BLOCKCHAIN TECHNOLOGY: ENVISION SMART FUTURE

Anusha Bhallamudi
Illinois Institute of Technology
Chicago, 60616, IL
abhallamudi@hawk.iit.edu

Curie Nandeshwar
Illinois Institute of Technology
Chicago, 60616, IL
cnandeshwar@hawk.iit.edu

Pragya Pramudita
Illinois Institute of Technology
Chicago, 60616, IL
ppramudita@hawk.iit.edu

Shivank Saxena
Illinois Institute of Technology
Chicago, 60616, IL
ssaxena12@hawk.iit.edu

M. Fátima Rojo del Prado
Illinois Institute of Technology
Chicago,60616, IL
mrojodelprado@hawk.iit.edu

ABSTRACT
In today's generation, the seething grasp of advancing technology is no longer a trend seemingly focused on the big areas like the IT industry, luxury items like cars, phones, etc. Thanks to ever the growing need of consumer to have the next best thing, newer ideas and proof of concepts are being showcased to get a taste of what the customer wants next. This trend is also visible in the social networking facet of the IT industry with the rapid increase in the number of apps using virtual currencies, blockchain technology, etc. One such networking site is Steemit, where users are connected in a social network with access to share their views in the form of videos, images, articles, etc. on their social network. Although you may think this one of those sites which is a copy of your popular social networking site, it is very much more different than that. Steemit is one of a kind of social media networking platform which works upon blockchain technology and is making headlines, with just over few years of it release for providing its users cryptocurrencies as rewards for their posts. This unique rewarding system has not only increased their user counts but has strengthened the virtual currencies like bitcoin by providing an alternative to the main currency in terms of security, reliability, transparency and costing. We will in this paper outline the salient features of bitcoin technology with Steemit company as a use case wherein we would explain the challenges faced by Steemit company using blockchain technology while proposing efficient and reliable solutions for the same.

Keywords
Blockchain, Cryptocurrency, Steemit, Steem, Cloud computing, Steemit tokens, Steem power, flags, content, illegal, blockchain, data base, platform, data, articles, publications, ITIL framework, service, consensus algorithm, Inequality algorithm, @cheetah bot, Hardware security model(HSM),

1. INTRODUCTION (Shivank Saxena)
Blockchain is a type of distributed and secure database technology using mathematical functions and codes, used in cryptocurrency which can track and verify each transaction being made within its environment. It is a rapidly advancing technology due to its multiple benefits such as de-centralization of data within the cloud highly safe and secure, more reliable and transparent. "Blocks" on the blockchain are made up of digital pieces of information which are stored on a public network. These blocks store the information related to transactions, ownership of a transaction and differentiating each block from one another. While functioning as a distributed network, multiple people can access, write entries into a record of information, and a community of users can control how the record of information is amended and updated [1]. In doing so, their computers get updated whenever any new block or any new piece of information is added by any user over the user as shown in figure1.

Fig 1. Physical Layout of a social media based on blockchain [6]

Steemit is a social media database company based on blockchain technology which supports community building and social interaction offering bitcoins as the rewards for their users. The fair accounting approach attracts the users and makes it popular among them. It is designed to capture the broad market by providing the pro-rata ownership or payment debt from the venture.

The company value all kinds of capital equally such as time, energy, attention or cash in developing the content or maintaining it and shares the resources only within the organization's community. It is the cooperation between cryptocurrency and social media that gives a powerful advantage in the market. The challenge faced by the company is deriving an algorithm for scoring individual contributions that act as a fair means of assessment of everyone's contribution to the community. In the real world, algorithms must be designed in such a manner that they are resistant to intentional manipulation for profit. Any widespread abuse of the scoring system could cause community members to lose faith in the perceived fairness of the economic system. Many existing social media platforms use one-user, one-vote principle. This makes the rankings prone to Sybil attacks and abuses which can be identified and blocked by the service providers. The people can also manipulate the algorithms of famous social media platforms such as Reddit, Facebook, and Twitter based on web traffic or censorship.

Steem is the fundamental accounting unit on the Steemit platform which acts as a cryptocurrency token. It operates based on the number of votes; one-Steem, one-vote. So according to this scheme, Users who contribute the most to the platform have more scoring which is measured with the help of their Steem account. Furthermore, members are only allowed to vote with Steem when it is committed to a vesting schedule. It is also designed around a relatively simple concept: everyone's meaningful contribution to the community should be recognized for the value it adds. When people are recognized for their meaningful contributions, they continue contributing and the community grows. Any imbalance in the give and take within a community is unsustainable. The challenge is creating a system capable of identifying what contributions are needed and their relative worth in a way that can scale to an unbounded number of people. [2] A proven system for evaluating and rewarding contributions is the free market. The free market can be viewed as a single community where everyone trades with one another and rewards are allocated by profit and loss.

This platform is designed to enable effective micropayments for all kinds of contribution by changing the economic equation. Readers no longer must decide whether they want to pay someone from their own pocket, instead, they can vote content up or down and will use their votes to determine individual rewards. This means that people are given a familiar and widely used interface and no longer face the cognitive, financial, and opportunity costs associated with traditional micropayment and tipping platforms [2].

Functioning of Blockchain

The data is stored by spreading it on the entire network of the blockchain which is parallelly received and computed by every computer on the network. Each of the computers is denoted as a "node" on the digital cryptocurrency network. In order to perform transactions on the blockchain, you need a wallet, a program that allows you to store and exchange your bitcoins. Since only you should be able to spend your bitcoins, each wallet is protected by a special cryptographic method that uses a unique pair of distinct but connected keys: a private and a public key. If a message is encrypted with a specific public key, only the owner of the paired private key can decrypt and read the message. If you encrypt a message with your private key, only the paired public key can decrypt it each node in the network can cross-check that the transaction request is coming by decrypting the message with the public key of a wallet. When a transaction request is encrypted using a wallet private key, a digital signature is generated using the source computer for maintaining the authenticity of the transaction. The digital signature is a string of text resulting from your transaction request and your private key; therefore, it cannot be used for other transactions. If any single character in the request message is changed, the digital signature will change, so no potential attacker can change your transaction requests or alter the amount of bitcoin you are sending. For sending the bitcoin you need to prove an individual need to prove that he/she owns the private key of a specific wallet as needed for encryption. Since the message is only broadcasted after it has been encrypted, therefore the private key it can never be revealed.

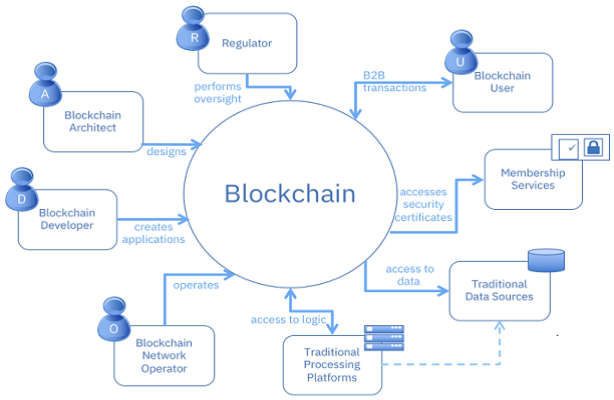

Fig 2. Structure of a Blockchain Network

Hashing is a process of accepting an input string of fixed length and delivering a cryptographic hash value based on mathematical algorithms of fixed 256 bits length. It uses the transactions for converting them into multiple hashes which need to be tracked. The hashes are deterministic in nature which can be quickly computed without causing problems related to previous images.

Steemit is a developing firm which works on all the above concepts of blockchain for the functioning of Steem crypto-currency, Steem dollars, Steem power but still are facing major issues such as improper distribution of the upvotes to earn more Steem rewards and Steem power and illegal data like child abuse or pornography being uploaded by the users. Steemit also underwent security threats due to cyber-attacks which has caused major disruption to their business and reputation. The following paper discusses each problem and in-depth solutions which Steemit should take over to deliver for an error free and reliable website.

2. STEEMIT TECHNICAL ISSUES

2.1 Content Governance (Anusha Bhallamudi)

When the exceptional math of Satoshi Nakamoto gets implemented, it was not so perfect in this real world as our world runs by rules. The limitations of the blockchain creates problems when not governed. Blockchain can complement, supplement and substitute legal enforcement But, inclusion of a proper law and mechanism can also make blockchain the ruler of technical world. [3]. Moreover, the blockchain without effective governance, can be either be counterproductive or excessive dangerous. We should also keep in mind that excessive or premature application of governance may forego opportunities and innovations to leverage technology.

The Steemit is a complicated system with lots of monetary theory and believes in proof of stake rather than proof of work. We believe that centralization and censorship are closely bound and aborts our freedom to express ourselves freely. Therefore, it uses public blockchain technique, which records all transactions and posts on the network and is completely transparent to all the users. The data stored in blockchain is available to all and the software involved is open source and freely available, thus making it effectively decentralized [4]. Thus, the content stored in it is censorship resistance, which means it cannot be tampered by anyone.

The two main problems faced by Steemians regarding governance is unbalanced distribution of Steem power among the users and

debate on transparency regarding development of new code. To properly resolve the above issues, we should first understand three main groups in Steemit network. They are witnesses, Steem developers and Steem holders i.e., users.

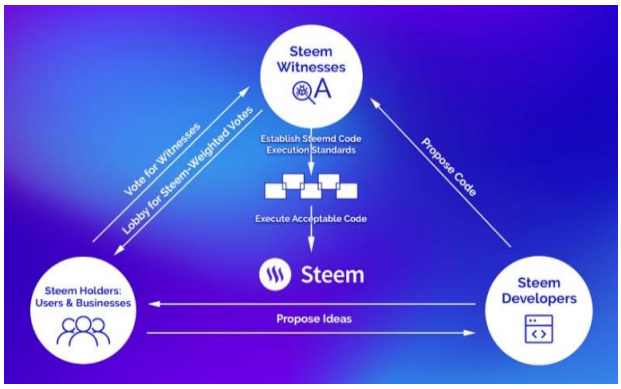

Fig 3. A flow chart depicting relation between different Steemit groups [5].

- **Witnesses:** To use a consensus mechanism called proof of stake, POS. The Steem community elects' witnesses to act as block producers and governance body. The Steemit selects top 21 witnesses to sign the blockchain transactions. Steemit schedules these witnesses to produce block every 3 seconds. Among these witnesses, 20 are selected through approval voting and 1 is selected through time sharing by the witnesses who didn't make it to top 20. Steemit makes sure that these witnesses are shuffled in every round. This gives a fair chance for everyone to be among top 20 whether they are popular or not.

- **Developers:** Steemit has recruited more than 50 excellent set of developers who do the coding part and ensure to make it much better and empowering network so that more Steem users get benefit out of it.

- **Steem users:** These users are people who posts and earn Steem crypto currency for their content and voting Steem powers. The witnesses are chosen among these Steem users.

2.1.1 Service Strategy

The sole purpose of creating Steemit platform is to provide a medium for people to express their thoughts freely. Steemit is a decentralized network where no single individual can control. If control is given to one person or group of persons, when faced with ambiguity they will be incapable of dealing with it properly. As Steemit is a decentralized blockchain, it is censorship resistance. But question here arises, when Steemit is censorship resistant how can we make the public access of code more transparent?

To solve the above issue, we have made a strategy of involving all the Steemit members to be part of deciding phase through voting. That will help us to establish a governing body who will decide standards for enhancing and authorizing the code. The top 21 witnesses who are selected through voting, will act as governing body. These 21 witnesses are also shuffled periodically, hence maintaining the fact that control does not lie in the hands of few people permanently. This will follow the principle of Blockchain that it is decentralized.

The other problem faced by Steemit users is unequal distribution of Steem power among whales (founders) and other users. This power enables whales to influence the voting. When a person has more Steem power he has more voting power. The whales and users with more voting power are misusing them with either upvoting their favorite content writers more than once or down voting other authors. This theory is called as *negative- voting theory.* With the use of negative voting or down voting these users can make a post go down from trending list of articles. This will affect the reward earnings of the authors and satisfy their *crab mentality* of whales [7].

Fig 4. Inequality in Steem currency and power distribution [8].

A lot of informative posts or articles go unnoticed and unrewarded. If only one or two whales, follow someone and vote their posts they will be consistently awarded hundreds of dollars and Steem power. On the other hand, upvotes from other users are worth very little. We will implement divide and conquer strategy to solve the issue of power of inequality. The strategy involves restricting the usage of whale's upvotes to certain level on each post they want to upvote. This will create chance for other users to use their Steem power for upvoting genuine and quality content. This strategy will help whales to maintain their wealth and other users to gain more rewards as well as Steem power. This strategy will promote Steemit platform as new users will gain popularity through their quality posts.

2.1.2 Service Design

To implement desired strategy to resolve censorship and inequality issues, we will utilize 4 Ps of ITIL Service design i.e. People, Process, Partners and Products in our strategic plan. In Steemit Service Design the four Ps will include following parameters:

- **People:** We will appoint separate teams for each issue management. The consensus issue will be handled by team of 21 witnesses and 5 developers. The inequality issue will be handled by team A of 30 highly qualified blockchain developers.

- **Process:** There will be two algorithms which will be developed by the coders for each issue. For the consensus issue witnesses will provide some standard protocols for development and authorization of new code. Coders will implement various algorithms for establishing flags and downvoting procedures which will be used by different Steemit users. For inequality issue the Team B developers will be further equally divided into two groups Tier 1 and Tier 2. Tier 1 will use different

analytical tools to research on standards, Steem power and wealth acquired by different users including whales and other users in Steemit community. Tier 2 will implement this research in writing down new code and algorithms.

- **Partners:** Steemit partners Block-trade and *Gopax*, who are responsible for distributing wealth in the form cryptocurrency to Steemit users. This distribution is based on newly developed codes.

- **Products:** Bots used like @cheetah, reputation rewards, curator rewards etc. will be more enhanced technically by the 15 blockchain developers from the remaining set of 50 developers recruited. The last 15 developers will be working under Service desk who will take care of daily tokens or feedbacks provided by Steemit users.

2.1.3 Service Transition

In the service transition stage, we will take care of transition planning and support. We must effectively manage the current scenarios without affecting the platform and must implement new code and algorithms.

The new Consensus algorithm will be set up by 21 witnesses who will set up quality standards for enhancement of code. These standards will be recorded in public ledger in the form of cryptographically signed contracts. When members of community agree on implementation of this algorithm than it is established as valid protocol. All the suggested standards will be posted by the witness on their panels. These posts will then be voted by the 21 witnesses to select the effective and reliable set of agreed standards. All the witnesses must establish the standards and sign the blocks of transactions. Once the signing of the block of transactions starts each witness must sign within 3 secs of the previous block created.

In Inequality algorithm voting power will be multiplied by each Steemit user's vesting Steem power. There will be fixed amount of vesting power each user can use. Each user can use only certain amount of Steem power to upvote the first post. The second vote will utilize less Steem power than the first one and so on. It will take 3 days for a user to regain their complete voting power. A single user cannot vote same post more than once. This will disable whales to upvote only their favorite content writers and provide equality for other authors.

2.1.4 Service Operation

The different management teams set up in Service designing phase will effectively handle smooth implementation of the newly developed algorithms. Four main departments will be responsible to handle service operations smoothly:

- **Witnesses department**: The top 21 witnesses elected by the Steemit users will act as gatekeepers and governing body of Steemit network. They will be responsible for signing of blockchain transactions and setting up standards for content writing too. The witness's department will also be responsible for the final authorization of codes developed by the developers.

- **Team A Developers:** The Team-A consists of 5 blockchain developers who will work under top 21 witnesses and create algorithms and codes based on standards provided by them**.**

- **Team B Developer:** The department of 30 highly qualified blockchain developers are further divided into two departments who will resolve incidents raised regarding inequality issues.

- **Service Desk:** It comprises of 15 developers who act as point of contact for Steemit users to resolve their issues regarding, Steem power, Steem dollar, or any other technical issues. They will take these tokens from the users through calls, emails or chat bots. Every minute incident token has a timeframe of 20 minutes to get resolved. If an incident takes more than 20 minutes, the Steemit user is provided the reason for delay and issue must get resolved within 24 hours.

A knowledge base is also created which collectively handled by the developers and witnesses to refer for further enhancements or handling incidents. The FAQ section in the Steemit network is updated timely based on information recorded in knowledge base.

2.1.5 Continual Support

In continual Service support our team ensures that the service design implemented and executed by us is enhanced and improved time to time. The service desk will work on user's feedback and guidance of Steemit witnesses to ensure continual support to Steemit Network. We must aim more on obtaining return and value of investment.

The change in real world governance will directly or indirectly affect the governance of blockchain technology too, so we must be ever ready to adapt the changes and maintain the efficiency of our network. With the ever-growing technology, new forms of blockchain technology are emerging in the digital world. To enhance our Steemit network we should implement these new technologies and provide excellent experience to our Steemit users.

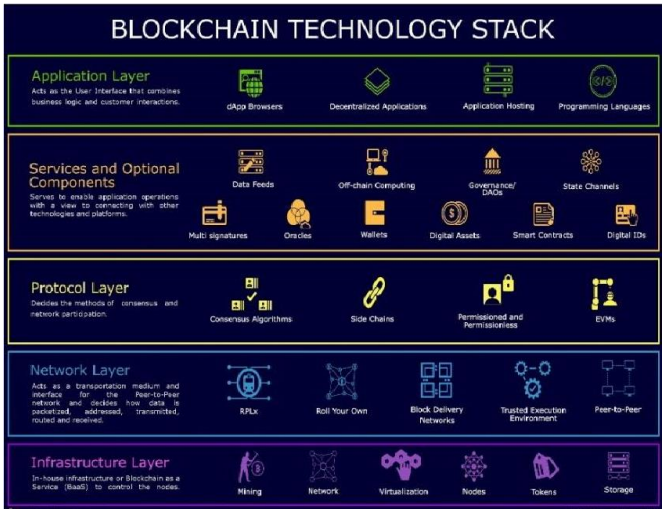

Fig 5. Blockchain Technology stacks [9]

Our developers will be trained on these technologies and interfaces for developing enhanced versions of codes and algorithms as represented below in the figure 5. This will provide a better form of governance in relatively decentralized network.

2.2 Security Concerns (Curie Nandeshwar and Pragya Pramudita)

It is essential for any business to meet the customer's expectation and demands to gain maximum business value. Security and privacy of user's data is the foremost and most important factor to be considered to ace in the long run. Blockchain being well-known technology to provide the security and privacy but still, have encountered few loopholes. Steemit which relies on cryptocurrencies and Steem wallet has faced a similar issue where the hackers have blown the Steemit security with cyber-attack. Therefore, there is a need to enhance the security feature of Steemit to avoid further cyber-attacks which would aid the growth of the business and gaining customer trust.

Most blockchain users remain susceptible to privacy attacks by hackers. Steemit was subjected to a cyber-attack sometimes back. In the attack, 260 accounts were compromised, and 6002347.00₹ worth of Steem Dollars and Steem had been stolen. There had been many instances where security of digital wallet was compromised when hacked. Granting that the features of blockchain technology guarantee more reliable and expedient services, it is important to consider the security and privacy issues and challenges behind the innovative technology. In this paper, we try to conduct a comprehensive survey on the blockchain technology by discussing its structure to different consensus algorithms as well as the challenges and opportunities from the perspective of security and privacy of data in blockchains.

2.2.1 Service Strategy

Protection of the block of data, transaction or information against the innumerable internal or peripheral, malicious or unintended threats is the main purpose of blockchain security. Detecting the threats, preventing them, giving a response to the threats are few of the protection measures typically looked upon by blockchain. Steem network uses Graphene which helps Steemit to scale up to 10000 or more transactions per second. Undoubtedly, Steemit has to have a strong mechanism to secure the data from cyber-attacks.

Transactions performed without leaking the transaction or identification information is the definition of privacy in the blockchain. Blockchain's privacy disallows or makes it extremely difficult for people to access the node of other or also copy another user's information or to use other's crypto pole. The consensus algorithm of blockchain has provided many variations to prevent the cyber-attacks but still, the unspoken truth about blockchain is that like any other system, it is vulnerable to different attacks by the malicious programmers or hackers. Steemit, during the cyber-attack, might have been susceptible to attacks like the double spending attack, Byzantine attack, [13] Sybil attack or the 51% attack.

Double-spending attacks:

Double-spending, as its name suggests is a flaw in the digital cash system where the same token is spent more than once. The diagram below explains the double spending attack working methodology.

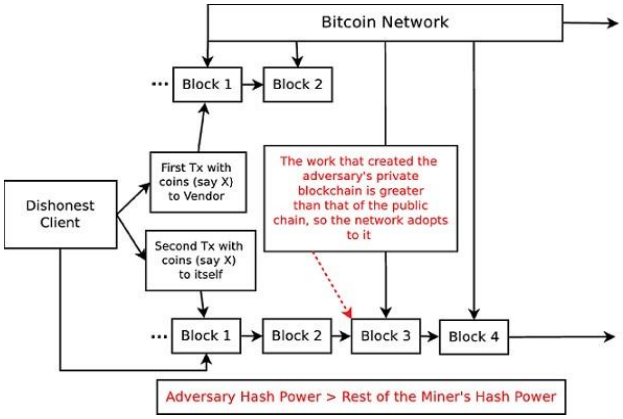

Fig 6: Double- spending attack [14]

A dishonest client creates a transaction to purchase a product from a vendor and at the same time creates another transaction using the same coin with the recipient address or wallet which is under the control of the dishonest client. In the above case, the attack would be successful if the client convinces the vendor to accept the transaction which was performed in the second time. As a result of the attack, the vendor will not be able to redeem it subsequently. A group of miners verify the process of transaction and identify that both transactions are trying to use the same input and hence it will process only one transaction and deny the other transaction [14]. If a miner mines a block with a faster rate, then the possibility of successful double spending become high. The increase in the computing resources of a minor increases the probability of double spend. A variant of double attack called the >50% attack is encountered due to the above scenario and considered to be the worst scenario as the entire stability of the network may be hampered due to this. Despite the use of strict transaction check-in blockchain, proof of work scheme, consensus protocol, double spending and other attacks such as the Sybil, Race attacks are still possible.

Hence, we propose the use of a hardware security model (HSM) to prevent the issue of cyber-attacks. Integrating the HSM into Steemit blockchain network will enhance its data security. The main purpose of HSM is to create private keys that cannot be retrieved except under a powerful controlled protocol. These keys provide security and access to the digital information which helps in strong data integrity as well as the user authentication can be typically improved. Using HSM will help Steemit secure and protect all its data and restrict the malicious and unintended intrusion of attackers.

2.2.2 Service Design

In service strategy, we discussed the strategy to tackle the cyber-attacks which had affected the Steemit reputation along with the monetary loss. So, in design, our main aim is to secure the cryptographic keys which act as a primary authorization mechanism which controls both transactions which includes issuance and transfer of assets. In authorization process, each transaction is signed using unique private keys which are required for issuance and transfer process and the signature is checked against the corresponding public keys which were recorded in earlier transactions being spent to determine the validity of new transaction. In simple cases, an asset or account defines a single key to be issued or transferred. However, multiple keys can be defined for different use patterns or different levels of security can be

achieved. Two signing keys, for example, can define a high - value asset that requires two separate parties to sign each issuance transaction. A joint account can also be defined with two signing keys that require only one to sign each transfer from either party. The required threshold number of signatures is called a quorum.

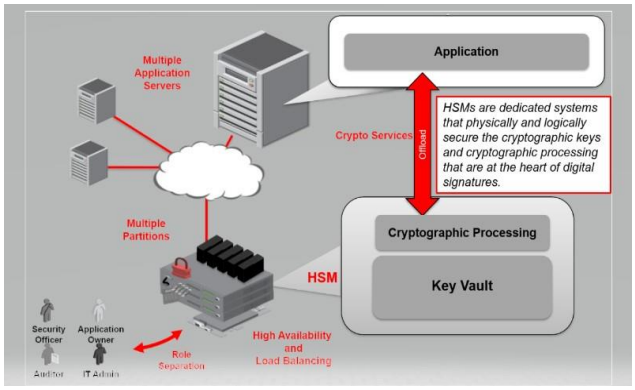

Fig 7: Working of HSM in blockchain

In order to safeguard and manage digital keys, we will use the Hardware Security Model (HSM). [15] HSM is a crypto processor that securely generates, protects and stores keys. HSMs typically guarantee a level of regulatory assurance, in compliance with either the Federal Information Processing Standard (FIPS) certification or Common Criteria, an international standard – meaning that each device meets strict industrial-grade security control requirements. Also, the keys stored in the HSM architecture cannot be extracted or used except under a highly controlled protocol. In every application requiring secure, verified digital signatures, HSMs are designed to virtually protect potential access points. HSM are widely used in bank data centers to verify PIN numbers whenever any customer withdraws cash from ATM or to validate transaction at merchant POS terminals for payments made. By deploying HSMs to Steemit system (computers and servers) will protect blockchain ledgers. [10] digital wallets and applications against hacks can provide the trusted computing environment which also enables to take full advantage of the blockchain protocol.

In order to carry out a successful attack, attackers would either need administrative privileges, access to data before encryption or physical access to the HSM, making the attack vector extremely difficult and unprofitable for a hacker.

What makes HSMs so robust and why Steemit should use it?

Any cryptographic operations must be carried out in a trusted environment – which means that there should be no exposure due to viruses, malware, exploits or unauthorized access. But in one big application, an ordinary wallet mixes access code, business logic, and cryptographic calls. This is a dangerous approach, as an attacker can then access cryptographic material or steal keys using crafted data and vulnerabilities.

HSMs are specially designed hardware systems for storing and managing private and public keys. The entire life cycle of the cryptographic key–from the provision, management, and storage to the disposal or archiving of keys–takes place in the HSM. Digital signatures can also be recorded through an HSM and all access transactions are logged to create an audit trail. An HSM is hardened against damage or tampering and can be placed in a physically safe area of a data center to prevent unauthorized contact. The module can be integrated into other hardware, connected to a server as part of a network or used offline as an independent device. HSM provides a trusted computing environment due to below-mentioned factors:

- It is built on specialized hardware and is certified and tested in special laboratories.
- The OS is built by considering all the security features.
- Provides Limited access through the network interface that is strictly controlled by internal rules.
- Also hides and protects cryptographic material regularly.

Taking all the security features provided by HSM into account, we have decided to deploy ultra-secure HSM-embedded PCs to Steemit that require two authentication factors (a key and a password) to ensure that unauthorized users cannot access the device. Thus, by using trusted computers embedded with HSM instead of digital wallets and as blockchain nodes gives the Steemit users' the assurance that they have the means to protect digital asset using a virtually impassable turnkey solution called HSM.

2.2.3 Service Transition

Once the design is completed and SDP is received, the next step is service transition in which the HSM's crypto processor is deployed into Steemit system. After successful deployment, the development team will hand over the application to testing team to perform various security checks and vulnerabilities. Testing team will also ensure that Steemit system is secure and security and redundancy is provided through consensus. In other words, consensus means, if any node of Steemit system is hit with DDoS, all other nodes of blockchain would keep the application running. If any of the nodes is hacked by a hacker and hacker tries to falsify the blockchain by showing more money in his account, it would not work as there would not be any consensus. So, the testing team will perform security testing by starting with blockchain nodes and then we will break each part of the system into individual parts as below and will finally test the whole application. Testing the nodes will include below checks as explained [12]:

Assessment of vulnerability and build review: To check all the nodes on a regular basis against vulnerability and make sure that it should not be exploited by any malicious person. This would avoid any future vulnerabilities.

Redundancy testing: This is done to find out what happens if we take nodes off the network. There should not be any single node on which blockchain is fully dependent instead it should rely on all the nodes.

Consensus Algorithm Testing: Testing is performed using the algorithm like Proof of Work, Proof of Stake [11] to check the data available on blockchain is legitimate or not.

Private keys: In blockchain, there will be a program running which has access to each node individual wallet using private key and password. This wallet can be used to access any users account and currency inside the wallet. So, the testing team will perform a security test like Password strength review using a brute force

method and Key storage review to make sure that the private key is secured.

Once the nodes are tested, security of Shared ledger which is a database containing the data used by Steemit is also ensured. This will be followed by testing the entire system which includes functional testing. After successful testing, the Steemit system will be ready to use HSM in real time environment and performance will be monitored periodically.

2.2.4 Service Operation

After the smooth transition of HSM into Steemit environment, the need for continual operation and maintenance arises for better performance and security of data, Steem power, and Steem dollars. Steemit should conduct its operations in the following way:

- Steemit will monitor and control security features of HSM's crypto-processors periodically so as to verify if a new update is available and updating the current system with the new update can bring better security Steem data.

- Different teams of Steemit like the IT operations, technical team, and application management team should be involved in the operation management of HSM and these teams will have to work hand in hand to provide greater consistency, control over the technical tasks. Doing this will simplify the processes, role conflict will decrease, increase the consistency over technical management activities, duplication of activities will not occur and hence will be more cost-effective to Steemit.

- Steemit should employee few own skilled labors who will be responsible for maintenance of the HSM infrastructure and will be readily available in case of an emergency incident.

- Steemit should also deploy a vendor management team who will connect with the HSM team to have answers on the technical hurdles faced. This team will be responsible to notify the vendor in case of any physical damage, configure each device as per the security policy, document each of the challenges faced in a known error database, track and maintain logs of the device's transactions.

- The access management team of Steemit will play an important role as it will be entitled to define the access of the HSM to only specific users depending upon their identity in the organization. This will secure the HSM environment from everyone's reach and hence will protect from external damage.

2.2.5 Continual Service Improvement

Steemit will have to continuously focus on improving the efficiency and maximizing the effectiveness of the delivered HSM solution under optimized service cost. CSI process will be performed throughout the service lifecycle to identify all the possible improvement areas. Steemit will periodically have to verify that the baseline for security measures are created and those are achieved through measurable targets. Continuous improvement for services and the HSM's hardware will be monitored in terms of functionality and physical damages. The technical team and IT operations team of Steemit will be mainly responsible for measuring the improvement metrics and consistency of HSM. Regular data center checks, infrastructure analysis, reviewing the trends, maturity assessments, internal auditing, reviewing existing deliverables, customer's feedback should be some of the recurring activities that must be planned in this phase to keep the security intact. Other various methodologies like fishbone analysis, Pareto charts, Ishikawa diagrams can be related and could also be used for validating and directing the measurement and metrics to enhance the continuous security improvements. These methods can also be used for illegal content posted via Steemit which is discussed in later section of this paper.

2.3 Illegal Data (Fatima Rojo)

Steemit is involved the publication of inappropriate or even illegal content. As we have already mentioned on other occasions, Blockchain technology allows data to be stored in the form of chain of blocks and thus carry out an ordered record in time without the possibility of modification or revision. If we talk about banking transactions, this is a great advantage, since in this way it is possible to control large amounts of transactions in a secure way, but what if these transactions instead of being money are about publishing content? What happens at Steemit if a user publishes inappropriate or illegal content? There is no way to eliminate it so that is why the data integrity issues have been questioned to Steemit. But how can we deal with this?

Today, Steemit proposes a method of flags or negative-voting to dispense this kind of problems, but it doesn't end them [17]. Let's take an example to understand how these flags are used.
Let's suppose that a Steemit user is engaged in publishing on the platform by sharing links to illegal downloads of books, movies, and other multimedia content. The rest of the users of the platform who access this content have the option (if their ethics accompany them) of assigning flags, which work in a way contrary to what we know today as "likes". It is a way of scoring negatively in such a way that the user's profile loses reputation and as they accumulate flags, their publications are hidden.

It seems to make sense and deal with the problem in a simple way, doesn't it? But is it that easy for users to assign these flags? Do these types of posts have enough visibility to receive so many negative scores and be hidden? The answer is no. On the one hand, following the example given above, there could be a situation where unethical users rate this type of publication positively despite the flags it receives. And, on the other hand, these publications may not be visible enough on the platform and may not even receive votes or be viewed by other users, but it will still be public on the net.
Besides, is it that easy for users to assign flags? Steemit works in such a way that a user who assigns flags loses voting power, i.e. could not vote for other interesting articles. This makes users tend not to use these flags in order not to lose their voting power [18].

Using ITIL to solve this issue

We have seen that the flags do not solve this great problem of data integrity, so how can we deal with it? In the case of replicated content, Steemit uses robots (as @cheetah) that use search algorithms and check whether the published content is plagiarism to automatically hide these publications. Steemit could propose a similar solution to deal with illegal or inappropriate content, but even so, despite hiding the publications, they would still exist in the chain.
Bearing in mind that any transaction registered in blockchain is unmodifiable, one of our proposals to resolve this is to modify the administration and treatment of publications. Instead of users

posting publications automatically on the net every time they write an article, users will have to make a publication request and wait a 24-hour period until their participation is finally published. During this 24-hour period, the article would be reviewed by the corresponding Steemit team, which will approve or disapprove it.
For this we will need two important things: a group of professionals with knowledge in legal issues that will be part of the content review team; and redesign the treatment of requests for publication of users before becoming part of the chain of blocks. For this purpose, we propose to use the ITIL [20] methodology in order to carry out these changes in the most successful way possible.

Within this methodology, we will need to redefine our Service Strategy in order to maximize the value generated by Steemit for its users, not only participants but readers, providing disclosure and sharing of valuable and properly regulated content. On the other hand, the service provided in question will be redesigned following the guidelines of Service Design offered by ITIL, carrying out new databases with which to manage publications and thus meet the need to share content in an appropriate manner.

2.3.1 Service Strategy

If we can't create value, our business won't get anywhere. Steemit, despite being a successful platform, is heavily criticized [16] not only by other members but by its own users as they consider that the values of this idea are lost with the existence of users who are engaged in publishing illegal or inappropriate content. According to ITIL "value is determined by the customer's perception, preferences and business outcomes" [21], and that is why it is of great importance to redefine the company's service strategy.

Vision, Mission and Values

At Steemit, the platform offered to users will remain the same, following the initial idea of sharing content. However, it will be necessary to define that such content, instead of being published directly to the network, will be accurately reviewed before being shared publicly and become part of the blockchain. This will ensure not only the authenticity of such content, but also legal compliance with respect to information that is being shared by users and therefore, the non-existence of the same in the chain of blocks.

Steemit will remain on its original values of bringing smart and social currency to publishers and community builders across the Internet through solidarity [22], consensus, liberty, equality and empowerment but adding the followings:

- Awareness: always making users aware of good content sharing practices.
- Trustworthiness: confidence that the Steemit community will not carry out inappropriate sharing content guidelines.

Strategic priorities

To meet Steemit new objectives, the following strategies are identified:

- Encourage members: encourage users to add value to the community through the built-in rewards structure.
- User awareness: promote and encourage users with the use of good content sharing practices, in order to create a clean community and let them know that anything out of place will be omitted for legal non-compliance.
- Maximize the value of the content: by ensuring the sharing of good and appropriate content minimizing the impact that the company is actually suffering in long term by somehow accepting the disclosure of illegal content.
- Create a group of Steemit professionals to review content: find profiles with experience in the legal field and compliance with legitimate content. A team of professionals will be created to review the articles published by users in order to ensure that there are no inappropriate publications or illegal content in the blockchain that cannot be removed later.
- Creation of a relational database: it will be necessary to create a relational database, with no blockchain mechanism, in order to store the publications in pending revision status so that these are not directly added to the blockchain.

2.3.2 Service Design

As mentioned above, to ensure that such content is not part of the blockchain, the relevant team of professionals will be responsible for reviewing user requests for publications. Once this has been approved, the members of the team will be responsible for publishing the article on the net and it will then be part of the chain of blocks. But how will these requests be handled?

As a solution, it is proposed to create a new regular database, which will store the pending articles to be reviewed each time users make a publication request. This will prevent publications from becoming directly part of the unmodifiable blockchain. To achieve this, we will follow the Service Design guidelines proposed by ITIL.

Service Design Package (SDP) Requirements

Establish a related database that stores the articles that users want to publish, i.e. they will be pending articles to be reviewed by Steemit expert team. Every time the user wants to publish an article, he will press the "publish request" button. The article will automatically be added to the database, which must be reviewed within 24 hours by Steemit team of experts.

Once the article has been reviewed, if the Steemit team considers it appropriate, it will be published, disappear from the relational database and become part of the blockchain. Otherwise, the article will be removed from the database and will never become part of the blockchain.

Database Design

Steemit will continue to make use of its Steem database based on the blockchain mechanism, whose content is immutably stored in the form of plain text. [23]. It will also continue using its ChainBase and AppBase, databases that Steemit uses which has faster load and allow Steem blockchain become modular, what makes Steemit more efficient and easier to maintain and scale.
However, it will make use of a new relational database where it will store publications pending revision. This database will consist of a table storing the pending articles to be reviewed. It will contain the following fields:

- id: auto-incremented identifier of the table and primary key

- idUser: identifier of the user who makes the request and foreign key that refers to the user
- idArticle: identifier of the article to review and foreign key that refers to the article
- requestDate: date when the request was made
- pending: status of the article to review

It will be also needed to create users and articles tables based on the ones in use within the blockchain, in order to relate the specific article to be reviewed with its author and the original article.

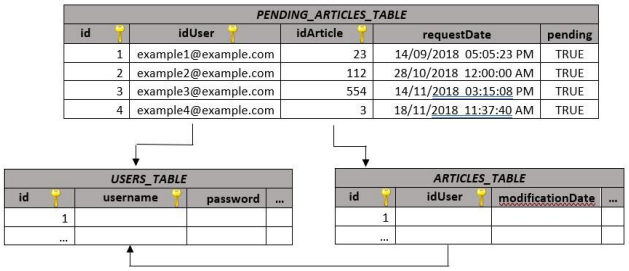

Fig 8. New Relational Database for Steemit

2.3.3 Service Transition

First step of this stage will be the acceptance of the SDP and change proposals. Once acquired the new configuration items and components, build and test will be carried out until the new change is released, deployed and supported.

Service Transition processes

The change being applied consists on adding a new relational database to store temporarily those articles from users which are to be reviewed before being added to the Steem blockchain. The reason for this change is the need for Steem to discard in some way those publications of inappropriate or illegal content that, today, are part of the chain and are immutable [24]. The economic valuation is approximate and since human resources constitute the most important economic component of this change and are above the physical resources required for the development of the project. Based on the tasks described above, the specialists involved in this project can be determined:

- Project manager
- Analyst
- Software developer

In this case, according to the work carried out in each phase of the project, the categories Project Manager and Analyst are attributed to the developer. The number of hours to be invoiced is obtained from the proposed planning for the development (Figure 3) of the project, with the days and weekly hours that the developer can dedicate to this project.

Human resources	Tasks	Salary per hour	Hours	Cost
Project Manager	Maintains contact with the client. Performs the functional and technic Analysis documentation. Defines, plans and performs system	$ 80	31	$ 2,480
Analyst	Analysis and the taking of requirem Schedules short-term scheduling tas Development of application elemer	$ 66	45	$ 2,970
			76	$ 5,450
			16% TAX	$ 872.00
			Total	**$ 6,322.00**

Fig 9. Estimated Costs

Within this stage, we establish the following planning to complete the Service Transition process including Change Management, Change Evaluation, Project Management, Application Development, Release and Deployment Management, Service Validation and Testing.

	Name of task	Start date	End date	Duration
Task 1	Components and items aqcuisition	01/14/19	01/15/19	2
Task 2	Software instalation	01/16/19	01/16/19	1
Task 3	Documentation	01/17/19	01/20/19	4
Task 4	Project Plan	01/21/19	01/22/19	2
Task 5	Risk Assessment	01/23/19	01/24/19	2
Task 6	Cost Estimation	01/25/19	01/26/19	2
	Review and correction	01/27/19	01/27/19	1
Task 7	Requirements Analysis	01/28/19	01/31/19	4
Task 8	Conceptual Design	02/01/19	02/04/19	4
Task 9	DB Logical Design	02/05/19	02/06/19	2
Task 10	DB Physical Design	02/07/19	02/11/19	5
Task 11	DB data load	02/12/19	02/13/19	2
Task 12	DB access methods	02/14/19	02/23/19	10
Task 13	Review and correction	02/24/19	02/24/19	1
Task 14	Testing	02/25/19	03/03/19	7
Task 15	Final documentation	03/04/19	03/13/19	10
	Review and correction	03/14/19	03/15/19	2
	Review and delivery	03/16/19	03/17/19	2

Fig 10. Development Plan.

2.3.4 Service Operation

During this phase, those events and incidents related to the changes implied by the implementation of the new database must be considered and dealt with, and the procedure recommended by ITIL for their treatment will be followed.

We will need to ensure that the following roles are fulfilled:

- Incident Manager: the person responsible for ensuring that everything is being done correctly, must now have knowledge of the new functionality that Steemit, understand the database and be prepared for any incident that may occur related to it.

- First-Level support: we will have the same Service Desk making sure that they know the new changes.

- Second-Level and Third-Level support: these teams oversee resolving incidents, they will have to have the capacity and know well those that may occur due to the new change.

This phase is of great importance as it is where the company's value is truly created, clearly defining how our service is delivered to the customer. In our case, the way we offer our users the ability to publish articles and ensuring the creation of a clean community and whose content sharing is free of inappropriate or illegal data.

In this way, the flow of activities in which our service is finally provided to our users would be as follows:

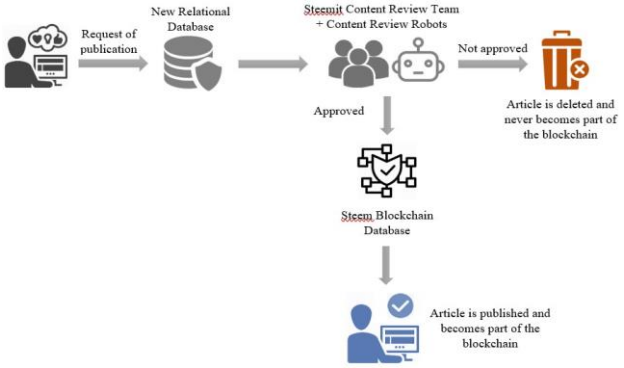

Fig 11. Service delivery activity flow

3. CONCLUSION

As we enter the era of blockchain, which follows censorship resistance, and decentralized technology, we should prepare ourselves with flexible, transparent and publicly accessible protocols. This paper has investigated, and designed Service management process based on ITIL framework to resolve issues faced by Steemit company, a blockchain based social media network. Steemit is an interesting social media platform where content writers are rewarded for their articles in the form of cryptocurrency called as Steem tokens. Steemit innovative business model is good but not flawless. It faces issues like governance, data security and publication of illegal contents. This paper has number of contributions. First, the paper introduces blockchain technology and its basic process. Then we go through the introduction of Steemit company. The paper explains how the team has designed Service centric IT business model for each issue to resolve it effectively. It also explains the concepts involved in various algorithms used like consensus algorithm, Inequality algorithm, Usage of HSMs, @cheetah bots etc. These functionalities designed by the team will resolve the issues and increase user traffic on Steemit network. By resolving these issues Steemit will once again win the trust of its lost customers and strengthen its bond with current users. The success of Steemit – a blockchain based social media network, will be a turning point in the Social media era. The IT Service model as described and designed in this paper is implemented and executed efficiently then sky is the only limit for Steemit Company.

4. REFERENCES

[1] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 2018, pp. 473-475.doi:10.1109/ICOIN.2018.8343163

[2] Steem: An incentivized, blockchain-based, public content platform. Retrieved September 2018 https://steem.io/ SteemWhitePaper.pdf

[3] Kevin Werbach, Berkeley Technology Law Journal 2018, Vol. 33 Issue 2, p487-550. 64p. ISSN. 1086-3818, DOI: 10.15779/Z38H41JM9N

[4] Alec Liu,"Who's Building Bitcoin? An Inside Look at Bitcoin's Open Source Development", MOTHERBOARD (May 7, 2013), DOI: [https://perma.cc/2A7U-N9KS]

[5] Ned Scott, Steemit CEO, Steem governance is multiparty, Steemit, DOI: https://steemit.com/steem/@steemitblog/steem-governance-is-multiparty

[6] DanPepijn; Doi: https://thenextweb.com/contributors/2017/08/2 1/blockchain-can-make-social-networks-private-profitable

[7] Team Steem, Steem white paper, (August 2017), DOI: file://A:/e%20books/1st%20sem/itm%20frameworks/project%20a rticles/SteemWhitePaper.pdf

[8] Orly, steemitbeta, DOI: https://steemit.com/steem/@orly/howto-fix-the-extreme-inequality-on-steem

[9] Hasib Anwar, Blockchain Technology stacks, 101 Blockchains DOI: https://101blockchains.com/web-3-0-blockchain-technology-stack/

[10] Marek R. Ogiela, Micha Majcher, Security of Distributed Ledger Solutions Based on Blockchain Technologies DOI: 10.1109/AINA.2018.00156

[11] Archana Prashanth Joshi, Meng Han and Yan Wang, A survey on security and privacy issues of blockchain technology

[12] Rohan Koul, Blockchain Oriented Software Testing - Challenges and Approaches

[13] Joanna Moubarak, Eric Filiol, Maroun Chamoun, On Blockchain Security and Relevant Attacks: 10.1109/MENACOMM.2018.8371010

[14] Mauro Conti, Senior Member, IEEE, Sandeep Kumar E, Member, A Survey on Security and Privacy Issues of Bitcoin DOI: 10.1109/COMST.2018.2842460

[15] OlivierBoireau, Securing the blockchain against hackers. DOI:10.1016/S1353-4858(18)30006-0

[16] U.W. Chohan, (2018, February 23), The Concept and Criticism of Steemit

[17] T. Aroha Kohi, (2017, January), Steemit – Value is Subjective.

[18] https://steemit.com/@cheetah

[19] B. Orand and J. Villareal. (2011), Foundations of IT Service Management

[20] Office of Government Commerce (OGC). (2007, May). ITIL v3 Service Strategy.

[21] Steemit. (2017, August). Steem Blue Paper. A protocol for anabling smart, social currency for publishers and content businesses across the internet

[22] Steemit Source Code. (2018, October). ChainBase – a fast version controlled, transactional database

[23] Steemit Source Code. (2018, September) AppBase, https://github.com/steemit/steem/tree/master/libraries/appbase

[24] Office of Government Commerce (OGC). (2007, May). ITIL v3 Service Operation.

RACI MATRIX

	Pragya Pramudita	Curie Nandeshwar	Anusha Bhallamudi	Shivank Saxena	M. Fátima Rojo del Prado
Abstract	R,A,C,I	R,A,C,I	C,I	R,A,C,I	C,I
Introduction	I	I	I	R,A	I
Content Governance	I	I	R,A	I	I
Security Concerns	R,A	R,A	I	I	I
Illegal Data	I	I	C,I	C,I	R,A
Conclusion	C,I	C,I	R,A	C,I	C,I