IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ANALYSIS OF BLOCKCHAIN-BASED TECHNOLOGIES AND THEIR APPLICATIONS IN CYBER SECURITY

Padala ajay kumar,Electrical and electronics engineering (EEE),C.V.R college of engineering

Hyderabad .

ABSTRACT

The blockchain, which has its features, got a lot of attention when it first came out and has been used in many different fields. At the same time, though, its security problems are constantly brought to light, and cyber attacks have caused it to lose a lot of money. At the moment, there isn't much concern or research in the field of blockchain network security. This paper talks about how blockchain can be used in different fields. It also analyses the security of each layer of the blockchain and possible cyber attacks systematically. It also talks about the problems that blockchain poses for network supervision and sums up the progress of research in protection technology. In this study, we look at the different ways that blockchain can be used with techniques that are common in the field of cybersecurity. It is a new kind of technology that is becoming more and more popular because it uses digital currencies. Even though Blockchain has a lot of potentials to improve the way online transactions work, it has a lot of security and vulnerability problems. This paper talks about the blockchain method, how it can be used, and security issues, which may help blockchain fans and researchers understand it better.

1. INTRODUCTION

Connectivity to the Internet is now available in an increasing number of locations. Data and computation outsourcing have been revolutionized by the widespread usage of cloud technologies, which have also allowed the emergence of the so-called Internet of Things (IoT) (IoT). In addition to the expansion of IoT devices, network technologies are also rapidly changing. For example, the recently developed 5G technology [1] has made it possible for devices to remain connected even when they are not in use.

An unknown person or group behind the Bitcoin currency, Satoshi Nakamoto, described how a network of computers, known as the blockchain, could be used to address the difficulty of maintaining transaction order and avoid double-spending [1]. Transactions are grouped into blocks with the same date, and the blocks are restricted in size. [2] The network nodes (miners) are responsible for ensuring that all of the blocks are linked together sequentially, with each block including its predecessor's hash. A robust and auditable record of all transactions is thus achieved through the use of the blockchain.

The scalability of distributed storage platforms [3], [4] has attracted great attention as a solution to this problem because of their capacity to network a large number of commodity storage devices. Cyberattacks could target devices that host digital content as those storage systems continue to expand in popularity. Encryption has recently been promoted as a differentiating characteristic to reduce the danger of data breaches [4], [5]. The distributed encrypted storage services have made progress, but no search functionality has yet been added to any of these services. This emerging paradigm has yet to properly investigate how to offer encrypted keyword search as a natural requirement.

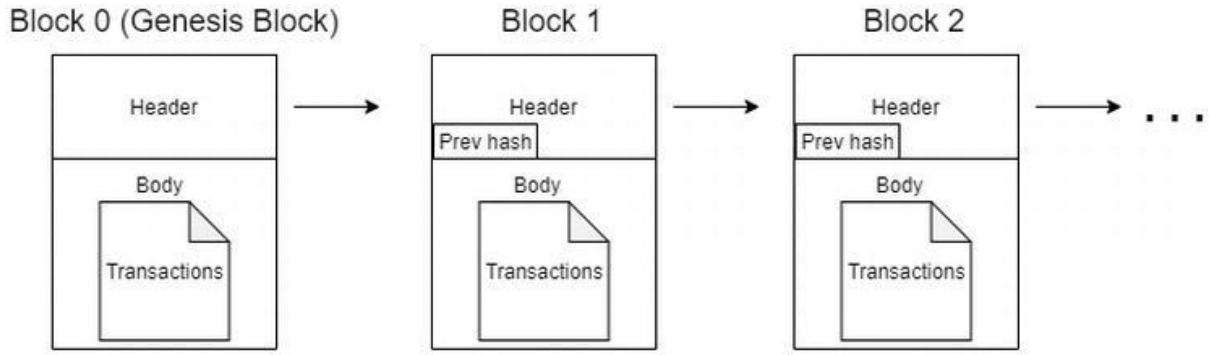

Figure 1. A blockchain is a chain of blocks.

Rather than having a single authority managing the entire process, the blockchain presents itself as a decentralized ledger that can be shared by anybody on a network of peers. In the case of blockchain, the ledger is structured in a chain of blocks, each of which agglutinates transactions sequentially. As a result, a block may be thought of as a structure made up of a header and a body, each of which contains a sequence of transactions. Each block is dated and signed by the person who crafted it. Blocks in the Bitcoin network are linked to each other by a cryptographic hash of their predecessor; the header of each block carries this hash so that each block is linked to the previous one (while ensuring the immutability of that previous block). It is known as the "genesis block" because it is the first block in a blockchain (Figure 1).

2. BLOCKCHAIN USE CASES FOR CYBERSECURITY

Even though the blockchain is not completely secure, it has evolved into one of the most dependable methods of transacting in digital networks. The technology's ability to guarantee data integrity, as intended, has been lauded. Many industries can gain from it if it is properly implemented.

Blockchain has the potential to be used in a wide range of applications because of its versatility. Integrity assurance can be used to construct cybersecurity solutions for a wide range of technology. Here are a few examples of how blockchain could be used to improve cybersecurity in the future:

1. Securing Private Messaging: More and more individuals are logging on to social media sites like Facebook and Twitter as the globe becomes a smaller village thanks to the internet. As the number of social media channels grows, so does competition. As conversational commerce grows in popularity, more social apps are being released every day. During these exchanges, massive volumes of metadata are gathered. Most social media platform users use passwords that are weak and unreliable to safeguard their accounts and personal information.

As an alternative to the end-to-end encryption, they now utilize, most messaging services are warming around to the idea of using blockchain to secure customer data. It is possible to build a standardized security protocol using blockchain technology. A unified API framework built on blockchain can be utilized to enable cross-messenger communication.

There has been a slew of attacks on Twitter and Facebook in the last several months. Millions of accounts were compromised as a result of these assaults, resulting in the loss of sensitive user data. This kind of hack may be prevented in the future if blockchain technology is properly introduced into these messaging platforms.

2. IoT Security: The use of edge devices, such as thermostats and routers, by hackers to break into larger networks is on the rise. Hackers are increasingly able to gain access to systems like home automation through edge devices like "smart" switches because of the current focus on Artificial Intelligence (AI). The security of many of these IoT gadgets is iffy at best.

In this situation, blockchain can be utilized to decentralize the administration of such comprehensive systems or devices. This strategy

will empower the device to independently make security judgments. Detecting and responding to questionable instructions from unknown networks without relying on a central admin or authority makes the edge devices more secure.

Hackers typically obtain access to a system's central administration and then take over all of the system's devices and systems. The decentralization of such device authority systems assures that such assaults are more difficult to carry out because of the blockchain (if even possible).

3. Securing DNS and DDoS: It is possible to conduct a Distributed Denial of Service (DDoS) attack by blocking the target resource's users from accessing or using it in any way. These assaults cause resource systems to slow down or stop working entirely.

On the other hand, a well-maintained Domain Name System (DNS) is a prime target for cybercriminals looking to compromise the link between an IP address and a website's name. Due to this attack, a website is rendered inoperable or can be redirected to another fake website or service.

However, by using blockchain to decentralize DNS entries, such threats can be lessened. Blockchain's decentralized solutions would have eliminated the single points of vulnerability that hackers attack.

4. Decentralising Medium Storage: Organizations are getting increasingly concerned about data intrusions and theft, which are becoming more and more prevalent. The majority of businesses continue to store data in a centralized location. A hacker can gain access to all of the data stored in these systems by exploiting only one vulnerability. As a result of such an attack, a criminal gains access to sensitive and confidential information, such as company financial records.

It is possible to ensure the decentralization of data storage while yet protecting sensitive information by utilizing blockchain. An effective mitigation strategy would make it nearly impossible for cybercriminals to get into information storage systems. There are a lot of storage service providers looking into how blockchain can keep data safe from intruders. When it comes to adopting blockchain technology, Apollo Currency Team is a great example (The Apollo Data Cloud).

5. The Provenance of Computer Software: Software downloads can be protected from foreign infiltration with the use of blockchain technology. In the same way that MD5 hashes are used to validate actions like firmware updates, installers, and patches, blockchain can be used to prevent malicious software from entering PCs. If we use MD5, we can check a new piece of software's identification against hashes found on vendor websites. The hashes on the provider's platform may already be compromised, thus this method is not fully foolproof.

Blockchain technology, on the other hand, makes it possible to store hashes indefinitely. Blockchain may be more efficient in checking the integrity of software by comparing it to the hashes on the blockchain because the information recorded in the technology is not mutable or changing.

6. Verification of Cyber-Physical

Infrastructures: Systems misconfiguration, data tampering, and component failure have all compromised the integrity of data created by cyber-physical systems. Blockchain technology's information integrity and verification capabilities can be used to authenticate any cyber-physical infrastructures. The chain of custody can be more assured with information created on infrastructure components via blockchain.

7. Protecting Data Transmission: Using blockchain technology to encrypt data in transit could be utilized in the future to prevent illegal access to data. An individual or a company can protect their data by using the technology's full encryption capability.

There would be a general increase in trust and integrity of data communicated via blockchain if this strategy were used. As the data travels across the internet, bad hackers can either alter or remove it entirely. Thus, inefficient methods of communication like email are left with a wide gap.

8. Diminish Human Safety Adversity caused by Cyber-attacks:

We've recently seen the introduction of unmanned military equipment and public transit as a result of cutting-edge technical breakthroughs. The Internet has made it possible for these autonomous vehicles and weapons to be created because it allows the transfer of sensor data to remote-control databases.

Hackers, on the other hand, have been hard at work breaking into networks like the Car Area Network and gaining access (CAN). These networks provide hackers complete control over critical automobile operations when they are tapped into. Human safety would be jeopardized if such events occurred. However, by verifying all data that enters and exits these systems on the blockchain, many problems might be avoided.

3. RESEARCH METHODOLOGY

Blockchain technology creates a secure and transparent environment for virtual currency transactions like Bitcoin. The blockchain is protected by the hash codes of each block. To put it another way, no matter how large the information or document is, the mathematic hash function generates the same hash code length for every block. As a result, any effort to modify a block of data results in a new hash value. The participants of a network that is open to all while maintaining user anonymity are bound to have trust concerns. Participants must therefore go through several consensus procedures, including Proof of Work and Proof of Stake, to develop confidence.

The first-ever blockchain technology is used by the digital currency Bitcoin. Peer-to-peer transactions over the internet can be made without the need for a third-party intermediary. In a decentralized network, nodes (computers) spread around the network check and verify new transactions to ensure their legitimacy. The mining process uses a variety of consensus models to reach this collective agreement. Adding a new transaction shows that each node has gone through and solved the complicated computational challenge, which is why they should be rewarded for their efforts. The network must validate the following conditions before a transaction can be considered valid:

The sender's Bitcoin balance is adequate to complete the transaction. You haven't already transferred the amount you're trying to send out. All nodes validate and agree on a transaction before it is added to a digital ledger and protected by cryptography that uses a public key available to all other nodes and a private key that must be kept confidential. Figure 1 depicts the transaction procedure in a Blockchain network. 2.

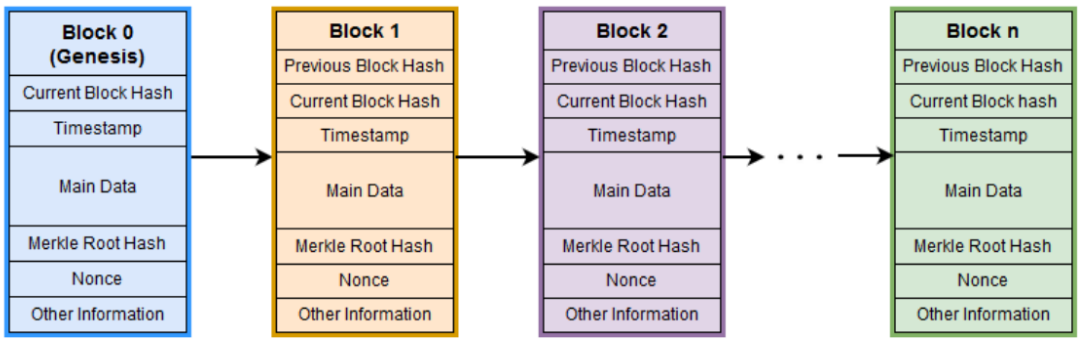

Fig. 2 A sequence of blockchain showing block structure

In the case of a Bitcoin transfer, the private key in your wallet must match the public address of your wallet to which the currency has been assigned for the transfer to be successful. The digital currency value is sent to your wallet's public address if the keys are identical.

3.1 Block Structure

A block contains several parts as shown in Fig. 3.

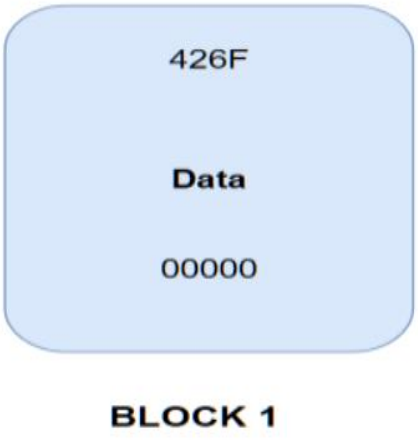

Fig. 3 Contents of Block

Main Data: Transaction data will be stored in blocks. For this transaction data to be useful, the relevant services for which blockchain is built must be considered. Financial transaction data will be maintained by financial entities like banks.

Timestamp: The timestamp is also included in the blocks. The timestamp in this context refers to the time and date at which a specific block is produced.

Hash: SHA-256 is one of the cryptographic hashing algorithms used to compute the block-specific hash.

The hash of the current block and the hash of the preceding block will be stored in the block. Immutability is ensured by the use of a hash. The Merkle tree function is used to build a hash. They are kept in the block's header.

The root hash of the Merkle tree generates a 64-character code by performing a mathematical hash calculation using all of the hash values associated with each transaction that occurred within a block. The Merkle tree root hash of all transactions in the block is stored for fast processing and data verification. This allows for efficient data processing and verification. A nonce is a 4-byte integer that can only be used once in a cryptographic transaction procedure. To create a new block in a Proof-of-Work algorithm, the nonce is utilized by miners as a counter to be solved. To get a less-than-target hash value, the complexity of the complex mathematical issue must be taken into consideration.

Block Properties: The hash of the previous block, Data, and a hash of the current block are the three basic components of a block in the blockchain. Anything can be stored on the block.

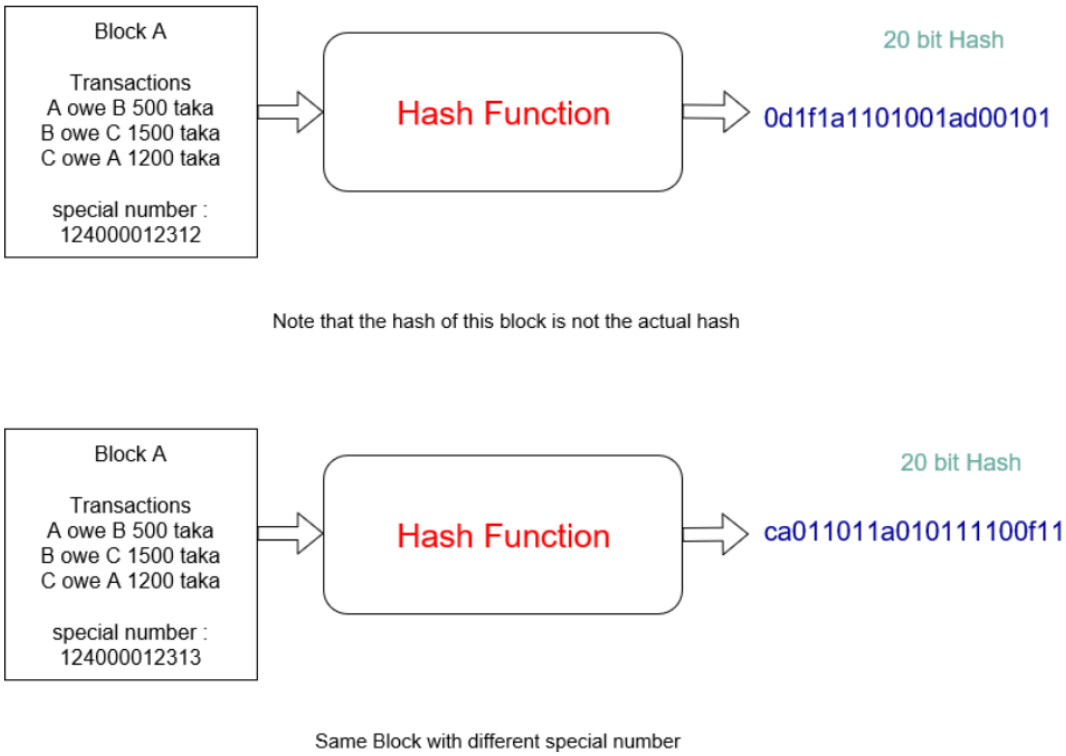

Fig. 3 An imaginary 20-bit hash algorithm

Hash Function: A hash function, for example, takes an input and outputs a string of specified length. Hashing algorithm 1. Each message's hash value is unique, yet it's always the same for the same input when using the hash function. Internal states are a part of a hash function. When it gets a message, those internal states will change. The internal states will vary in such a way that the hash

output makes it hard to determine the input message through combinations and permutations. As a result, we are unable to predict the output. Many computers must be used to hash out a block in blockchain technology.

The hash value can vary greatly depending on the input. There appears to be no pattern to these alterations, and they appear to occur at random. Whatever the case may be, it's completely random. A solution to cracking the rules that govern how things change as input changes have yet to be found. To prevent reversibility, the hash algorithm has been designed in such a way. Fig. Block A's special number increases by one, and the hash output of block 'A' substantially changes when this occurs. A single increment in the unique number does not correlate with the hash output. Even though the 20-bit hash is not the actual output of a hash algorithm, it is useful for understanding. The exact number is depicted in figure 3.

4. BLOCKCHAIN BLOCK

There are two parts to each block: a header and a list of all the transactions and events that took place in that block. Figure 4 depicts a blockchain block's construction. The following is an explanation:

4.1Block Header

There are three main sets of metadata in the block header.

4.1.1Version and Previous Block Hash

There are four bytes in the version field that are used to track software and protocol upgrades. As a reference, the previous block's hash field (32 bytes) contains 32 bytes of hash data. SHA256 is the cryptographic hashing algorithm used. This means that each block in a blockchain is connected to the previous block. The hash of the previous block is utilized to generate the hash of the current block. The genesis block is the first block on the blockchain.

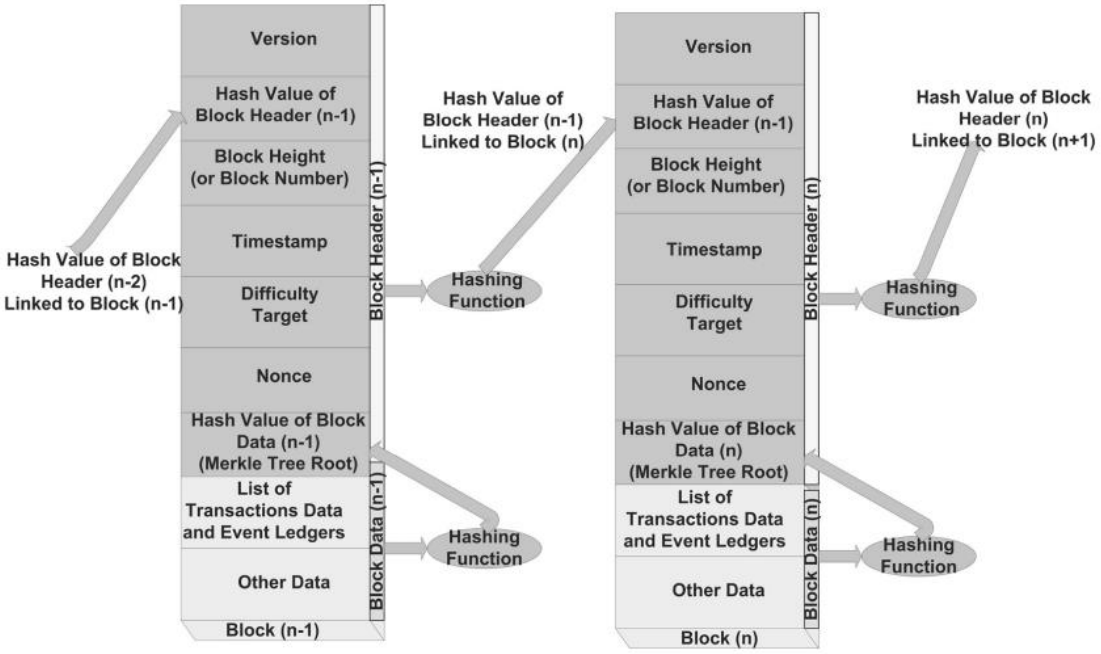

FIGURE 4 Blockchain chaining process.

4.1.2 The Mining Competition Scheme

The timestamp (4 bytes), the nonce (4 bytes), and the difficulty objective are all included in this collection of metadata (4 bytes). The block's timestamp is the date and time of its creation. Adding a nonce (a "number only used once") to a hashed block makes it easier to rehash the block and achieve the desired difficulty. Before solving for a block in the

blockchain, a blockchain miner must first uncover the nonce.

4.1.3 The Merkle Tree Root (32 Bytes)

The Merkle tree's root hash comprises a data structure of the block's transactions. Repeatedly hashing transaction node pairs until only one is left yields the Merkle tree's root. The process begins with the hashes of individual transactions and works its way up.

4.1.4Block Data

A user can check whether or not a transaction has been included in the block by using a Merkle tree. Having a way to verify that all previous event logs are included in the latest version and that all data is recorded and presented in chronological sequence helps.

4.1.5 Chaining of Blocks

A new block is created by the work of the miners. Any miner can add a new block to the chain. The miner creates a new hash for the freshly formed block by taking the hash from the previous block in the chain and adding its messages to it.

4.2 Smart Contracts

A digital token called "Ether" was proposed as a cryptocurrency for Ethereum when it was first established in 2015. Wei, Kwei (1K Wei), and Mwei (Mega Wei) are all standard units of currency for Ether prices and balances, and one Ether is (10 ** 18 Wei). Consensus mechanisms are used by Ethereum miners to preserve the network's state and handle potential conflicts, such as assaults or failures. Since users pay transaction fees and miners get paid for their work, Ethereum's present consensus mechanism relies on this assumption: that miners are more likely to stick with it rather than attack it because they are paid for their labor. Using the back-end Ethereum'smart contracts', any decentralized application (DApp) programming code can be run using any computational structure, including loops.

4.3 PROGRAM LISTING

1: A SIMPLE SMART CONTRACT

```
pragma solidity ¿=0.4.0;

contract Aeth {
//”public” makes variables accessible from
other contracts address public minter;
mapping (address =¿ uint) public balances;

 // Events allow clients to react to specific

// declare contract changes
event Sent(address from, address to, uint amount);

 // Constructor to create the contract

constructor() public { minter = msg.sender; }

// Sends an amount of newly created ETH to an add
ress

// To be called by the contract creator

function mint(address receiver, uint amount) public
{ require(msg.sender == minter);

require(amount ¡ 1e60); balances[receiver] += amo
unt; }

// Sends an amount of existing ETH

// from any caller to an address

function send(address receiver, uint amount) public
{

require(amount ¡= balances[msg.
sender],”Insufficient balance.”);

balances[msg.sender] -= amount;

balances[receiver] += amount;

emit Sent(msg.sender, receiver, amount);

}

}
```

Each block and each transaction can be accessed using a variety of primitives in solidity. As an example, the method calls msg. value to obtain the Wei amount sent through a transaction. Msg. the sender is another example of how the account address of the method's caller can be accessed. If someone wishes to call a specific function in a smart contract, they must know the exact signature of the smart contract's function. Smart contracts have a fallback feature that responds to transactions that signal incompatibility or non-functioning.

CONCLUSION

Security measures based on blockchain technology have seen a dramatic increase over the past few years. It's not just an academic tendency; industrial approaches have also firmly established themselves in this field. We've reviewed scholarly papers and established industrial methods for the past eight years. As demonstrated, blockchain technology is a

key enabler in the development of more intelligent and useful services. According to our findings, the ubiquity of Ethereum is a striking commonality between the worlds of business and academia. Because of this, new study opportunities have been discovered. Aside from that, studies have revealed that commercial proposals frequently exclude important aspects from their strategies. Another worrying fact is that a small percentage of academic papers use blockchain without presenting evidence that it is justified. To encourage more research in this field, several open issues have been identified. Predictably, Blockchain's future holds some important technological developments. Future work should focus on addressing various security concerns raised by other types of blockchain networks, such as private blockchain networks, which are frequently adopted by businesses and large corporations. Using a private blockchain makes the network more vulnerable to intrusions because it is more centrally located.

REFERENCES

[1] Sharma, P.K., Moon, S.Y., Park, J.H., 2017. Block-VN: a distributed blockchain-based vehicular network architecture in Smart City. Journal of Information Processing Systems 13 (1), 184–195.

[2] Lee, B., Lee, J.H., 2017. Blockchain-based secure firmware update for embedded devices in an internet of things environment. J. Supercomput. 73 (3), 1152–1167.

[3] Huckle, S., Bhattacharya, R., White, M., et al., 2016. Internet of things, blockchain, and shared economy applications. Procedia Computer Science 98, 461–466.

[4] Sari, A.; Rahnama, B., (2013) "Simulation of 802.11 Physical Layer Attacks in MANET," Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on, vol., no., pp.334,337, 5-7 June 2013, http://dx.doi.org/10.1109/CICSYN.2013.79.

[5] Sari, A., Rahnama, B (2013). "Addressing security challenges in WiMAX environment". In Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13). ACM, New York, NY, USA, 454-456. DOI=10.1145/2523514.2523586 http://doi.acm.org/10.1145/2523514.2523586

[6] Sari, A., Kilic, S., (2017); Exploiting Cryptocurrency Miners with OSINT Techniques, Transactions on Networks and Communications. Volume 5 No. 6, December (2017); pp: 62-76. http://dx.doi.org/10.14738/tnc.56.4083

[7] Sari, A., Qayyum, Z.A, Onursal, O. (2017) The Dark Side of China: The Government, Society and the Great Cannon, Transactions on Networks and Communications. Volume 5 No. 6, December (2017); pp: 48-61. http://dx.doi.org/10.14738/tnc.56.4062

[8] Sari, A. (2017); The Blockchain: Overview of "Past" and "Future", Transactions on Networks and Communications. Volume 5 No. 6, December (2017); pp: 39-47. http://dx.doi.org/10.14738/tnc.56.4061

[9] Sari, A, Akkaya, M., Fadiya, S., (2016) "A conceptual model selection of big data application: improvement for decision support system user organization" International Journal of Qualitative Research in Services, Vol.2, No.3, pp. 200-210. http://dx.doi.org/10.1504/IJQRS.2016.10003553

[10] Alzubi, A. and Sari, A. (2016) Deployment of Hash Function to Enhance Message Integrity in Wireless Body Area Network (WBAN). Int. J. Communications, Network, and System Sciences, Vol.9, No.12, pp. 613-621. http://dx.doi.org/10.4236/ijcns.2016.912047

[11] Sari, A., Akkaya, M. (2016) Contribution of Renewable Energy Potential to Sustainable Employment, Procedia - Social and Behavioral Sciences, Volume 229, 19 August 2016, Pages 316-325, ISSN 1877-0428, http://dx.doi.org/10.1016/j.sbspro.2016.07.142.

[12] Sari, A. Firat, A., Karaduman, A. (2016) Quality Assurance Issues in Higher Education Sectors of Developing Countries; Case of Northern Cyprus, Procedia - Social and Behavioral Sciences, Volume 229, 19 August 2016, Pages 326-334, ISSN 1877-0428, http://dx.doi.org/10.1016/j.sbspro.2016.07.143.

[13] Sopuru, J., Sari, A., (2016) When Technologies Manipulate our Emotions – Smell Detection in Smart Devices. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 988-991, ISSN 2229-5518.

[14] Kirencigil, B.Z., Yilmaz, O., Sari, A., (2016) Unified 3-tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 1001-1011, ISSN 2229-5518.

[15] Yilmaz, O., Kirencigil, B.Z., Sari, A., (2016) VAN Based theoretical EDI Framework to enhance organizational data security for B2B transactions and comparison of B2B cryptographic application models.International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 1012-1020, ISSN 2229-5518.

[16] Akkaya, M., Sari, A., Al-Radaideh, A.T., (2016) Factors affecting the adoption of cloud computing based-medical imaging by healthcare professionals. American Academic & Scholarly Research Journal, Vol.8, No.1, pp.13-22.

[17] Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Networks (VANET). Int. J. Communications, Network, and System Sciences, Vol. 8, No.13, pp. 552-566. http://dx.doi.org/10.4236/ijcns.2015.813050.

[18] Bal, M., Biricik, C.G. and Sari, A. (2015) Dissemination of Information Communication Technologies: Mobile Government Practices in the Developing States. Int. J. Communications, Network, and System Sciences, Vol. 8, No.13, pp. 543-551. http://dx.doi.org/10.4236/ijcns.2015.813049.

[19] Cambazoglu, Ş., and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. Int. J. Communications, Network, and System Sciences, Vol.8, No.13, pp. 533-542. http://dx.doi.org/10.4236/ijcns.2015.813048.

[20] Sari, A. and Akkaya, M. (2015) Fault Tolerance Mechanisms in Distributed Systems. International Journal of Communications, Network and System Sciences, Vol.8, No.12, pp. 471-482. DOI: http://10.4236/ijcns.2015.812042.