Blockchain Cyber Security Vulnerabilities and Potential Countermeasures

K. Sai Manoj* & P. S. Aithal**
*Postdoctoral researcher, Department of CSE, Srinivas University, Karnataka, Mangalore, India. & CEO, Amrita Sai Institute of Science and Technology and Innogeecks Technologies, Vijayawada, AP, India. E-mail : ceo@innogeecks.com
**Professor, College of Management, Srinivas University, Karnataka, Mangalore, India.

(February 2020)

ABSTRACT

Blockchain technology has attracted appreciable attention as a result of its big selection of possible application and it initial appear since a cryptocurrency, referred to as Bitcoin, however have as be employed inside several different industry and non-business applications. In contrast to the majority presented system to be supported decentralized system; this innovative expertise utilize peer-to-peer networks and circulated a system which incorporates blockchain register to stock up connections. Its construction is intended as a digital log file and hold on as a series of coupled teams, referred to as blocks. Every individual block is latched cryptographically with the previous block. Once a block has been another, it can't be altered. Several security specialists speculate that the inherent cryptographically nature of the blockchain system is comfortable to resist constant hacking and security threats. However, earlier studies on the security and confidentiality of blockchain technology include given away that several applications contain fall casualty to thriving cyber-attacks. As a result of the growing require for cryptocurrency and its current security challenges, earlier study haven't centered on blockchain technology cybersecurity vulnerabilities extensively, and we study after provide additional way to spotlight potential attacks against blockchain technology weakness to cybersecurity.

Keywords : Block Chain, Cloud Computing, Cyber security, Ledger, Smart Contracts, Cryptocurrency, attacks

1. INTRODUCTION :

The Cyber security framework comprises of those components engaged with the assurance of arranged PCs and data from digital dangers. The goal is to stop, avoid, recognize, recoup from, and react to dangers in the internet. The dangers take an assortment of structures and incorporate unapproved access to or utilization of data assets, and PC arrange assaults that deny, disturb, debase, or devastate data and system assets. They incorporate robbery of data, PC infections and worms, disfigurement of sites, disavowal of-administration assaults, PC and system infiltrations, and damage or creation of information. The security foundation serves to ensure against these dangers and guarantee the privacy, credibility, trustworthiness, and accessibility of information [1]. Blockchain is an exchange database which
contains data pretty much every one of the exchanges at any point executed before and takes a shot at Bitcoin convention.
It makes a computerized record of exchanges and enables every one of the members on system to alter the record in a verified manner which is shared over appropriated system of the PCs. For rolling out any improvements to the current square of information, every one of the hubs present in the system run calculations to assess, confirm and coordinate the exchange data with Blockchain history. On the off chance that lion's shares of the hubs concur for the exchange, at that point it is affirmed and another square gets added to the current chain.

Electronic copy available at: https://ssrn.com/abstract=3648436

The Blockchain metadata is put away in Google's Level DB by Bitcoin Core customer. We can imagine Blockchain as vertical stack having squares kept over one another and the bottommost square going about as establishment of the stack. The individual squares are connected to one another and alludes to past square in the chain. The individual squares are recognized by a hash which is created utilizing secure hash calculation (SHA-256) cryptographic hash calculation on the header of the square [2]. A square will have one parent however can have different kid each alluding to a similar parent square subsequently contains same hash in the past square hash field. Each square contains hash of parent obstruct in its own header and the arrangement of hashes connecting singular square with their parent square makes a major chain indicating the primary square called as Genesis square.

Blockchain innovation (BT) is a decentralized exchange and information the executive's innovation that give security, secrecy, and information uprightness without including any third-party association responsible for the exchanges.

 BT has value the executives abilities by utilizing electronic receipt records for exchanges perform more than web

 Blockchain Technology is additionally individual functional in the fields of fund, Gaming, betting, store network, assembling, exchange, and e-commerce.

 BT framework is a changeless database of every single chronicled exchange put away as a computerized record. Moreover, all hubs (clients) on the circulated blockchain system can deal with the mutual record.

 Blocks are orchestrated inside chains, wherever the base square be the establishment of the stack, each square be connected to the former square within the chain.

 Using cryptographic hash calculations, each square is distinguished by a created hash.

 The square within the chain container include single close Relative Square, yet different youngster squares.

 A square contains a header, made up of an interesting hash of its parent obstructs that interfaces it with its parent squares, shaping a chain.

 Block chain Technology framework be a computerized verification of proprietorship to fills in because a decentralized database framework, to which a ceaselessly developing rundown of exchange records is kept up, which contrasts starting conventional incorporated record frameworks [1].

2. RELATED WORK :

The utilization of Blockchain Technology in Bitcoin, which was propelled during November 2008, is to a great extent liable for the developing enthusiasm for BT. Bitcoin, a decentralized peer-to-peer advanced cash, track every single computerized occasion in an open record. It records all exchanges with the purpose of be shared between taking part parties and is checked by an accord of members in the mutual framework. When the data has been recorded during an advanced occasion, it can't be modified. Along these lines, Bitcoin contains a constant and obvious record of each occasion. Regarding security, Bitcoin is profoundly questionable in the advanced money showcase. In any case, Block chain Technology has discovered an extensive scope of uses in both the monetary and non-financial areas. A Blockchain makes an appropriated agreement in the computerized world, furnishing substances with a safe stage that keeps up past records of advanced occasions by making a verifiable record in an open record.

Exercises related with Block chain Technology are ordered interested in (3) three classifications in the perspective of association along with availability:

(a) The First-Generation open (Blockchain 1.0),

(b) The Second-Generation open (Blockchain 2.0),

(c) The Third-Generation Private (Blockchain 3.0).

Electronic copy available at: https://ssrn.com/abstract=3648436

Blockchain 1.0 sends cryptographic forms of money in applications identified with money, for example, cash moves, money repayments, and advanced instalments. Blockchain 2.0 incorporates brilliant agreements for monetary market along with budgetary application, this classification handle additional way with straightforward money exchanges. It incorporates stocks, securities, advances, contracts, titles, shrewd properties, and keen agreements. The third classification applies to applications past monetary forms, money, and markets. It incorporates zones, for example, government, wellbeing, science, proficiency, culture, and workmanship. Hence, blockchain inside this classification are viewed as private. Blockchain is a hopeful innovation that may well ease the danger of cyber-attacks coordinated toward a solitary end, which could cut downward whole system [3].

In any case, a coded interruption or framework weakness could enable increasingly negative outcomes to the security of the framework. For instance, if effective, an aggressor would obtain entrance not exclusively to the data put away at the purpose of assault yet additionally to all data recorded in the record. In this manner, security issues identified with blockchain are basic as far as cybersecurity, safety specialists require toward completely comprehend the degree as well as effect of the safety and protection moves identified with Blockchain previous to anticipating the possible harm starting an assault and confirm whether present innovation container survive diligent hacking endeavors [4].

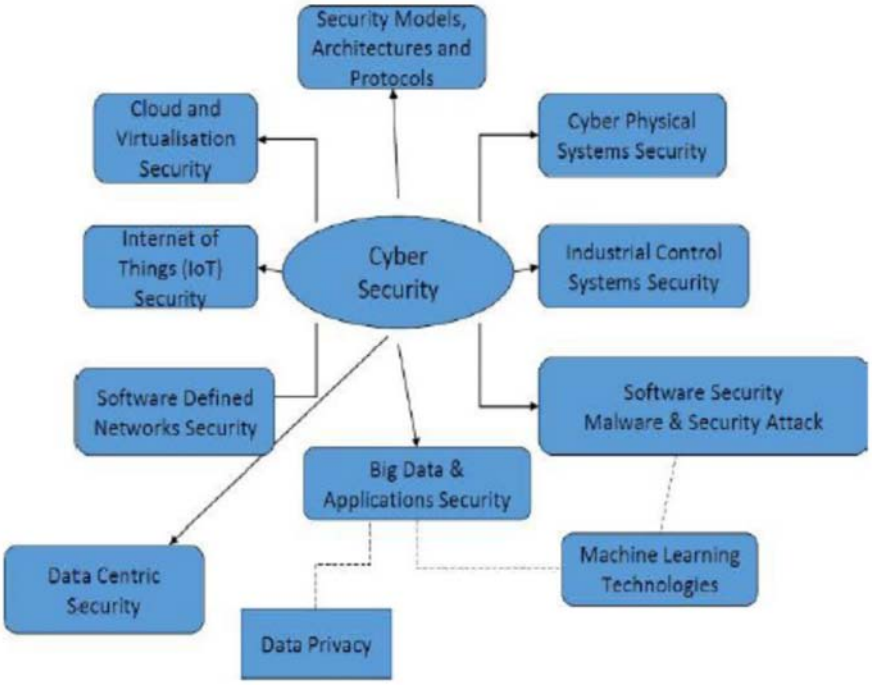

Figure 1: Cyber Security approach related technological branches

Past examinations have investigated the specialized engineering of BT in connection to cryptographic money. Albeit a few examinations have concentrated on the security parts of BT, inferable from the expanding interest for cryptographic money by it's present security challenges, these investigations have concentrated little on BT cybersecurity vulnerabilities. In view of such grounds, our examination shows an exhaustive survey of Block chain Technology security attacks by investigating assault vectors that attention on client security and it's attacks [3].

Electronic copy available at: https://ssrn.com/abstract=3648436

The above principles commitments of our examination are as per the following: first, initially investigation looks at safety measures difficulties and issues of existing digital currencies, together with the probability of assaults, concentrating essentially on issues of client protection and exchange obscurity. Their examination doesn't endeavor to fathom these difficulties and dangers, however rather exhibits a diagram of blockchain security, including looking at its vulnerabilities and talking about potential countermeasures.

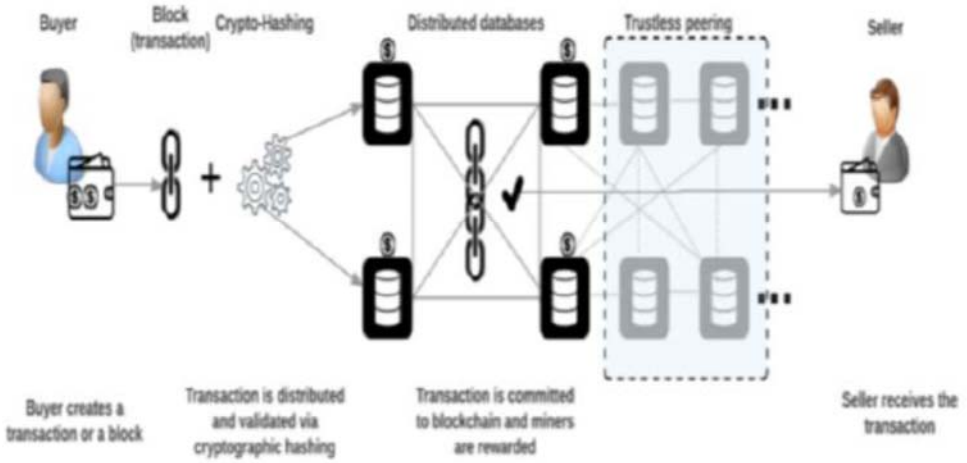

Figure 2: Block diagram of Public Blockchain

Fundamentals of Bitcoin

 Authentication: Bitcoin ID which is a decentralized validation convention enables clients to interface with Bitcoin, and BitID utilizes Bitcoin wallets and QR codes to give administration or stage passages.

 Integrity: Bitcoin's utilization of computerized marks guarantees value-based respectability and exchanges can't be changed later.

 Non-Repudiation: The individual who sent the message must be in control of the private key and thusly claims the Bitcoins, the sender requirements to sign the past hash and the goal open key.

Electronic copy available at: https://ssrn.com/abstract=3648436

Figure.3: Block diagram of Applications of Block Chain

Electronic copy available at: https://ssrn.com/abstract=3648436

Benefits of Bitcoin

 Fast and Cheaper: The exchanges made utilizing Bitcoin's wallets are quick and exchange expenses are insignificant.

 Decentralized Registry: Bitcoin cash is decentralized and no focal authority has full control and thus focal government or banks can't remove it from you and there is no chargeback. In any case, this is unimaginable with Bitcoins since the money is decentralized.

 Secure Payment Information: A Bitcoin exchange utilizes an open key and a private key. At the point when a Bitcoin is sent, the exchange is marked by open and private keys together which makes a declaration.

 Bitcoin Mining: You can make your own cash by setting up a Bitcoin Miner.

We examine, at different levels, the kinds of assaults that posture both reasonable and hypothetical dangers to BT. Second, as indicated by our examination, we talk about the restrictions of the state of the art arrangements that deal with safety dangers and empower solid protection. Third, in view of our exhaustive survey, we at that point give potential bearings to additionally investigate countermeasures for BT security vulnerabilities [5]. These research paper speaks to an exhaustive outline of security hazards and investigates genuine assault instances of Proof of Work (PoW) and Proof of Stake (PoS) based Block chain Technology and number of security dangers related with the advancement, usage, and utilization of Smart agreement based BT and future headings for potential countermeasures alongside BT cybersecurity vulnerabilities [4].

Network-level attack

At here, blockchain arrange safety issues to turn into the majority well-known research issue in the system safety measures ground. In any case, present be as yet different worries about its adaptability, security, accessibility, and manageability. With the ascent of the advanced money advertising, digital assaults that try to impact promoting and business-oriented administrations are always expanding. Among the various assaults, conveyed forswearing of administration (DDoS) assaults is one of the most widely recognized system data transfer capacity utilization assaults that have messed up administrations. DDoS assaults on blockchain-based stages dislike normal assaults, and in a decentralized and peer-to-peer innovation, it is supplementary troublesome and exorbitant than in customarily dispersed application design when an undertaking toward stifle the system utilizing an enormous volume of little exchanges happens. Be that as it may, blockchain-based stages.

In this manner, flexible along with decentralized blockchain arrangements can offer high availability, yet DDOS assaults resolve stay a decided threat to security. In a digital money environment, cash trades assume a foremost job, yet by and large, these frameworks experience DDoS assaults all the more as often as possible. Feder et al expressed that few cash trades have been closed down because of DDOS assaults. Mt. Goex is one of the principal trades to handle over 75% of bitcoin exchanges around the world [2].

It is the main Bitcoin mediator and is measured the greatest Bitcoin trade. EVasek along with Mooere did an extensive observational investigation of DDOS assaults in the Bitcoin biological system along with announced 58 assaults on trades and Bitcoin administrations. Specifically, present contain be 250+ one of a kind DDoS assaults on 40 Bitcoin administrations, where 7% of every single realized administrator has confronted assaults.

The creators additionally information to trades, mining pools, betting administrators, wallets, and budgetary administrations are undeniably more powerless against DDoS assaults than different administrations are.

Different reports show that 19.1% of little mining pools have been influenced by DDoS assaults, while 56.8% of enormous pools have confronted comparative assaults.

Electronic copy available at: https://ssrn.com/abstract=3648436

Their contrasted a legitimate methodology and an exploitative technique. Under the legitimate Paradigm, players of an alliance could put resources into extra figuring assets to improve the probability of winning the following race. Untrustworthy performer alliances concentrated on a mining group and set off an exorbitant DDoS assault to bring down the normal accomplishment of a contending mining pool [6].

Block Producers Plan : Hypothetically, inside several Blockchain frameworks, and danger of BP's (diggers, validate) conspiracy is approaching. In light of DPoS transferred a few validations, it is constantly conceivable to compose intrigue between them. As per vitalik, more than two significant assaults could dispatch within individuals conspiring BPs: restriction, change framework parameter, and twofold spend assaults.

Censorship Attack: Although a framework is at last intended in the direction of energize competitions and agreement between BPs, there is no assurance for engineers along with clients that their applications and exchanges won't be there edited. Oversight assault beside to DPoS implies that BPs will not procedure legitimate exchanges. On the off chance that solitary a solitary BPs (or minor gathering) edits an entity, it won't be a major issue for the system.

Table 1: categorization of Various Attacks

Smart Contract	Vulnerabilities	Categories of Bugs
The DAO, Maker's ETH-backed token	Reentrance	Reentrance (recursivecalling vulnerability A calling B calling A) Gametheoretic weaknesses
Rubixi, FirePonzi (Ponzi scheme)	Immutable bug Wrong constructor name	Variable/function naming mix-ups
King of the ether game	Out-of-gas send Exception disorder	Send failure due to 2300 gas limit
GovernMental (Ponzi scheme)	Immutable bug Stack overflow Unpredictable state Timestamp dependence	Arrays/loops and gas limits
FirePonzi	Type casts	Variable/function naming mix-ups
Parity multisig wallet	Visibility and delegate call	Unintended function exposure

Changing system parameters: In DPOS, all progressions have to be activated through dynamic partner authorization, in fact, conceivable to BPs intrigue along with modify their convention parameter singularly. On the off chance that an assault is a triumph, at that point, the assailant (or aggressor gathering) possibly will change the formation, expanding their square rewards, fork out specific partners, along with different choices on the convention. The edge for changing the standards is equivalent to supplanting 51% of the chosen observers. The more partner support in choosing observers, the harder it become to modify the standards. DPoS is planned so that these assaults are unrealistic without understood voter endorsement. In the EOS cases, changes near convention parameter contain time delays before they are really consolidated. Likewise, endorsement by 17/21 BPs is required to change the constitution, and they should keep up that endorsement for 30 back to back days before the progressions could happen. In the event that the client doesn't acknowledge transforms, they can remove that BPs

Electronic copy available at: https://ssrn.com/abstract=3648436

during that time and supplant them with makers that don't bolster the changes. At last, change the guidelines relies on everybody happening the system to overhaul their product, and no blockchain level convention can authorize, how system are altered. This implies hard forking "bug fixes" can be turned away lacking require a vote of the partners, in as much as they stay consistent with generally anticipated conduct of the code. By and by, just security-basic hard-forks ought to be actualized in such away. The designers and witnesses should trust that the partners will endorse even the most minor changes [7].

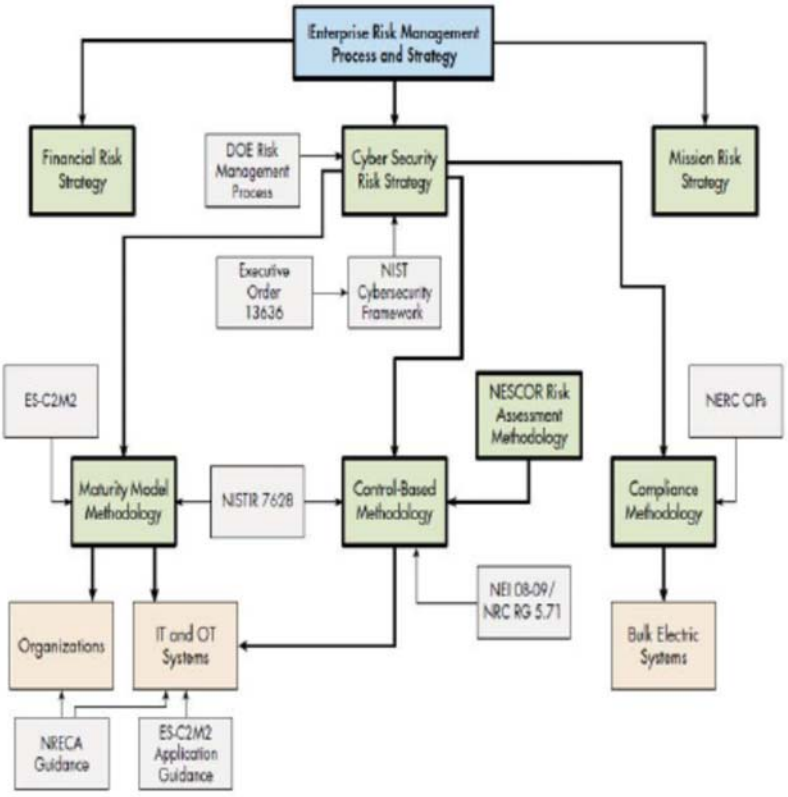

Figure 4: Cyber security monitoring process

Electronic copy available at: https://ssrn.com/abstract=3648436

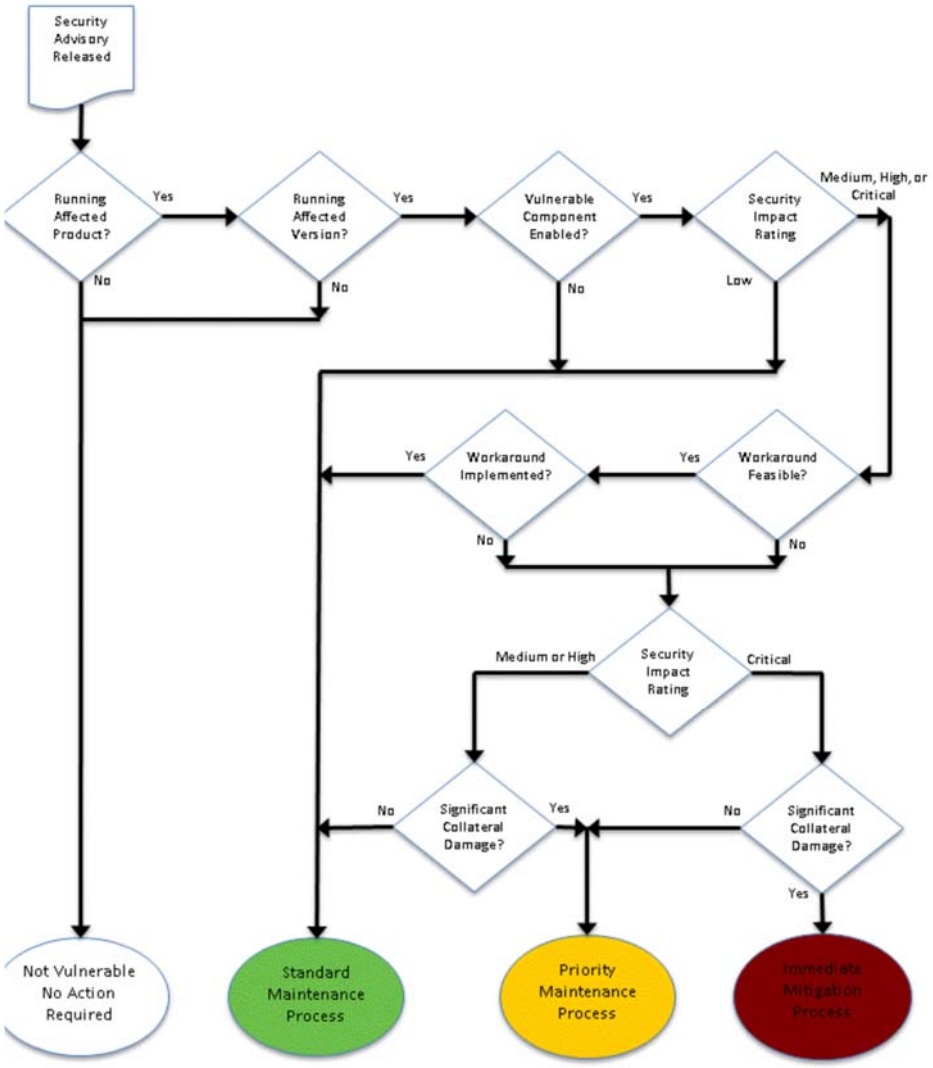

Figure 5 : Block Diagram of Risk Analysis

Attacks at scale: Another conceivable assault vector includes suppositions about what an industrial-scale DPoS blockchain resembles. As indicated by Larimer, EOS is probably going to scale such that huge server farms go about as BPs so as to give the degree of transmission capacity and speed the system requires.

It has not yet been seen by and by; be that as it may, on the off chance that it occurs, the suggestions merit considering. On the off chance that BP's is required toward exist inside committed server farms, they restricts the quantity of possible BP's and particularly restrains the number of elements to can step within near supplant BPs to sbe removed. In the event that there isn't any BPs with adequate assets to supplant BPs that has been removed, at that point, thus, the system may endure. Voters would need to settle on rebuffing a making trouble BPs and bringing down the general assets of the system [6].

Governmental: Governmental encounter experiences a comparable issue, through subway methods, the agreement be ponnzi conspire. Clients would send the agreement through guarantee of an expanded return and with the opportunity to win a "big stake."

The agreement put away it's clients' locations inside a powerfully measured cluster along with expected toward repeat more than the exhibits so as near patent them at what time a big stake be strike. In any case, it didn't constrain the size of the cluster. Legislative in the long run pulled

Electronic copy available at: https://ssrn.com/abstract=3648436

in enough clients that the gas allotment couldn't cover the whole exhibit [3]. Therefore, it would always neglect to reset the game and grant the big stake to the victor, with agreement's state remained successfully solidified.

Wallet security (private key security): By and large, cryptographic forms of money store their incentive in a document store called a wallet, whereby every customer claims a lot of private-open keys to get to the wallet. The significant shortcoming with the wallet is that it very well may be impacted, squeezed, and migrated simply like different stores. Clients regularly neglect to review their defensive PIN or secret phrase or lose the hard drive where the private key is found. This implies a client may not generally have the option to get to their store [7]. Considering this, ransoms are can cause a similar issue.

Wallet burglary utilizes exemplary instruments, for example, phishing, which incorporates framework hacking, the establishment of surrey programming, and the erroneous utilization of wallets. A blockchain framework can without much of a stretch be abused through any powerlessness that may add to a cryptographic arrangement since clearly any program bug otherwise absence of protected private key be able to establishment of a significant safety break. Speculatively, a crypto assailant ought not toward have the option to comprehend the first plain content, which is encoded. Be that as it may, it isn't hard to comprehend the arrangement of the squares, and even a decent cryptograph makes a plain book, for example, irregular babble, however positive characters or numbers are frequently establish in a similar spot within every square in the blockchain. This permits assailant the chance near endeavor a halfway portrayal of the natural content into each crypto secured square, where each square is an element of the former square [6]. In the cryptographic money space, Bitcoin has the biggest piece of the overall industry, wherever a Bitcoin file utilizes an open key, private key, and an individual location. As indicated by VanDam and Shparlinski, open keys can be produced securely from private keys utilizing a calculation called elliptic bend computerized signature (ECDSA). In any case, Vedral and Morikoshi contend that quantum PCs can break ECDSA. Furthermore, a machine can misuse quantum irregularity since its hidden truth is as yet obscure. This could permit the nearness of quantum bits (qubit), just as calculations that quantum PCs can play out that traditional PC can't. For instance, a quantum PC can run Shor's calculation and rapidly break any open key encryption by finding the elements of enormous numbers.

Unexpectedly, the Bitcoin convention address is determined to utilize the SHA-256 work for open keys, utilizing the RIPEMD-160 hash work and including a checksum for mistake remedy. While the scientific shortcomings of SHA-256 are astounding, no SHA-256 splitting episodes have happened, and subsequently, it has a solid and unsurprising future.

3. RESULTS :

The Analysis of Results

Various sizes of content records have been scrambled and Decrypted utilizing AES calculations, the consequence of the usage of AES has been contrasted and different calculations, for example, "DES, TDES, RC2 and Rijndael". The idea of the pressure was upon the time term that every calculation can take to scramble and to unscramble the various sizes of content documents. The essential motivation behind the factual examination in the term time that all calculations take to scramble or to unscramble content records with different sizes to contrast and with fine out the reasonable calculation that can be utilized to encode and to decode content document consequently as indicated by scope of the records measures, the separation applied between five even calculations, and they are "AES, DES, TDES, RC2 and Rijndael", and the distinctive size of the content documents which have been utilized in all calculations are "25 kb, 45 kb, 70 kb, 2 mb, 4 mb, 7 mb".

The investigation gave explicit time length to every calculation that can be expected to encode and decode content documents in the various sizes as follows AES. The execution part of

Electronic copy available at: https://ssrn.com/abstract=3648436

Rijndael figure and its backwards are dealt with, Thus in spite of the fact that Rijndael is appropriate to be actualized effectively on a wide scope of processors and committed equipment. The badly designed with the present examination discoveries, the pressure was in the job of following focuses:

- Resistance against every one of known's assaults.
- Speed and code conservativeness on wide officers of stages.
- Design effortlessness; too help similitude and dissimilarities with other symmetric.

4. CONCLUSIONS :

PoW is the most mainstream accord instrument and supporting innovation that looks after Bitcoin. Unmistakably the development of the Bitcoin with PoW and a protected time-stepping administration gives a solid security arrangement. In any case, it appears that this arrangement is exposed to various security dangers, for instance, double-spending (or race assaults) assault. Some blockchain stages were intended to be consent less by receiving PoW and improved security and secrecy, for instance, Bitcoin that utilizes Segwit and permits innovations like Lightning Network. ZeroCoin is a cryptographic expansion to Bitcoin that gives unlikable and untraceable exchanges by utilizing zero-knowledge confirmations.

Ethereum built up the PoS accord instrument that is fundamentally quicker and productive than the PoW framework since, in fact, anybody could turn into a digger, and it offers a straight scale comparative with the level of squares which an excavator could affirm on the grounds that it depends on the cryptographic money standard possessed system. As far as security, the PoS component additionally has its own downsides, for example, nothing-at-stake. Despite the fact that BitShares built up another accord model (DPoS) which is a propelled variation of PoS that gives a significant level of versatility. DPoS is structured as an execution of technology-based majority rule government utilizing the democratic and political decision procedure to shield the blockchain from malignant use. In parts of security, DPoS frameworks are defenseless against centralization as various observers are carefully constrained [7].

Truth be told, BT has profoundly changed the transaction-based ventures. In any case, there are some security concerns and dangers that keep this innovation from being utilized as a general stage in different executions around the globe. A few examinations and handy executions give arrangements against these dangers. Be that as it may, hearty and compelling security arrangements that can guarantee the correct working of BT, later on, are despite everything staying as difficulties and open research issues. With the rate of its development and advancement, it is accepted that BT may before long become an exceptionally normal innovation in business territories just as mechanical areas.

REFERENCES :

1. Stock B., Göbel J., Engelberth M., Freiling F. C., and Holz T. Walowdac-analysis of a peer-to-peer botnet. In Computer Network Defense (EC2ND), 2009 European conference on IEEE; 2009:13–20.

2. Vedral V, Morikoshi F. Schrödinger's cat meets Einstein's twins: a superposition of different clock times. Int J Theor Phys. 2008;47(8):2126-2129.

3. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: Big data (BigData congress), 2017 IEEE international congress on. IEEE; 2017:557-564.

4. ing S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper; 2012.

5. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf, retrieved on 28/04/2018 Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current

Electronic copy available at: https://ssrn.com/abstract=3648436

research on Blockchain technology?—a systematic review. PLoS ONE. 2016;11(10):e0163477. https://doi.org/10.1371/journal.pone.0163477

6. Petar T., Andrei D., Drachsler C., Arthur G., Florian B. Securify: Practical Security Analysis of Smart Contracts. arXiv:1806.01143v1 [cs.CR]. 2018

7. The Finney Attack, Available from https://bitcoincoreacademy.com/the-finney-attack, retrieved on 28/04/2018

****

Electronic copy available at: https://ssrn.com/abstract=3648436