43]shown in figure 5. A payee can calibrate the signatures to calibrate the chain of ownership.

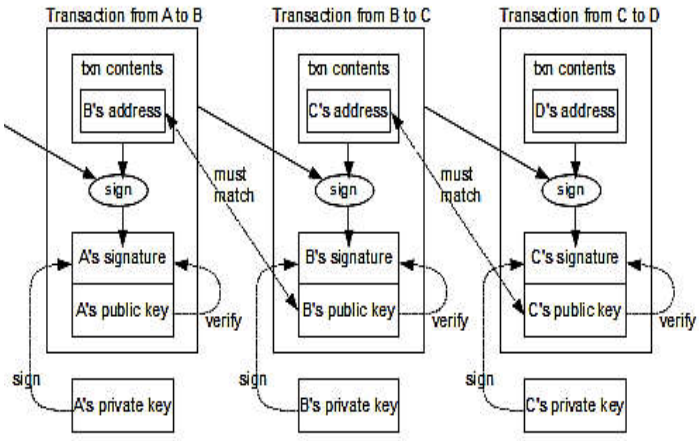

Figure 5 The Chaining of Transactions

Forking in Blockchain

In straightforward terms, fork is an application of a new set of rules to the Blockchainprotocol. Forks belong to the fact that various parties need to use common rules to maintain the history of the Blockchain. Forking signalize any divergence in Blockchainnon permanent or permanent [43]. The forking is said to happen when a Blockchain partitioned into two branches. It can happen as an outcome of a transformation in consensus algorithm or other software transformation. Then, depending on the nature [44] of transform, the fork can be categorized into hard fork and soft fork shown in figure 6.

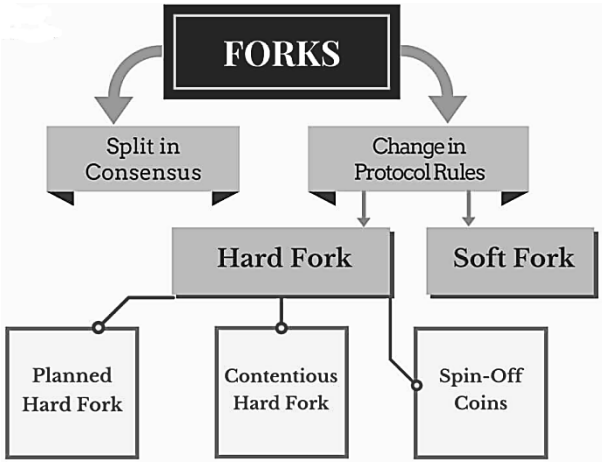

Figure 6 The Forks Structure

Hard Fork

A hard forkis a transform to the technology that will entirely prevent users who do not adopt it from using the transform Blockchain system. A hard fork is a permanent divergence from the prior [45] version of the Blockchain, and nodes running previous versions will no longer be accepted by the current version. A hard fork is a thoroughgoing transform to the protocol that makes prior valid blocks or transactions unacceptable. Any transaction in the forked chain will not be valid on the no longer young chain. All nodes and miners will have to be improved in the latest version of the protocol software if they choose to be on the new forked chain. This essentially creates a fork in the Blockchain, one path which follows the new, improved Blockchain, and one path which continues along the no longer young path. Hard Fork is normally done only when there is enough support from the mining community. When the oodles of miners give a positive signal towards the improved or fork, the developers of the chain start work on the improved code.

Soft Fork

A soft fork is a transform to the technology that will not completely prevent users who do not adopt the transform from using the transform Blockchain system. A soft fork is said to happen when a transform to the software protocol keeps it backward consistent. What this means is that the latest forked chain will follow the latest rules and will also honor the old rules. The actual chain will continue to follow the old rules. This kind of fork needs only a majority of the miners make better to enforce the new rules, as opposed to a hard fork, which needs all nodes to make better and agree with the new version. A new transaction types can often be added as soft forks, needs only that the participants for sender and receiver and miners comprehend the new transaction type. This is done by having the new transaction become visible to older clients as a "pay-to-anybody" transaction and getting the miners to agree to sacrifice blocks including this transaction unless the transaction confirmed under the new rules. This is how to pay to script hash was concatenate to Bitcoin. A soft fork can also occur at times due to a nonpermanent divergence in the Blockchain when miners using non-improved nodes contravene a new consensus rule their nodes don't be aware about.

Forks and Cryptographic Modification

If flaws are established in the cryptographic technologies for a Blockchain application, the only solution may be to create a hard fork, depending on the importance of the flaw. So long as, more than 60 percent of the network is on the new software version, the vulnerability could still happen. They chop and change to a new hashing algorithm could pose aimportance, practical difficulty because [46] it could invalidate all alive specialized mining hardware. Hypothetically, if SHA-256 were explored to have a flaw, there would need to be a hard fork to migrate to a new hash algorithm. The block that change over to the new hash algorithm would lock all previous blocks into SHA-256, and all new blocks would need to utilize the new hashing algorithm. Additionally, cryptocurrencie ssuch as Ethereum use Keccak-256 [47] while Litecoin uses the script hashing algorithm. One possibility for the requirement to converter cryptographic features present in a Blockchain system would be the development of a practical quantum computer system, which would be capable of greatly weakening alive cryptographic algorithms. The cryptographic algorithms utilized within most Blockchain technologies for private & public key pairs will need to be replaced if a sledgehammer quantum computer becomes a reality. This is because algorithms that rely on the computational complexity of integer factorization or work on extricate discrete logarithms namely DSA is very an easy target for quantum computing. The hashing algorithms and Merkle trees that are the other basis for Blockchains are much less an easy target for quantum computing attacks, but are still incapacitate when quantum computers become a tangibility.

Security in Blockchains

The security in Blockchain can be denied as the protection of transaction information and data in a block opposed to internal and malevolent, unintentional, and peripheral threats [48]. Normally, this protection involves prevention of threat, detection of threat, suitable response to threat using security policies, IT services and tools. The Blockchain technology uses many techniques to instate the security of transaction data or block data, regardless of the usage or data in the block. Numerous applications, namely as bitcoin use the encryption technique for data safety [49] describe in detail about using a combination of private and public key to securely encrypt and decrypt data. The other most safe concept of Blockchain is that the longest chain is the authentic one [50]. This alienates the security risks due to 52% the greater number attack and fork issues. As the longest chain is the eventually authentic, the other attacks become null and void as they end up being unparented forks [51].

1. Defense in Entrance. This is a plan which uses a lot of corrective measures to protect the data. It follows the principle that protecting data in multiple layers is more proficiently as against to single security layer.
2. Manage Smear. In this plan, we patch the awed part like application, operating system, code, firmware etc. By obtaining, testing and installing patches.
3. Minimum Prerogative. In this plan the access to data is diminished to the lowest level possible to reinforce the elevated level of security.
4. Manage Hazard. In this plan, we process the risks in an environment by recognize, assessing and controlling hazards.
5. Manage Penetrability. In this plan, we investigation for vulnerabilities and manage them by recognizing, authenticating, metamorphose and patching.

Privacy in Blockchains

The privacy is the competency of a single person or a group to seclude themselves or data therefore expressing themselves discerningly. Privacy in Blockchain means being able to perform transactions without [52] disclose identification information. Concurrently, privacy permits a user to remain compliant by discerningly divulging themselves without showcasing their activity to the entire network [53].The aim of ameliorate privacy in Blockchains is to make it extremely arduous for other users to copy or use other users crypto profile. An enormous volume of variations can be perceived when applying Blockchains technology. Below common characteristics are particularly valuable and are summarized as follows [54].

1. Stored Data Classify. Blockchain endue the exibility to store all forms of data. The privacy standpoint in Blockchain varies for personal and organizational data. Despite the fact that, privacy rules are applicable for personal data, more stringent privacy rules apply to sensitive and organizational data.
2. Storage Distribution. The nodes in the network that stores thorough copies of the Blockchain are called full nodes. The full nodes in amalgamation with the append-only characteristic of Blockchain leads to data no longer needed. This no longer needed of data supports two key features of Blockchain technology including transparency and verifiability. The similarity of application with data minimization adjudicates the level of transparency and verifiability of that network for an application.
3. Connect -only. It is not possible to change the data of previous blocks in the Blockchain undetected. The append only characteristic of Blockchain in certain cases does not curtail to the right to correction of users, principally if data is recorded wrongly. Distinctive observation needs to be provided while assigning rights to data subjects in Blockchain technology.
4. Public vsPrivate Blockchain. The accessibility of Blockchain is noticeable from the perspective of privacy. In an advanced level the banned data on a block can be encrypted for conditional access by authorized users as every node in the Blockchain has preserveda copy of the complete Blockchain.
5. Permissioned vsNon-permissioned category of Blockchain. With public or non-permissioned Blockchain applications, all users in principle are allowed to add data. Permitting the restoration of faith mediatorsinuences the distribution of rein over the network.

Blockchain Categorization

The last couple of years hasintroducedalong a massive increase in the prominence of Blockchain technology. Blockchains are normally categorized based on the permission model, which

determines who can admittance them. If any person can read and write to a Blockchains, it is permissionless. If only specific users can read and write to it, it is permissioned. Both protocols are part of the consensus procedure that helps to validate transactions, but differ widely on who is permitted to calibrate payments and maintain the shared ledger [55]. While permissionless systems are open to any person with the essential computing power and software to validate transactions in a Blockchain, permissioned systems rely on faith validators. It's foremost to note that while participant reach is the main discriminator [56] between permissioned and permissionless systems, both models share a number of core attributes. Both are decentralized peer-to-peer (P2P) networks through which every user has a copy of a shared add-only ledger of cryptographically secured transactions and utilize specific consensus protocols to ensure transactions. Both are frauds and meddleresistant systems that provide an unswerving signature for all records in the Blockchain.

Permissionless

A permissionless system is much like what Ethereumand Bitcoinare based upon and any personcan be a node and join a network to validate blocks that are contributing to the public ledger. In nature, anyperson can read the chain and add new blocks to it. This standpoint is in line with the actual vision for Blockchain to be open, neutral and public. The inadequacy of, the massive amount of computational power that is required to achieve consensus [57]. Every node in the network must solve a complex cryptographic puzzle called a proof of work to make sure transaction validity. What's more, the public character of the ledger makes it visible to every person, which is amatter for enterprise use cases that constrain increased privacy measures. When deciding whether to make use of a permissionless Blockchain, one must consider whether the application required the following standard.

Publicly available data-Since permissionless ledgers tend to permit any personto inspect and contribute to the Blockchain, the data is commonly public. Does the data for the applicationrequiredto be accessible to everyone. Is there any damage to having public data.

Full Transactional Memoir-In view of the open nature of data from these systems, any person can track the transfer of assets between accounts, from the creation of assets, to each transaction in progress.

Fabled data Endeavor-Since any personcould contribute to the Blockchain, some could submit fabled data to the Blockchain, imitate data from valid sources. Is there a way for the application to assure it only gathers data from venerable sources.

Data Fixity - Many applications follow the update, delete, create, and read functions for data. With a Blockchain, there is only read, create. There are methods that can be employed to beseech older data if a newer version is found, but there is no elimination process for the actual data. Can the application manage, possibly outdated unfaltering data. Does the data lend itself to being unfaltering.

Transactional throughput competency - At the present, transactions on Blockchain are not conducted at the same pace as other solutions, so some slowdown while intermission for data to be posted may be incurred. Can the application manage that.

Permissioned

A permissioned system like backwash dependon third-party validates that it has assumptive, like as Microsoft, MIT. Permission can be acquired through available validators, regulatory bodies or a business consortium in charge of making such conclusion. With this contrivance, authorization is required to read information on the chain, verify transactions and afterward add new blocks to it. Privacy is one of the [58] basic advantage of select a permissioned system. In this context, a bank may wish to harness the power of Blockchain and its decentralized nature while keeping the volume of its transactions private for the emulative edge. This type of sensitive information would only be visible to third-party validators, it has invited to its network as antagonistic to being publicly attainable. Permissioned systems are also immeasurably scalable as consensus models can be built on a simplified proof of stake (PoS) protocol as differentiate to proof of work (PoW) utilized in permissionless systems. While permissioned Blockchain are often thinking about an improvement over current systems,certain design characteristics must be thought about carefully to ensure security.

Faith - The faith is another critical opinion when deciding to build an application on a Blockchain. Within a permissioned Blockchain system the method of consensus is normally less computationally intensive, therefore, it could be possible for users to act spitefully. However, the faith does not need to surmount to all users. It is possible for the maintainer of theBlockchain to designate a finite set of mining nodes.

Interfere with explicit design -Another essential opinion is having aInterfere in explicit design. If a malicious mining node tried to alter a block, they might for example, forge a transaction to give themselves money.

Invariableness-Invariableness is essential and is one of the founding principles of the Blockchain. In normally, malicious transactions that enter the Blockchain cannot be unfinished, even if they are identified. To do so needs rewriting published blocks which indefeasibly forks the Blockchain and need the approval of the majority of mining nodes. In a permissioned system this can be convenient since the mining nodes are generally a faith set that have a particular relationship.

Invasion Incidents on Blockchain System

In most cases, the prospective user of Blockchain technology is the simple targets. This category includes those in the business of huge, well-adopted Blockchain implementations such as Ethereumand Bitcoin. The assaults have adopted several techniques to target prospective user and businesses using well established techniques. In this section, we survey primary attacks on Blockchain systems and vectors include.

DAO Incidents on Blockchain system

The DAO (Decentralised Autonomous Organisation) is a smart contract deployed in Ethereum on 28th May of 2016, which execute a crowd-funding platform. The DAO contract was infraction only after it has been deployed for 18 days.Its target is to codify the rules and decisionmaking apparatus of an

organization, remove the need for documents and prospective user in governing, creating a structure with decentralized control. Firstly, the attackerpublishes a malicious, smart contract, [59] which includes a withdraw () function call to DAO inits callback function. The withdraw () will send Ether to the callee, which is also in the form of call. Therefore, it will invocation the callback function of the evil-intentioned smart contract again. In this way, the attacker is capable of to steal all the Ether from DAO. Unfortunately, while programmers were working on fixing this and other difficult situation, an unknown attacker began using this approach to start draining the DAO of ether collected from the sale of its tokens.

Selfish Mining Incidents on Blockchain system

The selfish mining attack is operated by attackers for the objective of obtaining undue rewards or misspend the computing power of truthful miners [60]. The attacker holds explore blocks privately and then efforts to fork a private chain. Subsequently, selfish miners would mine on this private chain, and try to preserve a longer private branch than the public branch because they privately hold more newly explore blocks. For the moment, truthful miners continue mining on the public chain. The current blocks mined by the attacker would be manifest when the public branch approaches the length of private branch,[61] forasmuch the truthful miners end up misspend computing power and gaining no underprice, in view of the fact that, selfish miners publish their current blocks just before honest miners. As anoutcome, the selfish miners gain a competitive benefit, and truthful miners would be incentivized to join the branch maintained by selfish miners. By means of a further consolidation of mining, power into the attacker's side, this attack weakens the decentralized nature of Blockchain. This offer an attack scheme named Selfish-Mine, which can force the truthful miners to perform misspend computations on the musty public branch. In the opening situation of Selfish-Mine, the length of the private chain and public chain are the most similar.

Phishing Incidents on Blockchain system

The Phishing scams are the most familiar Blockchain attacks due to their spreading and favorable outcome rate. Phishing attacks endeavor to gain sensitive, confidential information such as credit card information, usernames, passwords, network credentials, shown in figure 7. Think about the Iota cryptocurrency. The sufferer lost $4 million in a phishing scam that lasted a number of months. The service worked as advertised and enabled sufferer [62] to triumphantly create and use their wallets as expected, providing a false sense of security and faith. The attacker then waited, perseveringly taking benefit of the building faith. After six months, the attacker collected logs, which included secret seeds, and then commence the attack. Using the information earlier stolen, the attacker transferred all funds from the sufferer wallets. The phishing attempts most often begin with an email attempting to instate sensitive information through any user interaction, such as downloading an infected attachment or clicking on a malicious link.

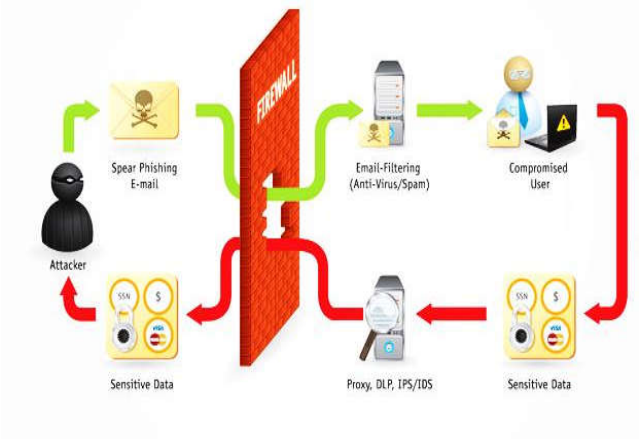

Figure 7 The Phishing AttackScenario

MalwareIncidents on Blockchain system

The malware that compromises an institution's data or harm the institution's information systems can be introduced in a heterogeneity of ways. A malware attack is a type of cyber attack in which malware or malicious software performs activities on the sufferer computer system, usually without his/her knowledge. They were the primary tool used by nasty performers to obtain cryptocurrency. The ransom ware was not new but became a pleasing due to the advantage of transferring and conceal funds through cryptocurrencies. The cybercriminals also had effortless access tools, in particular Hidden Tear, which [63] was meant to be an educational tool on ransom ware but was rapidly used by nasty performers to build hundreds of variants. Malicious performers began experimenting with different type of choice cybercurrencies, also known as altcoins. The ransom ware G and Crabdiscarded Bitcoin in the grace of Dash. GandCrab was added in to the famous RIG exploit kit, along with a different type of malware. GandCrab and other malware launched continual attacks against Adobe Flash Player and Microsoft Internet Explorer via malvertising.

Tor Man-in-the Middle Incidents on Blockchain system

The Tor network is generally used to hide a browser's location from look up to third parties. The numerous employ Tor to createlurking services from which consumers can buy and sell goods. The cryptocurrencies are the preferred or only form of payment. These services are also where ransom ware families often conceal their payment systems. Some are not conscious of Tor, so for comfort, effortlessly accessible Tor proxies are provided to help sufferer reaches these [64] sites and recover their files. Commonly, these include Tor proxy domains they have discovered through a searchengine or were directed to by ransom ware instructions. Unluckily for the sufferer, the attacker may not receive the sufferer ransom. In some cases, funds were redirected to an unassociated wallet using a malicious proxy. This comes about in early 2018 when a Tor proxy service was discovered supersede Bitcoin addresses respectivelytoransom ware with addresses under its control. Security researchers discover the operators scouring sites on the dark web for Bitcoin wallets at the back of the Tor-to-web proxy service onion. When a wallet was located, the cyber thieves use instead of the address with one of their own.

BGP Hijacking Incidents on Blockchain system

BGP (Border Gateway Protocol) is a practically routing protocol and regulates how IPpackets are forwarded to their destination. To inhibit the network traffic of Blockchain, attackers either leverage or manipulate BGP routing shown in figure 8. The BGP hijacking generally needs the control of network operators, which could potentially seize the opportunity to latency network messages. Maria *et al*. [65] pervasively analyze the influence of routing attacks, including both network-level and node-level attacks, on Bitcoin, and show that the number of the triumphingly to-be-hijacked internet prexes depends on the distribution of mining power. Because of the high centralization of some Bitcoin mining pools [66], if they are attacked by BGP hijacking, it will have a worthy of attention effect. The attackers can effectively divide the Bitcoin network, or latency the speed of block propagation.

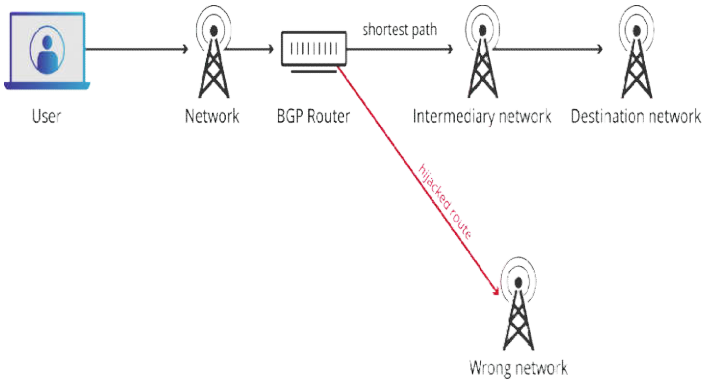

Figure 8 The BGP Hijacking Attack Scenario

Stealing of the Keys Incidents on Blockchain system

For all systems, the stealing of passwords or other access devices through different forms of attack is a common and recurring issue. Blockchains are no different. The majority of attacks belonging to Blockchains[67] have been designed to steal cryptographic keys, not inevitably attack the Blockchainsit self. This experience underscores the significance of enterprise key management to decrease the risk of stolen or compromised keys.

CryptojackingIncidents on Blockchain system

The Cryptojacking is the technique of hijacking a browser to mine cryptocurrency and has astonishingly shown a resurgence. Similar toransomware, cryptojacking campaigns experimented with altcoins. Since 2017, the Archive Poster plug-in for the Chrome browser was found to be mining Monero coins without permission [68]. The sufferer first learned of the problem when some started complaining of high CPU usage. By that period more than 110,000 people had downloaded the miner. At least four versions of the application included the cryptojackingJavaScript code from Coinhive, which comfortably embeds mining into websites or tools, fundamentally with aneasy to-use open-source API. The Cryptojackinginhabit in a gray area. Despite that, many sites do not expose mining, and visitors are left precarious about retard performance.

Web Application Incidents on Blockchain system

Attacks are aimed a web applications are often an outset step in mining private data and credentials that are used by hackers to compromise data on other systems [69]. Depending on the volume of data that is being used to benefit further access, data gleaned from a web application attack can form part of an advanced brute force attack that leverages purloin usernames and passwords to benefit access to customer accounts. In this type of attack known as credential stuffing purloin login credentials are serially and frequently input into the login fields on a website using automated scripts or alter software in order to gain access. Once the hacker triumphingly accesses an account using a purloin username and password, the hacker has access to the financial data and account funds.

Dictionary Incidents on Blockchain system

Dictionary attacks have been around for a period of ten years. Generally, they attempt to break a sufferer password or other authentication mechanism [70]. The dictionary attack extraordinarily a rainbow table attack. When we create a password for an online account, the service provider should not accumulate the password in plain text. As an alternative, it should take a cryptographic hash of the password and store its value. For example, if we use the highly insecure password, the server may protect it as 6baa61e4c9b93f3f0682250b6c, which is the SHA-1 hash of the password string. We can use different hashing algorithms and other method, like as salting, to make this more secure. In spite of, consider what happens if attackers see the preceding string. They might identify that string as the hash for the password. Despite the fact that, in most cases it is arduous to detect a string based on a hash, the reverse is not real. Detect the hash for a string is extremely convenient using a command-line interpreter such as Bash.

Eclipse Incidents on Blockchain system

The Eclipse attacks are a type of network attack that purpose at eclipsing certain nodes from the entire peer-to-peer network. This clearly means, monopolizing a node connectionso that it doesn't receive information from any nodes other than the attacking nodes. In contrast to Eclipse attacks are primarily focused on attacking single nodes rather the entire network at once [71].The primus afraid of Eclipse attacks are the attacks that can come after. The eclipse attack assent an attacker to monopolize all of the sufferer incoming and outgoing connections, which disassemble the sufferer from the other peers in the network [72]. Then, the attacker can filter the sufferer's view of the Blockchain, or let the sufferer's cost redundant computing power on outdated views of the Blockchain. Additionally, the attacker is able to leverage the sufferer's computing power to conduct its own malicious acts. Ethan *et al*. [73] think of two types of eclipse attack on Bitcoin's peer-to-peer network, such asbotnet attack and infrastructure attack. The botnet attack is launched from bots with miscellaneous IP address ranges and secondly infrastructure attack models the threat from an ISP, company or nation-state that has confluent IP addresses. The Bitcoin network might tolerate from disintegration and a sufferer's view of the Blockchain will be filtered due to the eclipse attack.

Distributed Denial of Service (DDoS) Incidents on Blockchain system

Distributed Denial of Service (DDoS) attacks first and foremost target huge organizations. Using botnets9 or other conciliate systems, a DDoS attack sends a stream of traffic and

data to a targeted website to overload the system and for the moment or [74] for all time disrupt system operations shown in figure 9. In a Blockchains network, the cyber security controls underlie at each node provide an additional layer of security that contributes circumference defense and defense in depth for the network.

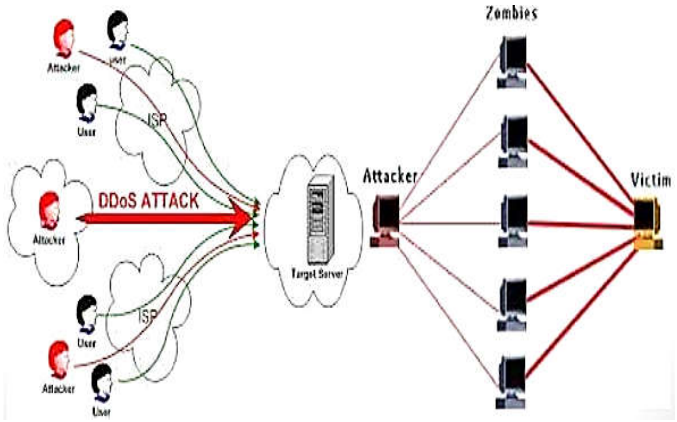

Figure 9 The Distributed Denial of Service (DDoS) Attack

Balance Incidents on Blockchain system

The Christopher *et al*. [75] proposed the balanced attack against POW-based Blockchain, which permits a low-mining-power attacker to momently interrupt communications between subgroups with identical mining power. The Blockchain into a DAG (Directed Acyclic Graph) tree, in which DAG = < B; E>. B is the nodes pointing blocks' information, and they are connected through direct edges E. After introducing a latency between correct sub groups of counterpart mining power, the attacker matter transactions in one subgroup and mines blocks in another suborder called block subgroup, to promise that the tree of block subgroup overburden the tree of transaction subgroup. Even though the transactions are committed, the attacker is able to overburden the tree containing this transaction and rewrite blocks with high probability. The balance attack inherently infringes the stubbornness of the main branch prefix and permits double spending. The attacker necessity to identify the merchant-associated with subgroup and create transactions to purchase goods from those merchants. Later on, the attacker matter transactions to this subgroup and propagates the mined blocks to the rest nodes of the group. While the merchant ship goods, the attacker stops delaying messages [76]. The attacker could triumphinglyreissue another transaction using precisely the same coins. The balance attack signalizes that POW-based blockchain is block unaware of.

Man-in-the-Middle (MITM) Incidents on Blockchain system

A Man-in-the-Middle (MITM)attack include an unauthorized actor positioning its system or access tool in transmissions between a user and a faith party in order to capture or impede datashown in figure 10. This can happen in any form of online communication, like as email, web surfing, social media, etc. Not only are they trying to eavesdrop on your private conversations, they can also target *all* the information internally your devices. There are two types of MITM attacks [77]. A normal attack involves an unauthorized actor within the physical closeness of the target who can gain access to an unsecured network, like as a Wi-Fi router. The second type is commonly referred to as a "Man-in-the-Browser" attack and involves the use of malware, which is injected into an uncircumcised user's [78] system and, without the knowledge of the user, records the data that is being sent to a faith third party website, such as a bank.

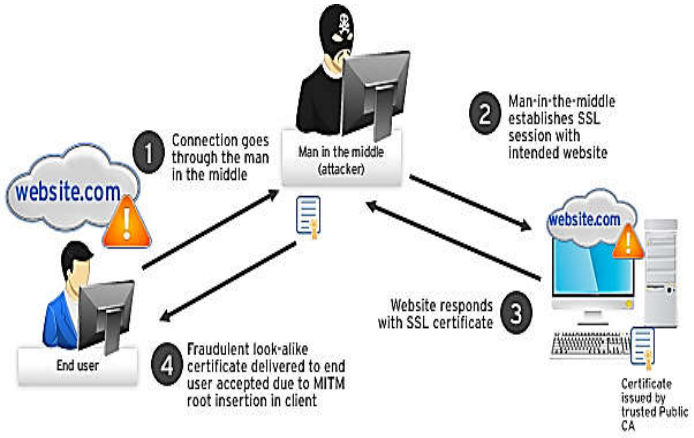

Figure 10 The Man-in-the-Middle (MITM) Attack

LivenessIncidents on Blockchain system

Aggelos *et al*. [79] introduced the liveness attack, which is able to delay as much as possible the verification time of a target transaction. They also present two instantiations of such attack on Ethereumand Bitcoin. Liveness attack be made up of three phases, namely attack preparation phase, transaction denial phase, and Blockchain retarder phase. In attack preparation phase such as selfish mining attack, an attacker builds advantage over truthful miners in some way before the target transaction TX is broadcasted to the public chain. The attacker builds the private chain, which is longer than the public chain shown in figure 11.

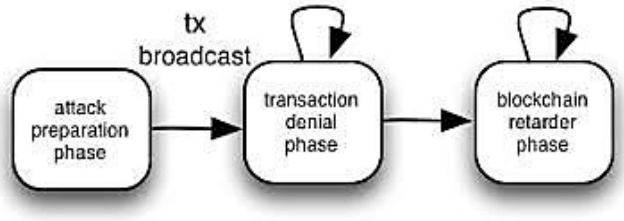

Figure 11 The Liveness Attack Scenario

In secondly transaction denial phase the attacker personally holds the block that contains TX, in order to prevent TX from being written into the public chain. In thirdly Blockchain retarder phase growth process of the public chain, TX will no longer be able to be personally held at a certain time. In this phenomena, the attacker will publish the block that contains TX. In some Blockchain systems, when the depth of the block that contains TX is greater than a stable, TX will be consideredvalid. For that reason, the attacker will continue building private chain in order to build a gain over the public chain. Later on, the attacker will publish her personally held blocks into public chain in suitable time to decelerate the rise rate of public chain.

Routing Incidents in Blockchain system

The Routing attacks are very identical in idea. They rely on inhibit messages propagating through the network and interfere with them before showing them to their peers. The only way for nodes to find out such tampering is when they receive a

varied copy of it from another node. However, what if they have no [80] other source of receiving data propagated through the network. In other words, what if the malicious node is able to split the network so that it splits it into two or more divisions which cannot communicate or see each other anymore. Routing attacks are split into two distinct smaller attacks. At first division attack the attacker attempt to split the network into two or more disjoint groups. This can be done by taking over certain points within the network that act as the linking point between the two groups. Secondly the delay attacks the attacker collect the propagating messages, tampers with them and in the end push them to the side of the network that has not look it before.

Ransomware Incidents on Blockchain system

In Ransomware attacks intimidate to block an institution's access to its own data, unless the institution makes a payment to the hackers. Ransom ware attacks are specifically pernicious in the financial services industry given the significance of customer data and the broader risks if it has strike a bargain. Ransomware attacks [81] dissemblance reputational risk for targeted financial institutions because depositors may withdraw funds in masse based on anxiety that their funds are not safe. The motive for ransom ware attacks is nearly always monetary, and unlike other types of attacks, the sufferer is usually notified that a seize the opportunity has occurred and is given instructions for how to recover from the infraction. Payment is often demanded in a virtual currency, like as bitcoin, so that the cybercriminal's identity isn't known. Ransomware attacks are renowned in view of them can be carried out anonymously. Ransomware malware can be proliferated through malicious email attachments, infected external storage devices, infected software apps and compromised websites. In a lockscreen transmutation of a ransom ware attack, the malware may change the sufferer login credentials for a computing device in a data abduction attack, the malware may encrypt files on the infected peripheral device, as well as other connected network peripheral device.

Sybil Incidents on Blockchain system

One of the primus problems when connecting to a peer-to-peer network is Sybil attacks [82]. A Sybil attack is atry to control a peer network by creating multiple counterfeit identities shown in figure 12. To the outside spectator, these counterfeit identities appear to be unique users. In spite of, behind the scenes, a single entity controls many identities at once. A Sybil attack is one where the attacker professes to be so many people at the same time. A peer-to-peer network, maintaining a Blockchain. Atruthful salesperson is analogous to any sincere node in the network that desire [83] to connect to other nodes in order to engage with them. Think about a malicious node that has been able to create so many identities in the network. Inside the network, this malicious node looks like it is a huge group of nodes representing a huge percentage of the network. The other sincere nodes may not be able to enucleate such behavior and may accept shared information from this malicious node consideration the data are arriving from so many different sources (i.e randomness is inflict). This insinuate that Sybil attacks target the network as a whole not a specific node. Such attacks are hard to explore, but unluckily, they do occur.

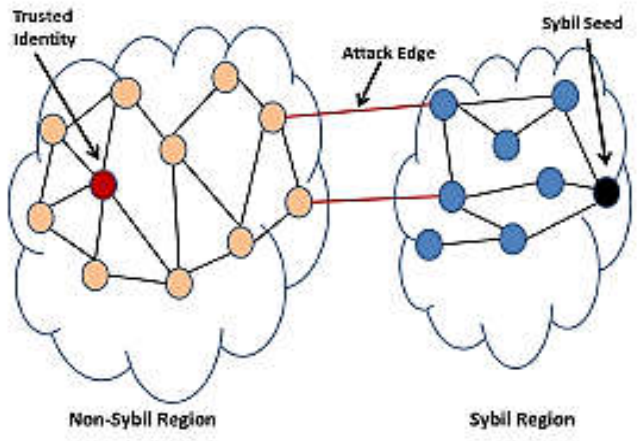

Figure 12 The Sybil Attack Scenario

Identity Based Incidents on Blockchain system

The permissioned Blockchains are not liable to from identity-based attacks like those targeting other IT systems, like as deceive or Sybil attacks. Such attacks could be employed to take over a larger number of the nodes in [84] a network and weaken the consensus validation and distributed architecture protections of a network. This type of risk can alleviate using a faithfulness multi-tenant cloud-based directory and identity management service that certifies the identities of persons seeking to involve in the network. Any outsider threat actor that efforts to take over nodes on the network would be identified by the service and rejected access to the network. These cloud-based services deploy their personal cybersecurity protections and provide an extra layer of protection for the network.

Double Spending Incidents on Blockchain system

A double spending attack happenswhen the same set of bitcoinsis spent in two dissimilar transactions shown in figure 13. Since its beginning in 2009, the Bitcoin has been tackling the critical technical problem of double-spending. For instance, an attacker could leverage race attack for double spending. This kind of attack is comparatively easy to implement in POW-based Blockchain, therefore the attacker can seize the opportunity the intermediate time between two transaction initiation and verification to hastily launch an attack. Prior to the second transaction is mined to be invalid, the Attacker has already got the first transaction's output, consequence in double spending. It involves arranging things so that a vendor sees a [85] transaction substantiation, but a double-spend transaction makes it onto another fork, which eventually becomes the main branch [86].

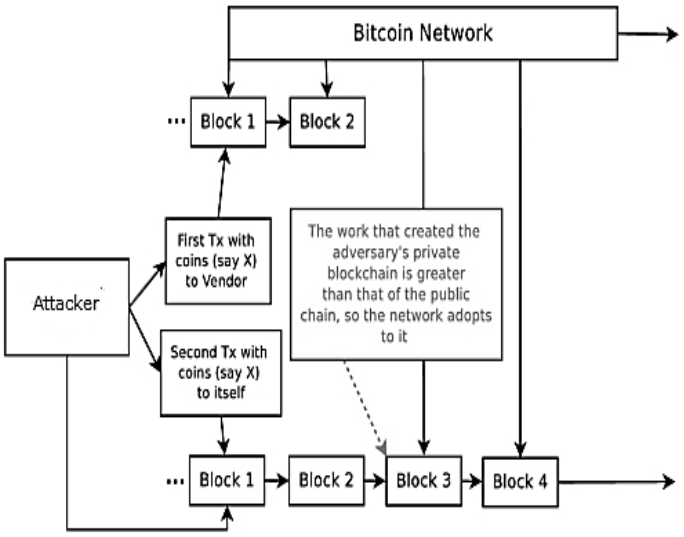

Figure 13 The Double Spending Attack Scenario

The Blockchain also introduces dissimilar attack vectors that malicious actors may seek to make use of. Attackers will also seek to create new fraud through mechanisms that will need to be created to decide and remediate deception. Finally, an integrity control system will be required to make sure that those in control of decision-making in relation to the chain are acting as fiduciaries of the chain, rather than as self-interested owners of the chain. By now, perhaps you have noticed that peer-to-peer network security will never be completely secure as well as at least in the time being. Although, peer-to-peer networks unquestionably improve security over centralized systems. In as much as, Blockchains are maintained over such networks, they can introduce potential solutions to trouble that exist today. Even if network security concerns are indefeasible today, we can at least attempt to limit them by educating the public and pointing them to best practices that can help mitigate them.

Security Improvement in Blockchain

The Blockchainsprovide for a number of opportunitiesin mitigating cybersecurity risks and preventing, detecting, and fight the types of cyber-attacks that are often directed at financial institutions.In this section, we summarize security improvement to Blockchainsystems, which can be used in the development of Blockchainsystems.

Distributed Architecturein Blockchain

The distributed architecture of a permissionedBlockchains is abenefit that can deter or minimize the influence of cyber attacks. Threat actors commonly select target a centralized database that, [87] once compromised, would contaminate and destabilize the system as anentire. A distributed network structure, provides inherent operational flexibility because there is no single point to lack of success. With the risk of reconciliation scatter among various nodes, an attack on one or a small number of participants would not outcome in the loss or the reconciliation of the ledger keep in computer nodes not subject to infraction.

The Smart Pool in Blockchain

This poses a grave threat to the decentralized nature, making Blockchainvulnerable to various kinds of attacks. Loi *et al.* [88] propose a novel mining pool system named SmartPool. The Smart Poolgets the transactions from Ethereum node clients [89], which contain mining task information. Then, the miner conducts hashing enumeration based on the tasks and returns the accomplished shares to the smartpool client. When the number of the accomplished shares reaches to a certain amount, they will be committed to smartpool contract, which is deployed in Ethereum. The smartpool contract will calibrate the shares and deliver bounty to the client and differentiate with the traditional P2P pool, SmartPool system has the many advantages. At first the core of the SmartPool is implemented in the form of smart contract, which is deployed in Blockchains and miners requirement first connect to Ethereum to mine via the client. After that mining pool can rely on Ethereum's consensus mechanism to execute. It makes sure decentralization nature of pool miners. The mining pool state is sustained by Ethereum and no longer need a pool operator. Secondly the Smart Pool leverages a novel data structure, which can inhibit the attacker from resubmitting shares in several batches. Besides, the verification method of SmartPool can promise that truthful miners will gain expected rewards even there live malicious miners in the pool.

The Consensus Establishment Mechanism in Blockchain

The use of a consensus mechanism for establishment new blocks of data providesan other key cybersecuritygain on apermissioned Blockchain network. A consensus mechanism needs a stipulated number of nodes to reach a consensus on whether a new block of data is valid and appropriate for inclusion in the shared ledger and whether the ledger itself, with its whole history, is accurate, pursuant to the network's establishment rules [90]. A consensus mechanism endue a sustained examine on the integrity of past transactions identified on the ledger and on the integrity of new blocks of data. An attacker attempting to settle the ledger would be required to co-opt the consensus mechanism by settlement enough nodes to frame up the consensus establishment process and thereby dishonest or interfere with the ledger. A permissioned Blockchain network may stop like as an attack from being effective if the network contains a enough number of nodes

Inhibit Sybil Attackin Blockchain

The first way to reduce a Sybil attack is to dilation the cost of creating a new identity. Because identities can map to entities on a many to one ratio, [82] we necessity a way to make it resource intensive to create too many identities. Blockchain use the cost of creation as a Sybil protection feature via mining. In proof of work algorithms, in order to create a new identity on the mining network, you'll to necessity another computer with the processing power to contribute. This attaches a valuable cost to adding hundreds or thousands of pseudonymous nodes that might be able to effect the acquisition of a fork or other Blockchain vote. The same goes for proof of stake, where purchasing computing power is changed by staking currency. There's a cost to join the [83] network and have a vote. That resource need limits the number of accounts a nasty actor can create. A second way to battle Sybil attacks are in need of some type of faith prior to allowing a new identity to join the network. This commonly takes the form of a goodwill system, where only instituted, long-term users can invite or vouch for

new entrants to the network. The chain of faith also enlarges to outright identity verification and few peer networks need you to submit identification before joining. Others permit you to join if you can answer a two-factor validate security code. All of these needs, some level of identity verification or faith building before an account receives voting special right, [82] making the creation of pseudonyms more challenging. They reduce the threat of Sybil attacks is by weighting user power based on goodwill. Users that have been around the longest and demonstrated themselves receive more voting power of sectarian judgment. This makes the system a meritocracy as an alternative a pure democracy, and it decreases the power of new users. As an outcome, numerous recent or less-active accounts don't grant a Sybil attacker any gain against venerable older, more effectual accounts.

Oyentein Blockchain

Loi *et al*. Introduce Oyente to discover bugs in Ethereum smart contracts [91]. Oyente leverages emblematic execution to analyze the byte code of smart contracts and it follows the execution model of EVM shown in figure 14. The Ethereum stores the byte code of smart contracts in its Blockchain, Oyente can be used to discover bugs in deploying contracts. It takes the smart contract's byte code and Ethereumomnibus state as inputs. At first, based on the byte code, CFG builder will statically build CFG (Control Flow Graph) of smart contract. Then, in pursuance of Ethereum state and CFG information, explorer headship simulated execution of smart contract leveraging stable embleenhance matic execution. In this scenario, CFG will be [92] further enriched and improved because some jump goal are not constants alternates, they should be computed during emblematic execution. The core analysis module uses the respective analysis algorithms to discover four various vulnerabilities. The validator module validates the discover vulnerabilities and vulnerable paths. The ratify vulnerability and CFG information will ultimately be output to the visualizer module, which can be employed by users to abolish program analysis and debugging.

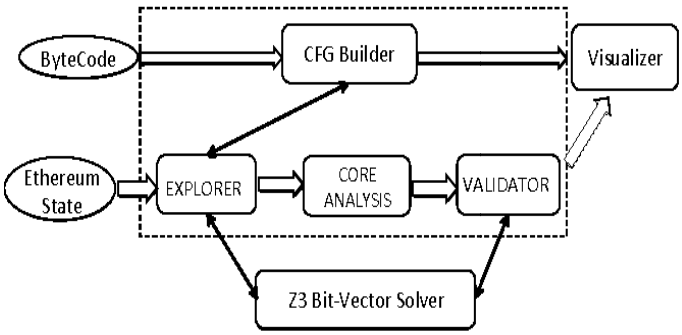

Figure 14 The Oyente Architecture Scenario

Transparencyin Blockchain

The transparency in permissioned Blockchain networks confers another degree of cybersecurity protection. For example, the transparency of a permissioned Blockchain among stockholder makes it more an objection for hackers to place malware in the network to accumulate information and to transmit it covertly to another database managed [93] by the infiltrator. Because each stockholder has an identical copy of the ledger, the network creates the chance for deploying increase obedience processes, including, among other things, real-time auditing or keep an eye on by other stockholder or by regulators granted limited access to the network. As anoutcome, vulnerabilities and threats may be identified briskly if good risk management and obedience controls are implemented.

Quantitative Frameworkin Blockchain

A quantitative framework, which is leveraged to analyze POW-based Blockchain execution performance and security provisions. The framework has two components first Blockchain stimulator and second security model [94]. The stimulator imitates Blockchain execution, whose inputs are parameters of consensus protocol and network. By means of simulator's analysis, it can gain performance statistics of the aim Blockchain, including network latency, block sizes, block propagation times, decrepit block rate, flow capacity etc. The decrepit block signify to a block that is mined but not written to the public chain. The flow capacity is the number of transactions that the Blockchain can manage per second. The decrepit block rate will be passed as a parameter to the security model component, which is based on MDP (Markov Decision Processes) for the win against double spending and selfish mining attacks. The framework lastly outputs most favorable adversarial action plan against attacks, and make possible to building security provisions for the Blockchain.

Administrator Risk Controls in Blockchain

The Permissioned Blockchain mostly are hosted on cloud platforms that have strong cybersecurity controls across various layers of the technology stack. Besides, major cloud service provider like Microsoft voluntarily submit to periodic independent audits headship by internationally accredited firms, which focus on the cloud service provider compliance to industry leading standards of the International Standards Organization (ISO), the National Institute of Standards and Technology (NIST), and others. The Cloud computing offers participants an effortlessly accessible and highly fault obstructive platform, resulting in less stoppage, lower risk of lost transactions, and lower risk of lack of success to reach consensus. The cloud service provider also has the capability to implement system wide improve and patches in a much more intense and extensive style, while leveraging maximum threat intelligence ascertain across the network.

Hawkin Blockchain

The Ahmed *et al*. Introduce Hawk, a novel framework for developing privacy-preserving smart contracts shown in figure 15. In Hawk, developers can write private smart contracts, and it is not essential for them to use any code encryption or obfuscation techniques [95]. Moreover, the financial transaction information will clearly not be stored in Blockchain. When programmers develop Hawk contract, the contract can be split into two parts, first privateportion, and second public portion. The private data and financial function concerned codes can be written into the private part, and codes that do not involve private information can be written into the public part. The Hawk contract is compiled into three portions. The first program that will be run on all virtual machines of nodes, just like smart contracts in Ethereum. Second, the program that will only be executed by the users of smart contracts. Third the program that will be executed by the manager, which is a particular reliable party in Hawk. The

Hawk can not only defend privacy against the public, but also defend the privacy between different Hawkcontracts. If the manager aborts the protocol of the Hawk, it will be automatically financiallyestreat, and the users will gain reimbursement. The Hawk can comprehensively defend the privacy of users when they are using Blockchains.

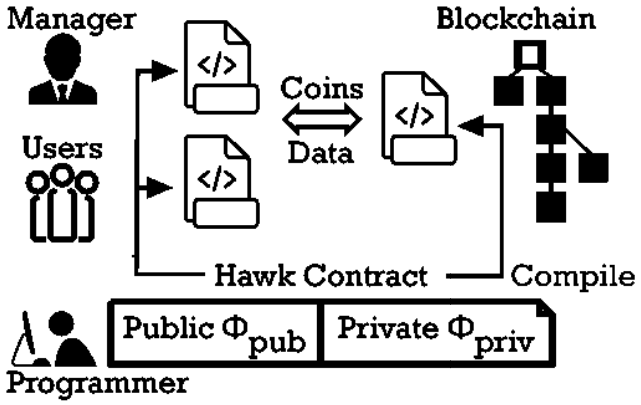

Figure 15 The Hawk Framework

Network Effectsin Blockchain

The distributed network structure of permissioned Blockchain creates inherent operational elasticity because there is no single point of lack of success in the network. On the other hand, the involvement of various entities, each with their own firewalls, is a source of outsider vulnerability. This structure dissemblance challenges in managing identities, involvement rights and restriction, private and public key storage, maintenance, and dispute, and security configurations across multiple outside parties [96]. Besides, financial industry involvement in permissioned Blockchain each has their own cybersecurity programs and follow their own cybersecurity risk deficiency techniques. This structure endue perimeter safeguards and safeguard in depth, but also needsextra planning to make sure these programs are not incompatible with, and indeed complement, the Blockchain network's cybersecurity program.

Town Crier in Blockchain

The F. Zhang *et al*. Introduce Town Crier (TC) that addresses this challenge by providing an authenticated data feed for smart contracts [97]. The Town Crier acts as a high faith bridge between existing Ethereum Blockchain and the HTTPS-enabled data websites. It brings back to website data and serves it to relying contracts on the Blockchain as concise pieces of data called datagrams. Since the smart contract deployed in Blockchain cannot access network straight, they cannot get the data through HTTPS. Town Crier precisely acts as a bridge between HTTPS-enabled data source and smart contracts. The basic framework of Town Crier is shown in figure 16. The Town Crier contract is the front end of the Town Crier system, which action as API between users' contracts and Town Crier server. The core program of Town Crier is executed in Intel's Software Guard Extensions (SGX) enclave [98]. The primary function of the Town Crier server is to instate the data requests from users' contacts, and instate the data from target HTTPS-enabled websites. Ultimately, the Town Crier server will return a datagram to the users' contracts in the form of digitally signed Blockchain messages. Town Crier can comprehensively defend the security of the data requesting process. The primary modules of Town Crier are respectively executed on decentralized Ethereum, SGX-enabled enclave, and HTTPS-enabled website. In addition, the enclave disables the function of network connection to maximize its security and relay module is designed as a network communicationhub for smart contracts, SGX enclave environment, and data source websites. Hereupon, it achieves segregation between network communication and the execution of the Town Crier main program. Further, if the Relay module is attacked, or the network communication packets are interfering, it will not modifythe normal function of Town Crier [97]. The Town Crier system enduea strong security model for the smart contracts' off chain data interaction, and also supports confidentiality. It enables private data insistence with encrypted parameters.

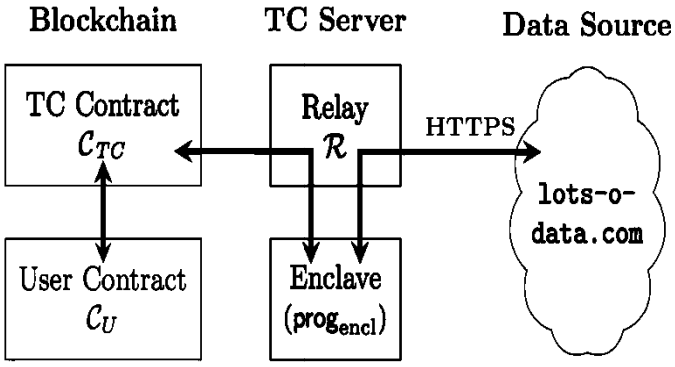

Figure 16 The Town Crier Framework

Roles and Accountability of Participantsin Blockchain

To retain robust network security, the roles and accountability of each type of participant must be distinctly defined and impose, and the cybersecurity risks posed by each type of participant must be identified and managed. It is also necessary to anticipate the security outcome of participants leaving and entering the network over time. Blockchain developers are consecutive start-up firms, although many are lead by seasoned industry veterans. Regardless of a developer's size or [99] the experience of its personnel, all Bblockchain developers, especially those developing solutions for the financial services industry, must conduct their design and development activities at a high level of tincture relative to security threats. Blockchain developers should expect threats come out from interoperability, demeanor threat modeling, demeanor intrusion testing using many attack vectors and scenarios, document the development process, and get individualistic audits of the design and development process. The handling entity implements and apply network rules and protocols. In the network rules should address what data to comprise and not to comprise on the Blockchain in view of emulative opinion, participant turnover, and best practices for privacy and security. The managing entity's roles and accountability may comprise the following first enforcing agreed upon cybersecurity standards, secondly endow secure and compartmentalized platforms to make easier collaboration and interoperability without debilitate security or emulative interests, thirdly handle participant entree and permissions, in fourthly handle the private and public key infrastructure, fifthly the manage validation audits on participants, and lastly reply to cybersecurityincidents that influence the network.

Immutabilityin Blockchain

The immutability of Blockchain records is a very necessary attribute of permissioned Blockchain. Immutability inhibit defeaturewith records in the ledger and creates a final auditable record. However, immutability also limits recovery choice when foul or malicious transactions are introduced into a Blockchain ledger. In most instances, a hard-fork is being expected to dissociate such transactions and something to a new the ledger around such transactions [100]. Participants in a permissioned Blockchain can set up governance structures and plan of action to address events in which foul or malicious transactions are introduced into the ledger [8]. Nevertheless, dependent upon network participants to weigh the advantage and disadvantage of immutability, and the impression of workarounds, when developing permissioned Blockchains, especially for financial services applications.

How Blockchain is Realignment Our World

This section highlights various types of Blockchain services and how can realignment our world using this service [101].

In the Government Scenario

The Estonian government has the partner of Ericsson on an initiative involving creating a new data center to move public records onto the Blockchain. Dubai has set look on becoming the world's first Blockchain powered state. In 2016 representatives of 30 government departments formed a committee committed to discover eventuality across health records, preventing the spread of conflict diamonds and shipping, business registration. The UK department of work and pensions is inquire into using Blockchain technology to record and administer profit payments. In July 2018, the UK's Food Standards Agency (FSA) completed a pilot using Blockchain to track the distribution of meat in a cattle slaughterhouse. Samsung company is creating Blockchain solutions for the South Korean government, which will be put to use in transport applications and public protection. The government of Gibraltar pilfera march of many other nation in the race to be the global hub for Blockchain basedfintech companies. The Government through the Gibraltar Financial Services Commission (GFSC) issued a ruling that effectively grants licenses which permit Blockchains to be used as conduits for the storage and transfer of digital assets.

In the Charity Scenario

This service goal to provide greater transparency to charity donations and intelligible links between giving and project outcomes. It is working with established charities accompanied save the kids, the water project and medic mobile. The clean water coin is the first coin designed and developed to be used by nonprofit organizations. The coin was designed and developed to permit a community to participate in providing clean water for the use of the people. The finest thing about the coin and the creator is that human beings can check how they are using their money. Bithope is composition to ahead develop and promote charity via cryptocurrencies crowdfunding. As cryptocurrencies are seen as a disrupting charity sphere, there is a need to rebuild faith, so that people can safely donate to charity and see their money used for what it's meant for. Give Track also provides real-time financial transparency to create a great future of charity donation. BitGive created the GiveTrack platform for effective benevolence. The creator of this stage is a non-profit organization which like better the use of bitcoin as the means of donating to charity. It is also the first bitcoin charity organization that is legally recognized for non-profit status in the USA.

In the Transport and Tourism Scenario

The Blockchain and tourism have the probable to turn into a very profitable combination as this technology can endow more security and transparency to critical touchpoints. In the circumstance of a travel agency booking flights and hotels for a client, it has to send the information to the different firms. IBM has said it will go public with a number of non-finance belonging Blockchain initiatives with global partners in 2018. This video imagine show capacity could be driven in the vehicle leasing industry. The Austrian National Tourist Office is built up history by being among the first in the world to run a digital ad expedition powered by Blockchain technology. In the Arcade City an application which aims to beat Uber at their own game by moving ride sharing and car hiring onto the Blockchain. The Webjetonline travel portal is developing a Blockchain solution to permit stock of empty hotel rooms to be efficiently tracked and traded, with payment orders routed to the network of middlemen sites besmeared in filling last minute vacancies. Maersk has been already an established transportation company that manages cargos across the whole world. Now, they are slowly transiting to Blockchain solution so that they can take advantage of the integrity, transparency, and security provided with it. The companies or transport ports will have better control over the goods. This also means that unlawful transport will be completely stopped as data once stored cannot be altered.

In the Manufacturing and Industrial Scenario

Blockchain tech makes easier coordination of all kinds of human interaction; helps arrange collaborative work effectively, and, all in all, lays the groundwork for transition of man-machine interaction to the new level. In the provenance project goal to endow a Blockchain based provenance record of transparency within supply chains. A good example here is SyncFab, a manufacturing supply chain Blockchain the world's primary peer-to-peer industrial marketplace for the manufacturing industry. The company goal to revolutionize the sphere by connecting buyers directly with the hardware manufacturers saving their time, money while increasing efficiency, transparency, and definitely, profitability. In the India's biggest conglomerate, Reliance Industries, has said that it is developing a Blockchain based supply chain logistics platform along with its own cryptocurrency, like Jiocoin. The STORJ.io distributed and encrypted cloud storage, which permit users to share unused hard drive space. A Blockchain platform which main attention on anti for gedmeasures, with initial use cases in the diamond, pharmaceuticals and luxury goods markets. In a SKUChain Blockchain system for permittracking and tracing of goods as they pass through a supply chain.

In the Healthcare Scenario

The SimplyVital health is a Blockchain solution that connects sick person and providers under one platform. It is a health data management solution and also uses machine learning and

algorithms prediction for the best possible solution. The analytical insights are conferring for sick person experience. It also works uniformly for private providers, health systems, and hospitals. The Gem startup is working with the Centre for Disease Control to put disease outbreak data onto a Blockchain which it says will rise the success of disaster relief and reaction. The prime components are the Health Nexus. It is a HIPAA-harmonious protocol that is accepted worldwide. A protocol that can be used to connect healthcare data and sick person control.

In the Media Scenario

Kodak One is an image, right management platform that executes on top of the Blockchain and uses KODAKCoincryptocurrency to fuel it. It empowers creative builders to license their work securely and safely. The licensing fees are also less and lead to more income when hosted on the Kodak One platform. It perfectly transforms the image economy and also make sure that ownership is maintained via the lifecycle of the images and also create a licensing platform that defend the rights of the image creators. Ujomusic is a Blockchain platform that entitlesmusic. It is created for music creators so that they can have absolute rights on music that they create. The Civil is a Blockchain project that is targetedtowards journalists. It is a market where journalism can sustain and flourish in the suitable direction. The numerous projects are running on Civil including FAQ NYC, Colorado Sun, Popula and so on. The project targetsto fix the loopholes in the present journalism practice and incentivize collaborative behavior than the rivalry.

In the Financial Services Scenario

The transfer of value across-borders has always been acostly and slow process. Blockchain is able to speed up, make simple, and decrease the costs significantly. For instance, if a person wants to transfer money from USA to their family in India, who have an account with a local bank, it takes a number of banks and currencies prior to the cash can be collected. Blockchain can speed up and, make simple this process, cutting out many of the conventional middlemen. According to a Deloitte study, Blockchain decrease the costs to 3-4% of the total amount and provides promise, real-time transactions across borders. Barclays has launched a number of Blockchain initiatives include tracking financial transactions, compliance and combating fraud. The Standard Chartered Bank considers Blockchain as their way to cut costs and make better the transparency of financial transactions. Loan and mortgage processing today, it's anintricate process with several stakeholders, inherent inefficiencies and frequent manual errors and lateness. The process could be notably simplified by incorporating smart contracts. For example, smart contracts could automatically calibrate land ownership and interface with various stakeholders such as legal and tax departments. By alienatingsilos, a Blockchain solution would delete inefficiencies, decrease time and cost, and support better customer incident. The Augur permitsthe creation of Blockchain based forecast markets for the trading of derivatives and other financial instruments in a decentralized ecosystem. Selling stocks and shares has always involved many middlemen, like as brokers and the stock exchange itself. Make a decentralized and secure ledger, a Blockchain giving every party a say in the validation of a transaction, speeds up the settlement process, permit for greater trade accuracy, and can cut out more middlemen. The ABRA cryptocurrency wallet, which uses the BitcoinBlockchain to keep and track balances stored in dissimilar currencies. Todayscenario, claims processing is a notoriously prolonged and intricate process, needs verification from several intermediaries before a payment can be made to the claimant. The smart contracts assurance to modify that and also claim form can be distributed across all participants in the chainfrom the claimant to the payer. Again, NasdaqLinq is a digital ledger technology that leverages a Blockchain to facilitate thecataloging, issuance, and recording of transfers of shares of privately held firmsin the Nasdaq Private Market.

In the Real Estate Scenario

The userfriendly automation of all episodic processes and documentation on a decentralized, Blockchain real estate platform could also assist by cutting out extra inspection costs, property taxes, as well as registration and loan fees, all enforced by quantifiable smart contracts. Omnipresence is one of the finest Blockchain use cases of real estate industry. It is one of the first real estate platforms that endow Software-as-a-Service to organizations and help them securely store and track property. The SaaS application executeson top of the Blockchain which means that it offers clearness, authenticity, and security. The smart contracts into Blockchain real estate ledgers and transactions has a clear capacity in streamlining several real estate processes, like as releasing apartment ownership, or rental documents upon anending of a cryptocurrency transfer. The advantage of this a particular part of the Blockchain use case when applied to real estate are already being recognized by a variety of private institutions and governmental bodies.The Meet Propy, the ideal Blockchain use case for property transactions. Utilize this Propy, somebody can buy and sell the property and enjoy the advantage of transparency and security by using Blockchain. This way both the seller and buyers are secure as it is next to improbable to cheat using Propy.

In the Social Network Scenario

The AKASHA is a decentralized social media network that defendsuser's freedom of manifestation by providing privacy, access to information and is built on top of the Ethereum. It does it with the assist of code and ensuring that privacy is maintained in every possible way. Yours is a social network where the associate can post content and get paid on Bitcoinmoney. It is for people who love to share their knowledge and opinion and still want to get paid for it.

In the Retail Scenario

The Loyyal is a universal reward and loyalty platform that uses modern technologies like as smart contracts and Blockchain. Utilize this technology, multiple industries, brands and another form of organization can form a distinct relationship with customers and create a loyalty and reward system. The OpenBazaar is a free online marketplace that proposal for zero restrictions to their users without no platform fees, and at the same time earn cryptocurrency. The users can create their personal store, sell their items and reach a new audience. The platforms use cryptocurrency as a medium of money. This

means that there is no requirement for banks or credit cards. The platform also proposal forfull customization and peer-to-peer network. This is one of the finest online marketplaces that is powered by Blockchain.

In the Data Management Scenario

Essesntia. one is a data management framework built on top of the Blockchain, and enduea modular decentralized and interoperability. It include of vital components Essences. Essences own their data and are interlinked viaseveral services, whereas the synergies act as the connective tissue of operations such as connecting platforms, resources and so on. Factom is about faith, veracity, and immutability. They are securing world's system with technology that can help protect systems and make sure that the people are lifted out of poverty. By using Blockchain, systems mileage transparency, veracity, completeness, and security. Also, the requirement for a reliable framework that can make veracity a party of the larger landscape. In short, with Factom, it will be easier to build data products and take conclusion based on it. The Factom software is also pluggable to a current system.

Blockchain Misapprehension and Limitation

The following sections are a rapid exploration of [102] various types of Blockchain misapprehension [103] and limitations [104].

Malevolent Users

The Blockchain system can constrain transaction rules and specifications, it cannot constrain a code of conduct. This is troublesome in permissionless Blockchain systems, since users are pseudonymous and there is not a one-to-one mapping between Blockchain nodes and users of the system. PermissionlessBlockchain provide encouragement to motivate users to act fairly in spite of, some may select to act maliciously if that provides greater incentives. The largest problem for malevolent users is getting enough power to cause destruction. The malevolent users can be annoyances and create short-term disservice, Blockchain can perform hard forks to combat them. Whether harm done would be reversed would be up to the developers and users of the Blockchain system

Preliminary Stage

Blockchain is a very preliminary stage what it means is, there are not many full proof projects in the current where Blockchain has been used, though being discussed too much. Until now industries and companies are in the process of using the technologies very a small number have been successfully implemented.

Resource Utilization

Blockchain technology has enabled a worldwide network of value where every transaction is substantiated and the Blockchain is kept in synch amongst a multitude of users. For Blockchain system utilizing proof of work, this means there is a huge number of users churning away processing time and consuming a lot of electricity [105]. A proof of work method is a solving a problem for hard to create, easy to verify proofs, it requires valuable resource usage. Moreover, strain on resources occurs whenever a new full node is created the node must get most of our all the Blockchain data. This process uses a lot of network bandwidth. Blockchains are frequently compared to databases, and while they both store information, Blockchain have limits on the amount of data that can be stored and are not meant to be a usual storage medium. In order to swiftly calculate hashes on transactions and distribute transactions amongst the network, transactions essential to be relatively small.

Less Number of Available Technical Talent

There are not many developers who develop software for Blockchain, which is animpediment for the people to use Blockchain as a technology in the real world.

Blockchain Control

A common misapprehension is that permissionlessBlockchain are systems without control and ownership. The phrase "no one controls a Blockchain" is frequently yell in spite of, while no user, government, or country controls a Blockchain, there is still a group of core developers who are in charge of the system's development. These developers may act in the attention of the community onhuge, but they still maintain some level of control [106].

Time to Process

In view of the fact that, the transactions necessity to be validated across the thousands of nodes or network on which the Blockchain is based, it becomes a time consuming process, and might be not appropriate for every circumstance.

No Trust

Another common misapprehension comes from people hearing that there is no faithful thirdparty in a Blockchain and assuming Blockchain systems are "waggly" environments. While there are no faithful third party certifying transactions on permissionlessBlockchain systems, there is still a great deal of trust needed to work within a Blockchain system. There is faith that most users of the Blockchain are not colluding in confidential. If a single group or individual can control more than 50 percent of all block creation power, it is practicable to unsettle a permissionlessBlockchain system. Although, commonly obtaining the essential computational power is prohibitively costly.

No Correction and Alteration

All the transaction that takes place in a Blockchain are not correct so nobody gets to know what is the data which is stored in a distinctive block.

Private and Public Key Infrastructure and Identity

This is not the instance, as thereis not a one-to-one relationship of private key pairs to users in other words a user can have multiple private keys, nor is there a one-to-one relationship between Blockchain addresses and public keys in other words multiple addresses can be derived from a single public key. The nodes on the BitcoinBlockchain validate transactions before they are added to a block and afterward incorporated into the Blockchain. One situation of this validation needs the user that initiated the transaction to sign the transaction with a private key. Blockchain nodes calibrate the signature to prove the user does in fact own the Bitcoin value being transferred. The digital signatures are frequently used to demonstrate identity in

the cybersecurity world, and this can lead to uncertaintyabout the potential application of a Blockchain to identity management. A Blockchain transaction signature investigation process links transactions to the owners of private keys, but endues no vantage for associating real-world identities with these owners. In some instance, it is presumable to connect real-world identities with private keys, unless these connections are made via processes outside, and not clearly supported by, the Blockchain.

Bitcoin is the Not Known Name

This means the identity of a person is not invisible. The address of the bitcoin becomes the identity and can be effortlessly accessed in open public Blockchain, and it is a stable record, this is also a fact, therefore if a person wants to interchange the bitcoin for fiat currency he requirement to do a certain paperwork known as KYC (know your customer) and the identity of a person in expose.

Transfer of Burden of Credential Storage to Users

Since Blockchain are not centralized, there is no natural central place for user key handling. Users must handle their own private keys, meaning if one is missing, anything related to that private key is missing such as digital assets. There is no "fail to remember my password" or "rescue my account" characteristic of Blockchain systems.

Lack of awareness

As technology is not much used so there is very low consciousness among people. Which brings the last limitation.

CONCLUSION

The technology that has the most influence on our lifestyles in the last decade is Blockchain. Blockchain at the latest introduced and revolutionizing the digital world, bringing a new perspective to elasticity, security and efficiency of systems. Blockchain is a new technology, based on hashing, as it is used at present, is a tamper-resistant database of transactions consistent across a huge number of nodes. Blockchain is a decentralized ledger used to securely exchange digital currency, transactions and perform deals. In Blockchain every member of the network has access to the latest copy of the encrypted ledger so that they can validate a new transaction. For Blockchain technology to transmutation industries and quotidian lives of people there is a lot of technological development still to be made. It proposesa secure way to exchange any kind of service, good, and transaction. Industrial growth,growing depends on trusted partnerships, but growing regulation, fraud and cybercrime are impeding expanded. In this paper, we are concerned with analyzing Blockchain architecture and attacks cases on Blockchain systems, focusing on their security enhancements in Blockchain. It attempts to highlight role of Blockchain in shaping the future of manufacturing, banking and industrial, healthcare, financial services, Government and tourism and transport. Last but not least, we are also explaining the forking in Blockchain, limitations and categorization in Blockchain.

References

1. ScienceDaily. Big data, for better or worse: 90% of world's data generated over last two years. 2013.
2. https://www.ibm.com/blogs/insights-on business/consumer -products/2-5-quintillion-bytes-of-data-created-every day how does-cpg-retail-manage-it/
3. Yusuf Perwej, "An Experiential Study of the Big Data," for published in the International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Vol. 4, No. 1, page 14-25, March 2017, DOI:10.12691/iteces-4-1-3.
4. Nikhat Akhtar, FirojParwej, Yusuf Perwej, "A Perusal Of Big Data Classification And Hadoop Technology," International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Vol. 4, No. 1, page 26-38, May 2017, DOI: 10.12691/iteces-4-1-4.
5. K Schwab, A Marcus, JO Oyola, W Hoffman, and M Luzi. Personal data: The emergence of a new asset class. In An Initiative of the WorldEconomic Forum, 2011.
6. Yves-Alexandre de Montjoye, ErezShmueli, Samuel S Wang, and Alex Sandy Pentland. openpds: Protecting the privacy of metadata through safeanswers. PloS one, 9(7):e98790, 2014.
7. Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutorials 18, 2084–2123 (2016)
8. Yusuf Perwej, "A Pervasive Review of Blockchain Technology and Its Potential Applications", Open Science Journal of Electrical and Electronic Engineering (OSJEEE), New York, USA, Volume 5, No. 4, PP 30-43, October, 2018, www.openscienceonline.com.
9. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE Symposium on Security and Privacy, pp. 839–858 (2016)
10. A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, \Is bitcoin a decentralized currency?," IEEE Security Privacy, vol. 12, pp. 54{60, May 2014.
11. Q. Lin, P. Chang, G. Chen, B. C. Ooi, K.-L. Tan, and Z. Wang. Towards a non-2pc transaction management in distrubted database systems.In SIGMOD, 2016.
12. A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun,\ Tampering with the delivery of blocks and transactions in bitcoin," in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Com- munications Security (CCS'15), pp. 692{705, New York, NY, USA, 2015.
13. A. Thomson, T. Diamond, S. chunWeng, K. Ren, P. Shao, and D. J. Abadi. Calvin: fast distributed transaction for partitioned database systems. In SIGMOD, 2012.
14. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, \Blockchain contract: Securing a blockchain applied to smart contracts," in IEEE International Conference on Consumer Electronics (ICCE'16), pp. 467{468, Jan. 2016.

15. Condos, J., Sorrell, W. H., and Donegan, S. L., "Blockchain Technology: Opportunities and Risks", 2016.
16. Glaser, F., and Bezzenberger, L. 2015. "Beyond Cryptocurrencies - a Taxonomy of Decentralized Consensus," Proceedings of the 23rd European Conference on Information Systems (ECIS 2015), Münster, Germany.
17. Tapscott, D., and Tapscott, A. 2016. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World. New York, NY: Penguin Random House.
18. Harvard Business Review. 2017. "Blockchain - What You Need to Know." HBR Ideacast, from https://hbr.org/ideacast/2017/06/blockchain-what-you-need-to-know.html
19. Nasdaq. 2016. "Building on the Blockchain - Nasdaq's Vision of Innovation." Retrieved 23.02.2018, from http://business.nasdaq.com/Docs/Blockchain%20Report%20March%202016_tcm5044-26461.pdf
20. Bogart, S., and Rice, K. 2015. "The Blockchain Report: Welcome to the Internet of Value." Retrieved 23.02.2018,
21. Walport, M. 2015. "Distributed Ledger Technology: Beyond Block Chain." Retrieved 23.02.2018,
22. Nakamoto, S. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." Retrieved 23.02.2018, from https://bitcoin.org/bitcoin.pdf
23. Arthur Gervais, Hubert Ritzdorf, Ghassan O Karame, and SrdjanCapkun.Tampering with the delivery of blocks and transactions in bitcoin. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 692–705. ACM, 2015.
24. Nasdaq. 2016. "Building on the Blockchain - Nasdaq's Vision of Innovation." Retrieved 23.02.2018, from http://business.nasdaq.com/Docs/Blockchain%20Report%20March%202016_tcm5044-26461.pdf
25. Yonatan Sompolinsky and Aviv Zohar. Secure high-rate transaction processing in bitcoin. In Financial Cryptography and Data Security, pages 507–527. Springer, 2015.
26. Puschmann, T. 2017. "Fintech," Business Information Systems Engineering (BISE) (59:1), pp. 69-76.
27. Mougayar, W. 2016. The Business Blockchain : Promise, Practice, and Application of the Next Internet Technology. Hoboken, New Jersey: Wiley.
28. Quantum Mechanic. Proof of stake. Available from: https:// bitcointalk.org/index.php?topic=27787.0.
29. M. Milutinovic, W. He, H. Wu, M. Kanwal, "Proof of Luck: an Efficient Blockchain Consensus Protocol", *Proc. 1st Workshop on System Software for Trusted Execution SysTEX '16*, 2016.
30. Yves-Alexandre de Montjoye, C´esarA Hidalgo, Michel Verleysen, and Vincent D Blondel. Unique in the crowd: The privacy bounds of human mobility. Scientific reports, 3, 2013.
31. Latanya Sweeney. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-BasedSystems, 10(05):557–570, 2002.
32. Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and MuthuramakrishnanVenkitasubramaniam.l-diversity: Privacy beyond kanonymity.ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1):3, 2007.
33. Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. t-closeness:Privacy beyond k-anonymity and l-diversity. In ICDE, volume 7, pages106–115, 2007.
34. M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications, Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing, ACM Press, pp 33-43, 1989.
35. X. YI, "Hash function based on chaotic tent maps", *IEEE transactions on circuits and systems- II: Express briefs*, vol. 52, pp. 354-357, 2005.
36. K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, R. Wattenhofer, "On scaling decentralized blockchains", *3rd Workshop on Bitcoin Research Barbados: BITCOIN*, 2016.
37. F. M. Benčić, I. P. Žarko, *Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph*, 2018, http://arxiv.org/abs/1804.10013.
38. Sean O'Melia, Adam J. Elbirt, "Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions" in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, IEEE, vol. 18, no. 11, pp. 1505-1518, Nov. 2010.
39. J. Katz, "Public-key cryptography" in Handbook of Information and Communication Security, Springer, pp. 21-34, 2010
40. R. Gennaro, S. Goldfeder, A. Narayanan, "Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security", *International Conference on Applied Cryptography and Network Security*, vol. 19, pp. 156-174, 2016 Jun.
41. J. A. Garay, A. Kiayias and N. Leonardos, The bitcoin backbone protocol: Analysis and applications., EUROCRYPT(2), 9057 (2015), 281-310.
42. M. Swan, "Blockchain thinking: The brain as a dac (decentralized autonomous organization) [C]", *Texas Bitcoin Conference*, pp. 27-29, 2015.
43. M. Ali, J. C. Nelson, R. Shea, M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains", *2016 USENIX Annual Technical Conference USENIX ATC*, pp. 181-194, 2016, June 22–24, 2016, 2016.
44. Bahsoun, J.P., Guerraoui, R., and Shoker, A., "Making BFT Protocols Really Adaptive," 2015 IEEE International Parallel and Distributed Processing Symposium, Hyderabad, India, pp. 904-913, 2015.
45. Wong, J. and Kar, I., "Everything you need to know about the Ethereum hard fork", Quartz Media, July 18, 2016.

46. Masashi S., Shin'ichiro M., "Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography", International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July-3 Aug. 2017.
47. National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 202, SHA-3 Standard: Permutation- Based Hash and Extendable-Output Functions, August 2015.
48. Ben Sasson Eli, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, EranTromer, MadarsVirza, "Zerocash: Decentralized anonymous payments from bitcoin", *Security and Privacy (SP) 2014 IEEE Symposium on*, pp. 459-474, 2014.
49. F. Tschorsch and B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Communications Surveys & Tutorials, 18 (2016), 2084{2123.
50. X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems, (2017),
51. X. Liang, J. Zhao, S. Shetty and D. Li, Towards data assurance and resilience in iot using blockchain, in Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE, IEEE, 2017, 261{266.
52. Ryan H., Amir H., Aniket K.," Blockchain Access Privacy: Challenges and Directions ",IEEE Security & Privacy , Volume: 16 , Issue: 4 , PP 38 - 45 , August 2018.
53. L. Zhang, Z. Cai and X. Wang, Fakemask: a novel privacy preserving approach for smartphones, IEEE Transactions on Network and Service Management, 13 (2016), 335{348.
54. G. Zyskind, O. Nathan *et al*., Decentralizing privacy: Using blockchain to protect personal data, in Security and Privacy Workshops (SPW), 2015 IEEE, IEEE, 2015, 180-184.
55. Xiwei X., Ingo W., Mark S., Liming Z., Jan B., Len B., Cesare P., "A Taxonomy of Blockchain-Based Systems for Architecture Design ", 2017 IEEE International Conference on Software Architecture (ICSA), Sweden, April 2017.
56. F. Tschorsch, B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies", *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 464, 2016.
57. [57] Till N., Hannes H.," Network Layer Aspects of Permissionless Blockchains", IEEE Communications Surveys & Tutorials, 06 September 2018, DOI: 10.1109/COMST.2018.2852480
58. Xinping M., Qingzhong L., Lei L., Lizhen C.,"A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size", IEEE Trustcom/Big DataSE/ISPA, Tianjin, China, Aug. 2016.
59. Xiangfu Z., Zhongyu C., Xin C., Yanxia W., Changbing T.," The DAO attack paradoxes in propositional logic",4th International Conference on Systems and Informatics (ICSAI), Hangzhou, China, Nov. 2017.
60. S. Solat, M. Potop-Butucaru, Zeroblock: Preventing selfish mining in bitcoin, Ph.D. thesis, University of Paris (2016).
61. N. T. Courtois, L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency", *arXiv preprint arXiv:1402.1718*, 2014.
62. Muhammet B., ZahitZiya G.," Detection of phishing attacks ",6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, March 2018.
63. Egele, Manuel *et al*. "A survey on automated dynamic malware-analysis techniques and tools. " ACM Computing Surveys (CSUR) 44. pp2-6, 2012.
64. Xiaogang W., JunzhouL., Ming Y., Zhen L. ," A novel flow multiplication attack against Tor ",13th International Conference on Computer Supported Cooperative Work in Design, Santiago, Chile, April 2009.
65. M. Apostolaki, A. Zohar, L. Vanbever, Hijacking bitcoin: Routing attacks on cryptocurrencies, in: IEEE Symposium on Security and Privacy, 2017, pp. 375-392.
66. D. Secure Works, BGP hijacking for cryptocurrency profit (2014).
67. P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in Security and Privacy (SP), 2012 IEEE Symposium on, pp. 523-537.
68. ShayanE., AndreasL.,TroyM.,Jeremy C.," A First Look at Browser-Based Cryptojacking", IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, April 2018 DOI: 10.1109/EuroSPW.2018.00014
69. Eric A., MohamedK., VincentN., Rim A.," An Automated Approach to Generate Web Applications Attack Scenarios", Sixth Latin-American Symposium on Dependable Computing, Rio de Janeiro, Brazil, April 2013,DOI**:** 10.1109/LADC.2013.22
70. D. Vishwakarma, C.E.V Madhavan, "Efficient dictionary for salted password analysis", Electronics Computing and Communication Technologies (IEEE CONECCT) 2014 IEEE International Conference, Jan 2014.
71. Daniel G.,StefanieR.,Thorsten S.,Neeraj S.," Mitigating Eclipse attacks in Peer-To-Peer networks", IEEE Conference on Communications and Network Security, San Francisco, CA, USA, Oct. 2014, DOI**:**10.1109/CNS.2014.6997509
72. A. Singh, T. Ngan, P. Druschel, D. S. Wallach, Eclipse attacks on overlay networks: Threats and defenses, in: 25th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 2006.
73. E. Heilman, A. Kendler, A. Zohar, S. Goldberg, Eclipse attacks on bitcoin's peer-to-peer network, in: 24th USENIX Security Symposium, 2015, pp. 129-144.
74. Paul c. Hershey, Charles B. Silio, "Procedure for detection of and response to Distributed Denial of Service Cyber-attack on complex enterprise systems", IEEE, 2012

75. C. Natoli, V. Gramoli, The balance attack against proof-of-work blockchains: The r3 testbed as an example, in: arXiv preprint:1612.09426, 2016
76. L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security , 2016, pp. 17–30.
77. M.-H. Chiu, K.-P. Yang, R. Meyer, T. Kidder, "Analysis of a man-in-the-middle experiment with Wireshark", *Proc. Int. Conf. Secur. Manage. (SAM'11)*, pp. 461-464, 2011.
78. X. Bai, L. Hu, Z. Song, F. Chen, K. Zhao, "Defense against DNS man-in-the-middle spoofing" in Web Information Systems and Mining, New York, NY, USA:Springer, pp. 312-319, 2011
79. A. Kiayias and G. Panagiotakos. On Trees, Chains and Fast Transactions in the Blockchain, 2016. http://eprint.iacr.org/2016/545
80. A. Chakrabarti, G. Manimaran, "A Scalable Method for Router Attack Detection and Location in Link State Routing", *DCNL Tech. Report*, Oct 2002.
81. Daniel G.,Thaier H.,"Detection and prevention of crypto-ransomware",IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON),New York City, NY, USA,Oct. 2017, DOI: 10.1109/UEMCON.2017.8249052
82. L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, A. Panconesi, "SoK: The evolution of Sybil defense via social networks", *Proc. IEEE Symp*, 2013.
83. L. Shi, S. Yu, W. Lou, Y. T. Hou, "SybilShield: An agent aided social network-based Sybil defense among multiple communities", Proc. IEEE INFOCOM, 2013.
84. D. Faria, D. Cheriton, "Detecting identity-based attacks in wireless networks using signal prints", *Proc. ACM WiSe*, pp. 43-52, 2006-Sep.
85. G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in Proceedings of the 2012 ACM Conference on Computer and Communications Security, ser. CCS '12. New York, NY, USA: ACM, 2012, pp. 906–917.
86. Hyunjae L., MyungJae S., KyeongSeon K.,Yeongeun K., Joongheon K., "Recipient-Oriented Transaction for Preventing Double Spending Attacks in Private Blockchain",15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Hong Kong, China, June 2018, DOI**:** 10.1109/SAHCN.2018.8397151
87. G. Zyskind, O. Nathan *et al*., "Decentralizing privacy: Using blockchain to protect personal data", *Security and Privacy Workshops (SPW) 2015 IEEE*, pp. 180-184, 2015.
88. L. Luu, Y. Velner, J. Teutsch, P. Saxena, Smart pool: Practical decentralized pooled mining, in: USENIX Security Symposium, 2017.
89. E. community, Official go implementation of the ethereum protocol (2017).
90. Kejiao L., Hui L., Hanxu H., Kedan L., Yongle C., "Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain", IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/Smart City/DSS), Bangkok, Thailand, Dec. 2017, DOI**:**10.1109/HPCC-SmartCity-DSS. 2017.61
91. L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: The ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254-269.
92. L. Luu, D. Chu, H. Olickel, P. Saxena, A. Hobor, Oyente: An analysis tool for smart contracts (2016).
93. RyosukeA.,HirokiW.,Shigenori O.,Shigeru F.,Atsushi N.,"Storage Protocol for Securing Blockchain Transparency",IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC),Tokyo, Japan, July 2018, **DOI:**10.1109/COMPSAC.2018.10298
94. G. Zyskind, O. Nathan, A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," IEEE Symposium on Security and Privacy Workshops, pp. 180 - 184, 2015.
95. A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: IEEE Symposium on Security and Privacy, 2016, pp. 839-858.
96. T. Jin, X. Zhang, Y. Liu, K. Lei, "BlockNDN: A bitcoin blockchain decentralized system over named data networking", *2017 International Conference on Ubiquitous and Future Networks (ICUFN)*, Jul. 2017.
97. F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town crier: An authenticated data feed for smart contracts, in: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 270-282.
98. Intel Corporation.Intel® Software Guard Extensions Programming Reference , 329298-002us edition, 2014
99. Fabio A.,IoannisC., Andrea V.," The role of blockchain and IoT in recruiting participants for digital clinical trials", 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, Sept. 2017, DOI: 10.23919/SOFTCOM.2017.8115590
100. Frank H.,Simone W., Eyal R.,Moritz Böhmecke S.,"The immutability concept of blockchains and benefits of early standardization", ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), Nanjing, China,Nov. 2017, DOI: 10.23919/ITU-WT.2017.8247004
101. Roman Beck, "Beyond Bitcoin: The Rise of Blockchain World", Computer, Volume 51, Issue 2,Page(s):54 – 58, IEEE Computer Society, February 2018, DOI**:**10.1109/MC.2018.1451660
102. T.D. Smith," The blockchain litmus test", IEEE International Conference on Big Data (Big Data), Boston, MA, USA, Dec. 2017, DOI**:**10.1109/BigData.2017.8258183
103. Valentina G., FabrizioL., ClaudioD., Chiara P., Víctor S. ,"To Blockchain or Not to Blockchain: That Is the Question", IT Professional, Volume 20, Issue 2, Page(s):62 -74, IEEE Computer Society, April 2018 DOI**:**10.1109/MITP.2018.021921652

104. Sin K. L., XiweiX., Yin K. C., Qinghua L., "Evaluating Suitability of Applying Blockchain",22nd International Conference on Engineering of Complex Computer Systems (ICECCS), Fukuoka, Japan, Nov. 2017 DOI**:**10.1109/ICECCS.2017.26
105. Bitcoin blockchain size reaches 100 GB, Coinfox, December 19, 2016.
106. Narayanan, A., "Analyzing the 2013 Bitcoin fork: centralized decision-making saved the day," MultiChain, July 28, 2015.

How to cite this article:

Yusuf Perwej., Nikhat Akhtar and Firoj Parwej.2018, A Technological Perspective of Blockchain Security. *Int J Recent Sci Res.* 9(11), pp. 29472-29493. DOI: http://dx.doi.org/10.24327/ijrsr.2018.0911.2869

****