Blockchain Security/Blockchain Privacy Preserving

*Survey paper on Blockchain, it's security and privacy

Arsalan Shahid Baig - 1820182070
Computer Science And Technology
Internet Of Things, Security And Privacy

***Abstract*—Blockchain emerged as a decentralized technology allowing any kind of data that can be secured and stored without any kind of authority to control it. As the trust is distributed equally between everyone, security and privacy is one of the main aspect of blockchain.**

***Keywords*—** B lockchain, Decentralized, Security, Privacy.

I. Introduction

Block chain is a distributed ledger technology which is based on peer–to–peer (P2P) topology, it allows large amounts of data to be stored on thousands of servers around the world at the same time it lets everyone can see everyone's entries which makes it difficult for an individual to take control of it. Virtually anything can be tracked and traded on a block chain network.

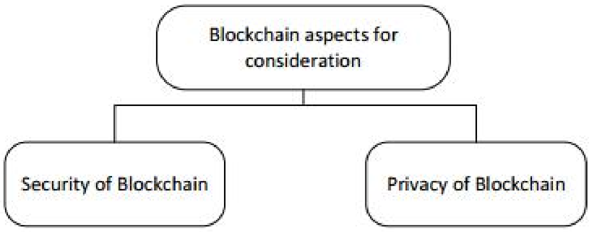

Fig. 1. Above image illustrating the main aspect of blockchain

It is a security management system for the block chain network using different frameworks of cybersecurity, assurance services and reduce the risk against hack attack and assurance services. Blockchain produces data structures with existing security qualities. In most Blockchain technologies the data is structured into the form of blocks, and each block contains a transaction or group of transactions. Each new block connects to all the blocks in a cryptographic chain in such a way that it's nearly impossible to tamper. All transactions within the blocks are validated and verified upon by a consensus mechanism, ensuring that each transaction is true and correct.

II. History

The blockchain type protocol was first proposed by an American cryptographer named David Chaum in his dissertation ”Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups.” in 1982.

In 1991 Stuart Haber and W. Scott Stornetta worked on one of their projects that involved a chain ob blocks where no one could edit the logs of the document including timestamps. In 1992 their system was upgraded and Incorporated with Merkle trees which made the system more efficient and was able to collect more documents in a single block.

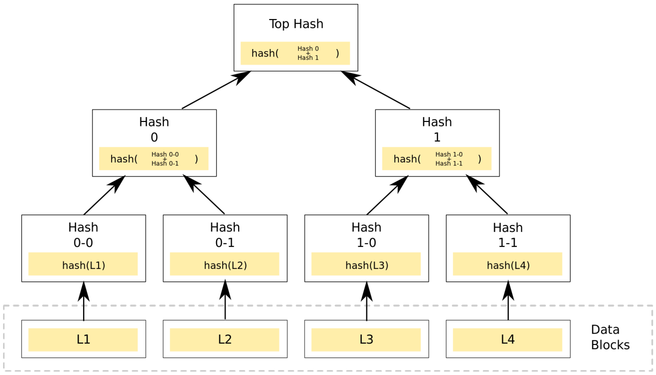

Fig. 2. Merkle Tree

In 2008 Satoshi Nakamoto envisioned the blockchain for the first time from where the technology has evolved into many applications even beyond cryptocurrencies. He released a white paper in 2009 where he provided with details that how the technology is secure and trustable as it is a decentralized technology, meaning no one has an authority and control over another or over the technology in that aspect. The first application of blockchain also came in 2008, which was Bitcoin, which was an electronic Peer-To-Peer system as described by Satoshi Nakamoto in his white paper. He formed the first origin block which was the source block and from that the other blocks were mined, connected with each other forming a large chain of blocks carrying different pieces of information and transactions.

In 2013 Ethereum was borned as the new public blockchain. Ethereum was developed by Vitalik Buterin who was the first contributors of the Bitcoin code base had worked on developing Ethereum which had additional functionalities compared to bitcoin. In Ethereum unlike Bitcoin you could record other assets to such as slogans and contracts this feature expaded the functionalities of ethereum from a cryptocurrency to a platform for developing decentralized applications. Etherium was officially launched in 2015 evlolving in becoming one of the biggest applications of blockchain

In 2015 linux revealed an open-source blockchain project called the Hypeledger which acts as collaborative development platform of distributed ledgers. It mainly uses the blockchain technology to improve the performance and reliablity of the systems to support transictions of businesses world wide.

In 2017 a child company called EOS formed from a parent company called Block.io, the company published a paper where they described the new blockchain protocol powered by the EOS system and acting as the native cryptocurrency. The difference between usual block chain protocols and EOS is that it tries to make the use of real CPUs and GPUs of the provided computer.

III. Supported technologies and Applications

The security and privacy of blockchain technology can be applied on almost every field in IoT. But in some cases it is not necessary because it might have some Scalability issues since it may have a lot of data to handle, like a large number of participating nodes which compromises the block size, especially for the 5th Generation networks that could effect the network usage, network propogation and congestion should be taking under account when blockchain technology is implemented on these kind of system which has a large userbase.

A. *Healthcare*

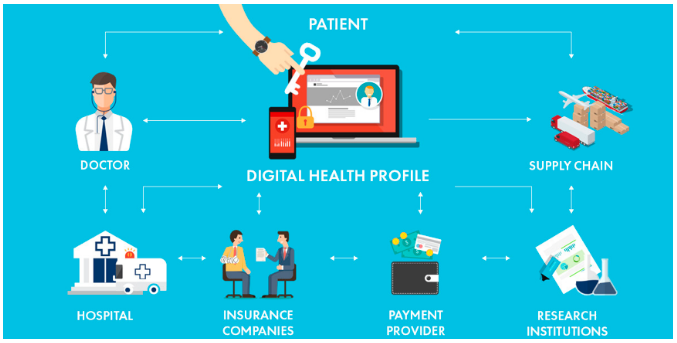

Fig. 3. Blockchain in healthcare

IoT is used in healthcare to allow the healthcare systems to feed the medical data related to the patients, their family, friends and even the healthcare providers. The data stored is called the EMRs (Electronic Medical Records), the stored data is usually confidential and should be kept secure so a model of consortium blockchain is introduced in healthcare. A new healthcare data is created as new block is distributed and instantiated, to maintain the privacy and immutability of the EHRs (Electronic Health Records) Guo et al introduced an attribute based signature scheme, called the Ma-ABS, it uses multiple authorities and uses blokchain technology and can resist attacks involving N-1 currupted authorities collusion. Additionally MA-ABS is unable to forge in suffering an attack involving selective predicate attack So Liang et al made use of the blochain network in the mobile healthcare applications to protect the integrity and auditing further and investigation.

B. *5G Network*

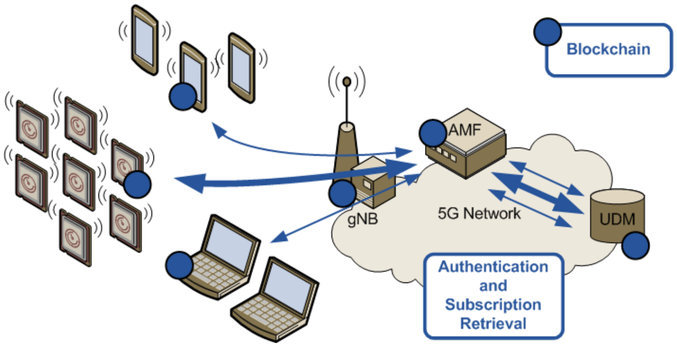

Fig. 4. Blockchain in 5G

The 5G technology enables a society which is fully mobile and connected to billions of objects, this obviously requires security and privacy where the use of blockchain comes in. Fan et al proposed a blockchain based scheme which involves privacy preserving and data sharing. Based on the idea to add blocks to the blockchain, each new block is interconnected to the blockchain by its hash value, the previous hash value can be found from the block header.

There are multiple opportunities for implementing blockchain technology in 5g such as:

- Crowd sourcing: This allows the smaller infrastructure to make out the cellular towers that will be the part of the overall infrastructure of the operator.
- Infrastructure Sharing: Sharing infrastructure is an obvious opportunity in 5G in which the the mobile network operator offers the telecommunication service with cellular tower, which is considered as active sharing.
- International Roaming: Roaming is one of the issues in the telecommunication sector as it involves third parties to settle payment and charges methods so in this, smart contracts are introduced to achieve a blockchain based payment and roaming method in which the consumption usage is tracked.
- Network Slicing: Network slicing is when an instantiating of a physical structure or the network service and capabilities. A blockchain with decentralized storage such as Storj or IPFS can be used to most of the NSB functionalities, smart contract will allow different requestors to negotiate several contracts autonomously and dynamically.
- Management and Authentication of Massive Machine Communicaitons (mMTC) and Ultra Reliable Low Latency Communications (uRLLC): These are the two main pillars of 5G where lots of IoT devices are to be connected with less than 1ms of latency. The incorporation of so many IoT devices gives the opportunity for new services and business models to be offered to the mobile customers in the future. it is estimated that 5G will be managng these IoT devices through trusted and centralized operators.

C. Vehicle Industry

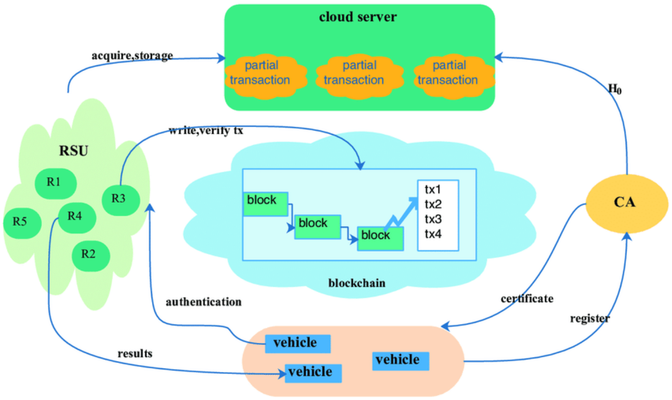

Fig. 5. Blockchain in IoT Vehicles

IoV (Internet of Vehicles) is a rising concept, this allows the integration of the vehicles into the IoT world and in order to establish the communications between vehicles and their networks such as Vehicle to Vehicle, vehicle to road, vehicle to human vehicle to sensor and vice-versa.

Now recently blockchain technology has been tried to apply to the IoV, using the decentralization security model Huang et al proposed an ecosystem model involving blockchain called the LNSC. This model uses elliptic curve cryptography (ECC) to calculate the hash functions of electric vehicles and charging piles. To avoid the location tracking in the vehicles, Dorri et al proposed the decentralized architecture of privacy preserving where the overlay nodes manage blockchain. Additionally the hash of the backup is stored in the blockchain.

Without central manager's administration Lei et al proposed a key management for vehicular communications based ob blockchain. Based on the blockchain structure the authorities are removed and the key transfer processes are authenticated and verified by the security manager network.

Kang et al introduced a peer-to-peer electricity trading system called PETCON, illustrating the operations in detail of the localized peer-to-peer electricity trading. Using the consortium blockchain method the PETCON system can publicly share and audit the records without relying on any kind of third party whether even it is trusted or not.

There is also an issue of forwarding the reliable announcements without leaking the users the user's identity, so Li et al proposed a privacy preserving scheme called the Creditcon which uses the blockchain using an anonymous vehicular announcement aggregation protocol to build a trust in IoV.

A blockchain based reputation system was proposed by Yang et al, which judges the recieved messages whether they are true or false based on the sender's reputation values.

D. Energy

The Internet of Energy provides an innovative way to increase the visibility of nergy consumption in a Smart Grid. Gao et al introduced a monitoring system based on a sovereign blockchain technology on the Smart Grid called the GridMonotiring, for ensuring provenance,transparency and immutability.

GridMonitoring system is based of 4 layers:

1) Registration and authentication layer.
2) Processing and consensus nodes.
3) Smart meter.
4) Data processing on the smart grid network.

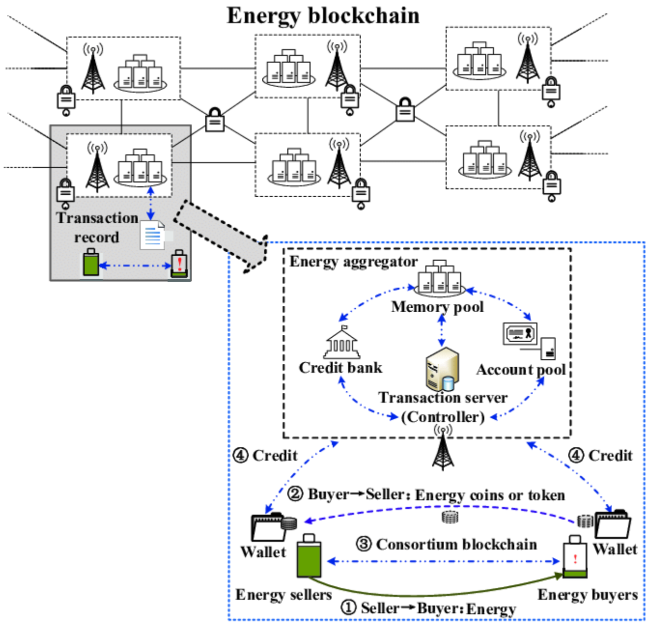

Fig. 6. Blockchain in IoT Energy

Based on the distributed blockchain Liang et al proposed a data protection framework in modern power system, which can fight against data manipulation such as false injection data attacks. To guarantee the accuracy of data, consensus mechanism is used which is implemented by every node and has representative characteristics:

1) Setting of public/private key update frequency.
2) Miner selection.
3) Block generation.
4) Release of meter's memory periodically.

For secure energy trading, li et al introduced energy blockchain, this is based on the Stackelberg game and the consortium blockchain technology. Aitzhan and Svetinovic implemented a private decentralized energy trading system based on tokens for an in decentralized smart grid energy systems.

E. Access Management

For the management for the IoT devices Novo proposed a distributed access control system which uses the blockchain technology. This system's architecture consists of six components:

1) Wireless sensor networks.
2) Agent node.
3) Managers.

4) Blockchain network.
5) Smart contract.
6) Management hubs.

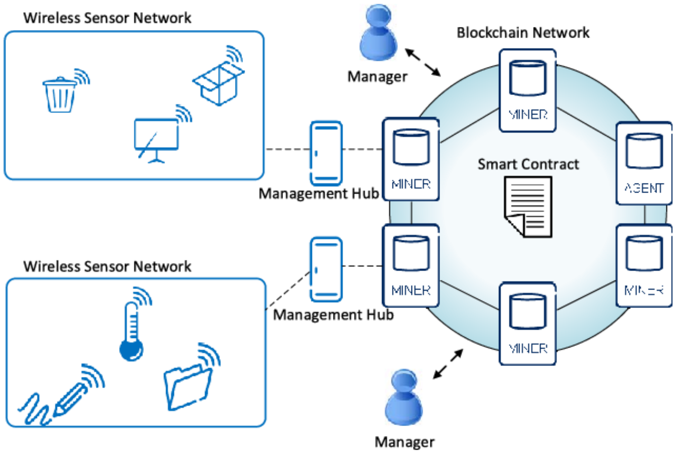

Fig. 7. Blockchain in IoT Access Management

The system introduced can bring some advantages the the access control in IoT such as:

1) Mobility: Used in isolated administrative systems.
2) Co currency: Allows the policies to be modified continuously.
3) Accessibility: ensures that the control rules are available at all times.
4) Scalability: As the devices can be connected through different networks.
5) Lightweight: Can be implemented in wide range of the system and dont have to be modified for it.
6) Transparency: Where the system preserve the location privacy.

F. Cloud Computing

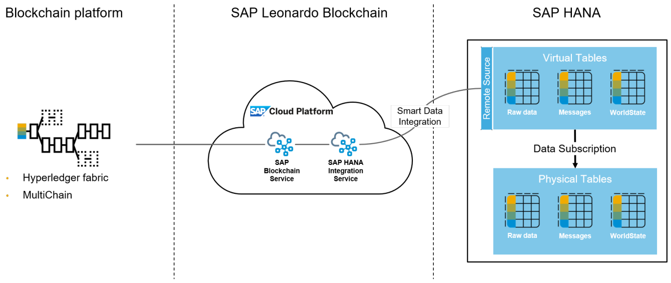

Fig. 8. Blockchain in IoT Access Management

In the world of IoT, billions of of devices upload large amounts of data. Xu et al introduced a blockchain based intelligent resource management system for cloud in order to reduce the total cost of energy consumption. The users use their individual private ID keys to sign a transaction, the lock is rejected when it does not pass verification. So Sharma et al proposed a cloud architecture that uses three of the emerging technologies which are Software Defined Networking (SDN), fog computing and a blockchain technique. The sdn controls the fog node which are used to provide programming interfaces to the network management operators. Blockchain is used to provide reliable, scalable and high availability services. Additionally Xia er al proposed a data sharing system based on blockchain called the MeDshare, used for cloud service providers, this system consists of 4 layers which are:

1) Data query layer.
2) User layer.
3) Provenance and Data structuring layer.
4) Existing database infrastructure layer.

There are many ways to implement the intrusion detection systems (IDS) in the IoT world. That are based on machine learning. To improve the IDSs Alexopoulos et al introduced the idea of making use of blockchain technology to secure the exchange the alerts between the communicating nodes. Modern IDSs must be based on the communication among distributed IDSs and demand the extensive sharing of data aong other entities and the trust system. In order to deal with concerns such as privacy that are raised exchanging data and supress insider attacks, the blockchain technology is applied. So this way the use of third party trust which has a risk of single point failure can be avoided.

IV. Application Scenario - Smart Grid

A. What is a Smart Grid ?

A Smart Grid is an electrical grid that is integrated with two way network which is computerized. In an older traditional grid, the electrical grids sends power in a single direction, from the power plant to offices and home. But a Smart Grid improves the network by providing it with instant feedback on system wide operations, electric use and power interruptions back to the regional power grid operators and electric plant.

Smart grid can use live monitoring to customize and synchronize itself to an optimal state of performance delivering the power evenly even in the peak usage hours.

B. Use of Security and privacy of blockchain in Smart Grid

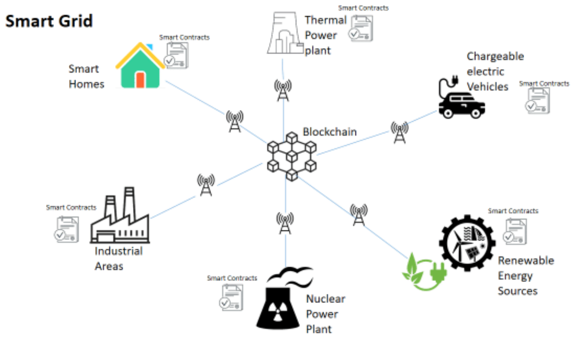

Fig. 9. Blockchain in Smart Grid

By the increasing use of smart grid blockchain has been implemented on smart grid. the applications of blockchain can be divided into different parts of smart grid as follows:

1) Power Generation: The blockchain technology gives the implementing agencies a full knowledge of the overall operations of the power grid live. This helps them develop the dispatching plans that will help them maximize on the profits.
2) Power Distribution and Transmission: Blockchain implementation enables the automation and control systems to have decentralized systems that would minimizes or just eliminates the challenges faced by a centralized system.
3) Power Consumption: The implementation of blockchain would benefit a lot by managing the trading of energy between the consumers and the different energy storage centers as well as electric vehicles.

With the increased use of mirogrid, energy trading is becoming popular in research and industry. The adoption of blockchain in the trading process of energy market helps in reducing the effort required and time. Hence with implementing blockchain peer-to-peer energy trading becomes a much more promising future. In the peer-to-peer trading system, the blocks inside the chain records the units which are generated by the electricity which allows sellers and buyers to make a deal instantly and not be dependent. This gives the buyers the freedom of choices and prices instead of depending on the intermediate seller.

In this platform the focus also goes to the anonymity and privacy of the users, the advantage is that this provides users with the freedom to directly negotiate the process. Luo et al blended the concept of implementing blockchain with the multi agent to form a multi layer(2-layer), based trading system for electricity. The first layer is for the users where they can discuss their pricing issues, the second layer is based on blockchain which provides a secure and trusted platform for fund transactions.

The Blockchain technology is also implemented in the microgrid operations for its possible advantages. A scheduling mechanism based on blockchain technology has been design, the utilization of it provides a platform which can be trusted so that all DERs are secured and trusted. Munsung et al examined to simplify the distribution and control of the DER in the microgrids where the optimal power flow which is decentralized had is for scheduling the mox for DERs. The introduced scheme here can reduce the Peak to Average ratio to give the electrical grid an advantage by benefiting them and smoothing the dips in the load caused by constraints supply. In a new perspective the decentralization of the MVDC (Medium Voltage Direct Current) link control is implemented using blockchain, this control distributes the responsibilities between the grid operators within the energy system.

The smart grid is also implemented in electric vehicles, mainly in the charging of the EVs as it is the primary concern. Because if the Evs are charged uncoordinated it can overwhelm the power grid and cause stress. Hence blockchain technology has been introduced by liu et al to adapt the integration of charging the EV to smart grid. The EVs will use the blockchain technology integration to find the nearest charging station, including the best location and price to charge an EV while also ensuring the security and privacy of all the systems involved.

V. Security and Privacy Issues

Although blockchain is mainly implement to increase the security and preserve the privacy of the networks, blockchain it self has some issues which are listed below:

- 51 percent Attack.
- Phishing and Social engineering
- Back doors in its protocol
- Bugs

But in here we will be discussing one of the main threats to blockchain, which is the 51 Percent Attack. In this attack the attacker can direct the transactions back to him self by printing duplicate blocks on a side branch and refutes what ever is happening in the main chain. However given a solution with intensive resources of the hash function and the issue of recent bitcoins so far this option seems unlikely.

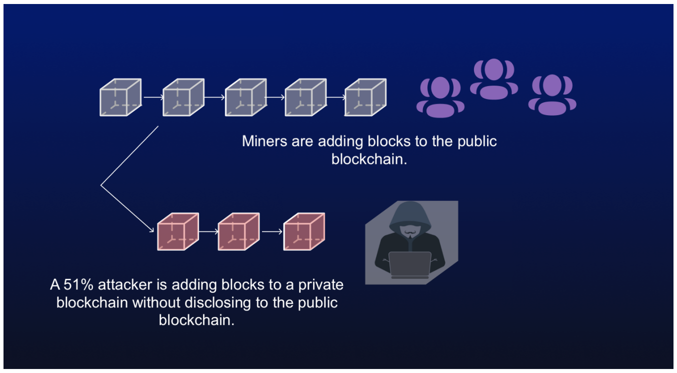
Miners are adding blocks to the public blockchain.
A 51% attacker is adding blocks to a private blockchain without disclosing to the public blockchain.

Fig. 10. Image illustrating 51 Percent Attack

Now lets consider a scenario where a malicious attacker tries to generator a duplicate chain in the blockchain faster than the normal honest users, now that even if he is successful he wouldn't be able to make any changes, like creating coins from air/out of nothing and or stealing coins that none has transferred to him. The nodes can not accept a wrong transaction as a block. So an attacker can only edit on one of his own transactions which he recently made by returning the payment to himself. The time it takes for honest chain and the attacker's chain is called the binomial random walk. To make the event successful the target approach of the honest block should be +1, and the unsuccessful event is to increase by one block in the attacker's chain with a separation of -1. The attacker's ability to catch up in the constrained environment is a bit similar to the Gambler's Ruin problem. The gambler with almost unlimited credit starts the game and can hold unlimited parties involved in it. we can calculate the probability of the attacker overtaking by:

Let p = probability of honest user finding next block;

Let q = probability of attacker finding next block;

qz = probability of attacker winning the race if he is z blocks behind

The equation can be written as:

$$q_z = \left\{ \begin{matrix} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{matrix} \right\}$$

Now lets suppose that p is less than q, the probability decreases at an exponential rate with the increasing number of blocks in which the attacker is behind. Now if he does not manage to get ahead in the beginning his chances of being successfully become small. Now we should also put in consideration that how long the payment process is to make sure that the sender wont be able to change the transaction. Now lets suppose that the attacker who is also a sender, he wants the recipient to believe that the payment process has been carried out but after a moment the attacker returns the payment back to himself. The recipient generates a key and gives the public key to the attacker after signing. This does not give the sender to prepare the block in advance to complete the transaction at the time. Now only when the transaction is sent the dishonest sender can form a duplicate chain containing the duplicate version of the carried out transaction. The receiver waits till the transaction is added t the blockchain and z number of blocks are added after that. He is not aware of what the attacker is doing, but assuming the honest blocks were build on the same rate as average the expected value of the growth of the attacker's block can be found by Poisson distribution:

$$\lambda = z\frac{q}{p}$$

Now to find out the probability in which the attacker can still move on, we use this equation:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \left\{ \begin{matrix} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{matrix} \right\}$$

Or after regrouping:

$$1 - \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

By analyzing the last equation we can pretty much verify the probability decreases exponentially while z is increasing.

VI. Conclusion

The block chain technology can definitely revolutionize the world of IoT. It can be implemented in almost all the applications and can be very important asset for the cyber security department. In conclusion this technology is not ready enough to be implemented in large scale since it can have draw backs which are usually related how much data it can handle and store within it. But as the technologies are developing exponentially, so will the capabilities of the blockchain technology and the current systems where the blockchain can be implemented. And this will happen soon.

References

[1] Ehab Zaghloul; Tongtong Li; Matt W. Mutka; Jian Ren, ”Bitcoin and Blockchain: Security and Privacy”, Date of Publication: 22 June 2020, Link: https://ieeexplore.ieee.org/document/9122595

[2] Mohamed Amine Ferrag; Makhlouf Derdour; Mithun Mukherjee; Member; IEEE, Abdelouahid Derhab; Leandros Maglaras; Senior Member; IEEE; and Helge Janicke, ”Blockchain Technologies for the Internet of Things:Research Issues and Challenges”, Date of Publication: 22 November 2018, Link: https://ieeexplore.ieee.org/document/8543246

[3] Jiewu Leng; Man Zhou; J. Leon Zhao; Yongfeng Huang; Yiyang Bian, ”Blockchain Security: A Survey of Techniques and Research Directions”, Date of Publication: 25 November 2020, Link: https://ieeexplore.ieee.org/document/9271868

[4] Joe Abou Jaoude; Raafat George Saade, ”Blockchain Applications – Usage in Different Domains”, Date of Publication: 01 March 2019, Link: https://ieeexplore.ieee.org/document/8656511