BLOCKCHAIN APPROACH TO CYBER SECURITY VULNERABILITIES ATTACKS AND POTENTIAL COUNTERMEASURES

Bosubabu Sambana^{1*}, Yegireddi Ramesh², Molli Srinivasa Rao³,
T. Chalapathi Rao⁴ and N P Patnaik M⁵

^{1*}Assistant Professor, Department of Computer Science and Engineering,
Viswanadha Institute of Technology and Management, Visakhapatnam,
Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh, India

²Associate Professor, Department of Computer Science and Engineering,
Aditya Institute of Technology and Management, Tekkali
Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh, India.

³Professor and Head of the Department, Department of Computer Science and
Engineering, Viswanadha Institute of Technology and Management,
Visakhapatnam, Jawaharlal Nehru Technological University Kakinada,
Andhra Pradesh, India

⁴Sr. Assistant Professor, Department of Computer Science and Engineering,
Aditya Institute of Technology and Management, Tekkali
Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh, India

⁵Assistant Professor, Department of Computer Science and Engineering,
Viswanadha Institute of Technology and Management, Visakhapatnam,
Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh, India

^{1*}bosukalam@gmail.com, ²rameshyegireddi@gmail.com,
³srinivasmolli@rediffmail.com, ⁴chalapathit520@gmail.com,
⁵nppatnaikm@gmail.com

Abstract— Blockchain Technology has pulled in apparent consideration because of its enormous determination of potential applications. It at first showed up as cryptographic money, alluded to as Bitcoin, in any case, it has since been utilized in a few unique organizations and non-business applications, rather than most existing frameworks that are upheld concentrated structures, this new innovation uses peer-to-peer arranges and circulated system that join blockchain registers to store exchanges. Its structure is expected as an advanced log record and hangs on as a progression of coupled groups, alluded to as squares, each individual square is locked cryptographically with the past square. When a square has been another, it can't be modified.

A few security authorities conjecture that the intrinsic cryptographically nature of the blockchain framework is agreeable to oppose consistent hacking and security dangers. In any case, past examinations on the assurance and protection of blockchain Technology have indicated that few applications have succumbed to flourishing digital assaults. Because of the expanding interest for digital money and its present security challenges, past investigations haven't fixated on blockchain technology cybersecurity vulnerabilities broadly. Here, our examination stretches

Received: December 18, 2019

Reviewed: March 20, 2020

Accepted: March 24, 2020

* Corresponding Author

out upon the past investigations on vulnerabilities and explores the classifications of potential assaults. Our investigation at that point gives extra course to highlight potential attacks against blockchain innovation defenselessness to cybersecurity.

***Keywords—* Blockchain, vulnerabilities, Cloud Computing, Cyber security, Ledger, Smart Contracts, Cryptocurrency, Attacks**

1. INTRODUCTION

Blockchain technology, as its name implies, is a chain of blocks. Each of these blocks contains a set of transactions that have been cryptographically verified to be accurate, and these blocks are connected in a chain that respects the chronological order of the transactions contained in each block – hence the name blockchain. A blockchain represents a distributed ledger that stores the events that occur in the system. This ledger is immutable, and its contents are verified by all the nodes in the system – community verified. This simple idea provides the basis for a surprisingly wide variety of applications. The rest of this paper reviews the technology behind blockchain and then studies its uses.

Over the past decades, the ability to innovate and the speed with which companies embrace innovation have become a central aspect in the long-term competitiveness of companies. Today's quickly changing market forces companies to adapt more flexibly, which is made possible by promoting and adopting innovative solutions. A company which underestimates innovation cannot exist in the long term [8]; Hence, innovation ensures survival [1].

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.

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 [2].

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[3].

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 performed over the web
- BT is additionally being applied 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 in chains, where the base square is the establishment of the stack. Each square is connected to the former square in the chain.
- Using cryptographic hash calculations, each square is distinguished by a created hash.
- A square in the chain can have one parent 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. The main square is known as a beginning square (the first Bitcoin square was made in 2009).
- Thus, BT framework is a computerized record of proprietorship that fills in as a decentralized database framework, to which a ceaselessly developing rundown of exchange records is kept up, which contrasts from conventional incorporated database frameworks.

With the need for next-generation financial technology recently increasing, there have been active studies on blockchain for the secure use of electronic cash by communicating solely between peers and without the involvement of third parties.

A blockchain is the public ledger for transactions and it prevents hacking during transactions involving virtual cash. As a type of distributed database and data record list that continuously grows, it is designed to disable arbitrary tampering by the operator of distributed peers. Transaction records are encrypted according to a rule and operated in computers that run the blockchain software. Bitcoin is an electronic currency using blockchain technology [4].

Fig. 1 How to works entire Block Chain Technology

Using blockchain can provide higher security compared to storing all data in a central database. In the data storage and management aspect, damage from attacks on a database can be prevented. Moreover, since the blockchain has openness attribute, it can provide transparency in data when applied to an area requiring the disclosure of data. Due to such strengths, it can be utilized in diverse areas including the financial sector and the Internet of Things (IoT) environment and its applications are expected to expand. The blockchain finalizes a transaction record through the work authentication process, when a person who loans electronic cash forms a block by combining the transactions over the network.

The hash value is then generated by verifying it and connecting the previous block. This block is periodically updated and reflected on the electronic cash transaction details to share the latest transaction detail block. This process provides security for the transaction of electronic cash and allows the use of a reliable mechanism. Cloud computing has been applied to many IT environments due to its efficiency and availability. Moreover, cloud security and privacy issues have been discussed in terms of important security elements: confidentiality, integrity, and authentication, access control, and so on [5].

CONSIDERATION FOR BLOCKCHAIN SECURITY:

Challenges Blockchain technology has been implemented or realized as cyber money and is actually used. Note, however, that various security issues occurring in blockchain agreement, transaction, wallet, and software have been reported. This paper checks the trends of security issues raised to date and the security level of the current blockchain. We think this attempt is very important as the results can serve as base data for developing future blockchain technology and supplementing security [6].

Settlement of Blockchain Although there should only be one blockchain since it is the sequential connection of generated blocks, a blockchain may be divided into two because the two latest blocks can be generated temporarily if two different peers succeed in mining the answer for generating the block at the same time. In such case, the block that is not chosen as the latest block by the majority of peers in the Bitcoin network to continue mining will become meaningless. In other words, the Bitcoin will follow the majority of peers who have 50% or more mining capability (operating capability). Therefore, if an attacker has 51% mining capability, a "51% Attack", wherein the attacker has control of the blockchain and he/she can include falsified transactions, can be a problem. According to a study, an attacker can realize illegal gain with only 25% operating capability through a malicious mining process instead of 51%. Since the current operating capability of the whole Bitcoin network is already high gaining meaningful operating capability is considered to be difficult.

2. RELATED WORK

The utilization of BT in Bitcoin, which was propelled in November 2008, is to a great extent liable for the developing enthusiasm for BT. Bitcoin, a decentralized peer-to-peer advanced cash, tracks every single computerized occasion in an open record. It records all exchanges that are 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, BT has discovered a wide scope of uses in both the monetary and nonfinancial 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 [7].

Exercises related with BT are ordered into three classifications in the perspective of association and availability:

- a) The first-generation open (blockchain 1.0),
- b) The second-generation open (blockchain 2.0), and
- c) The third-generation private (blockchain 3.0).

Blockchain 1.0 sends cryptographic forms of money in applications identified with money, for example, cash moves, money repayments, and advanced installments. Blockchain 2.0 incorporates brilliant agreements for monetary markets and budgetary applications. This classification handles more than 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 promising innovation that may ease the danger of cyber attacks coordinated to a solitary point, which could cut down the whole system [5].

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. In this sense, security specialists need to completely comprehend the degree and effect of the security and protection moves identified with blockchain before anticipating the potential harm from an assault and confirm whether the present innovation can withstand diligent hacking endeavors.

Fig. 2 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 with its present security challenges, these investigations have concentrated little on BT cybersecurity vulnerabilities. Among these examinations, Conti *et al.*, concentrated on the major foundation of Bitcoin digital currency, outlines of its utilization and functionalities, and its protection perspectives. Atzei et al examined Ethereum savvy contracts and offered a scientific classification of general programming entanglements and bugs identified with BT vulnerabilities. With the rise of dynamic advancement assault strategies by programmers, the current ways to deal with security are turning out to be obsolete and less successful. In view of such grounds, our examination shows an exhaustive survey of BT security vulnerabilities by investigating assault vectors that attention on client security and its vulnerabilities [8].

The three principle commitments of our examination are as per the following: First, our investigation looks at the security difficulties and issues of existing digital currencies, including the probability of assaults, concentrating essentially on issues of client protection and exchange obscurity. Note that our 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.

Fig. 3 Block diagram of Public Blockchain

PREREQUISITES OF BITCOIN

- **Authentication:** BitID which is a decentralized validation convention enables clients to interface with Bitcoin. 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 needs to sign the past hash and the goal open key.

Fig. 4 Block diagram of Applications of Block Chain

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 address security 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. This 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 BT and number of security dangers related with the advancement, usage, and utilization of Smart agreement based BT and future headings for potential countermeasures against BT cybersecurity vulnerabilities [9].

NETWORK-LEVEL ATTACK

At present, blockchain arrange security issues to become the most well-known research issue in the system security field. In any case, there are 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.

In a decentralized and peer-to-peer innovation, it is more troublesome and exorbitant than in customarily dispersed application design when an undertaking to stifle the system utilizing an enormous volume of little exchanges happens. Be that as it may, blockchain-based stages, for example, Ethereum and Bitcoin, are defenseless against DDoS assaults. Subsequently, there are sufficient assurance estimates required both at the system and application level. For a situation model, in 2016, the Ethereum and Bitcoin systems persevered through the equivalent DDoS assaults as in 2014.

In this manner, flexible and decentralized blockchain arrangements can offer high availability, yet DDoS assaults will 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. Gox is one of the principal trades that handle over 70% of all Bitcoin exchanges around the world. It is the main Bitcoin mediator and is considered the greatest Bitcoin trade. Vasek and Moore did a wide observational investigation of DDoS assaults in the Bitcoin biological system and announced 58 assaults on trades and Bitcoin administrations [10].

Specifically, there have been 250+ one of a kind DDoS assaults on 40 Bitcoin administrations, where 7% of every single realized administrator has confronted assaults.

The creators additionally report that 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. Johnson *et al.*, considered a progression of game-theoretical models of rivalry between two pools of fluctuating sizes so as to complete a DDoS assault against another mining pool [16].

They 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 player alliances concentrated on a mining pool and set off an exorbitant DDoS assault to bring down the normal accomplishment of a contending mining pool [6].

BLOCK PRODUCERS COLLUDE

Hypothetically, in any blockchain framework, the danger of BPs (diggers, validator) conspiracy is approaching. In light of DPoS transferred a few validators, it is constantly conceivable to compose intrigue among them. As per Vitalik, three significant assaults could dispatch in those conspiring BPs: restriction, changing framework parameters, and twofold spend assaults.

Fig. 5 Block diagram of Block Chain enhanced Security Transformation

CENSORSHIP ATTACK

While a framework is at last intended to energize plutocracy and agreement among BPs, there is no assurance for engineers and clients that their applications and exchanges won't be edited. Oversight assault against to DPoS implies that BPs will not process legitimate exchanges. On the off chance that solitary a solitary BPs (or minor gathering) edits an individual, it won't be a major issue for the system. The following fair larger part of the BPs will presumably approve the exchange in the accompanying square, which could cause deferred exchanges by not handling them in their squares. In DPoS frameworks, the assault will be a triumph if most of BPs is under the aggressor's control (more than two-thirds of all BPs) [11].

CHANGING SYSTEM PARAMETERS

Under DPOS, all progressions must be activated by dynamic partner approval.⁴⁸ It is, in fact, conceivable that the BPs intrigue and change their convention parameters singularly. On the off chance that an assault is a triumph, at that point, the assailant (or aggressor gathering) may change the constitution, expanding their square rewards, forking out specific partners, and 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 becomes to change the standards. DPoS is planned so that these assaults are unrealistic without understood voter endorsement. In the EOS case, changes to convention parameters have 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 [12].

Table I. Various categorizations of Various Attacks

Smart Contract	Vulnerabilities	Categories of Bugs
The DAO, Maker's ETH-backed token	Re-entrance	Re-entrance (recursive-calling vulnerability A calling B calling A) Game-theoretic 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

In the event that the client doesn't acknowledge transforms, they can remove that BPs during that time and supplant them with makers that don't bolster the changes. At last, changing the guidelines rely on everybody on the system to overhaul their product, and no blockchain level convention can authorize how rules are changed. This implies hard-working "bug fixes" can be turned out without requiring a vote of the partners, inasmuch as they stay consistent with the 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.

Fig. 6 Cyber Security Monitoring Process

Fig. 7 Block Diagram of Cyber Security 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 BPs are required to be in committed server farms, it restricts the quantity of potential BPs and particularly restrains the number of elements that could step in to supplant BPs that are removed. In the event that there isn't any BPs with adequate assets to supplant BPs that have 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 [16].

GOVERNMENTAL

GovernMental encounter experiences a comparable issue, though through subtler methods. The agreement was a Ponzi conspire. Clients would send Ether to the agreement with the guarantee of an expanded return and with the opportunity to win a "big stake." The bonanza was gathered from a bit of every member's entrance and was granted to the last client to participate if nobody else had sent Ether to the agreement in a 12-hour period.

The agreement put away its clients' locations in a powerfully measured cluster and expected to repeat over the exhibits so as to clear them when a big stake was hit. In any case, it didn't constrain the size of the cluster. Legislative in the long run pulled 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, and the agreement's state remained successfully solidified [13].

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 [8]. 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 programming bug or absence of secure private key can be the establishment of a significant security break [15].

Fig. 8 Secure operation procedures on various End-to-End User

Speculatively, a crypto assailant ought not to 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 certain characters or numbers are frequently found in a similar spot in each square in the blockchain. This permits an assailant the chance to endeavor a halfway portrayal of the plain content in each crypto secured square, where each square is an element of the former square.

In the cryptographic money space, Bitcoin has the biggest piece of the overall industry, where a Bitcoin wallet 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 [14].

3. CONCLUSIONS

A blockchain has discarded the server to prohibit the association of the focal authority has encouraged exchanges through the members who together store the exchange records and, finally, support the exchanges utilizing P2P organize innovation. The blockchain has a distributed structure and uses the companion arrange and the figuring assets of friends. Specialized measures such as evidence of work and verification of stack have been executed to improve the security of the blockchain. Although the security of the blockchain is constantly upgraded, issues have proceeded to be reported and there are dynamic examinations on security. An aggressor makes different endeavors to get to a client's personal key put away in the client's PC or cell phone so as to hack the bitcoin.

There are studies on utilizing a safe token or sparing it safely to ensure the individual key. In this examination, we talked about the blockchain innovation and related center advancements and surveyed the pattern of studies to date to talk about further territories to be contemplated. Different current issues ought to be taken into a record to utilize blockchain in the distributed computing condition. Blockchain gives rise to numerous issues even now, for example, the security of exchanges, wallet, and programming and various studies have been directed to fathom these issues.

The secrecy of client data ought to be ensured when utilizing blockchain in the distributed computing condition and the client data should be totally erased while evacuating the administration. In the event that the client data isn't erased however instead left behind, the client data can be speculated from the rest of the data. Along these lines, this study discussed the technique for giving security by introducing a strategy for secure blockchain use and removal convention. It appears that reviews on effectiveness are likewise required adjacent to security, considering the environment wherein a monstrous measure of data is transmitted.

Ethereum developed the PoS consensus mechanism that is significantly faster and efficient than the PoW system since technically anyone could become a miner, and it offers a linear scale relative to the percentage of blocks which a miner could confirm because it is based on the cryptocurrency quota owned mechanism. In terms of security,

the PoS mechanism also has its own drawbacks, such as nothing-at-stake. Although, BitShares developed a new consensus model (DPoS) which is an advanced variant of PoS that provides a high level of scalability. DPoS is designed as an implementation of technology-based democracy using the voting and election process to protect the blockchain from malicious usage. In aspects of security, DPoS systems are vulnerable to centralization as a number of witnesses are strictly limited.

In fact, BT has radically changed the transaction-based industries. However, there are some security concerns and risks that prevent this technology from being used as a general platform in other implementations around the world. Several studies and practical implementations provide solutions against these risks. However, robust and effective security solutions that can ensure the proper functioning of BT in the future are still remaining as challenges and open research issues. With the rapidity of its growth and development, it is believed that BT may soon become a very common technology in business areas as well as industrial sectors.

REFERENCES

- [1] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys & Tut.*, vol. 18, no. 3, pp. 2084–2123, Mar. 2016.
- [2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [8] Decker, Christian, Jochen Seidel, and Roger Wattenhofer., "Bitcoin Meets Strong Consistency".
- [3] Cachin C. Architecture of the hyperledger blockchain fabric. In Workshop on distributed cryptocurrencies and consensus ledgers 2016, 310(1), pp. 4.
- [4] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." *International Journal of Web and Grid Services*, 2018, 14.4, pp.352-375.
- [5] Li, Wenting, et al. "Securing proof-of-stake blockchain protocols." *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, Cham, 2017, 8(1), 297-315.
- [6] Mengelkamp, Esther, et al. "A blockchain-based smart grid: towards sustainable local energy markets." *Computer Science-Research and Development*, 2018, 33.1, pp. 207-214.
- [7] Gao Y, Nobuhara H. A proof of stake sharding protocol for scalable blockchains. *Proceedings of the Asia-Pacific Advanced Network*. 2017; 44:13-6.
- [8] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. A systematic literature review of blockchain cyber security. *Digital Communications and Networks*. 2019, 12(5), pp. 1-14.
- [9] Sharma PK, Moon SY, Park JH. Block-VN: A distributed blockchain based vehicular network architecture in smart City. *JIPS*. 2017, 13(1), pp. 184-95.
- [10] "How Blockchain Can Fight Fraud Based on Know-Your-Customer Data", *Nasdaq.com*, 2019. [Online]. Available: <https://www.nasdaq.com/articles/how-blockchain-can-fight-fraud-base-d-know-your-customer-data-2019-02-11>. [Accessed: 19- Sep- 2019].
- [11] Koliass C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. *Computer*. 2017, 50(7), pp. 80-4.
- [12] Trautman LJ, Ormerod PC. Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. *Am. UL Rev*. 2016, 66(1), pp. 1231.
- [13] Konstantinos Christidis, and Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, vol 4.
- [14] T. FitzPatrick (2012), Key Success Factors of eLearning in Education: A Professional Development Model to Evaluate and Support eLearning, *US-China Education Review*, 2012, A 9, 789-795.
- [15] Ramzi Abdel Hai (2005), e-higher education. Determinants, justifications and media, *Dar al-Wafa we have printing and publishing*, Alexandria Egypt.
- [16] Jawad Kazem al-Najjar (June 2010) Improving the quality of education using the blackboard E-Learning System *Journal of the Faculty of Basic education-Number 6*, 6th