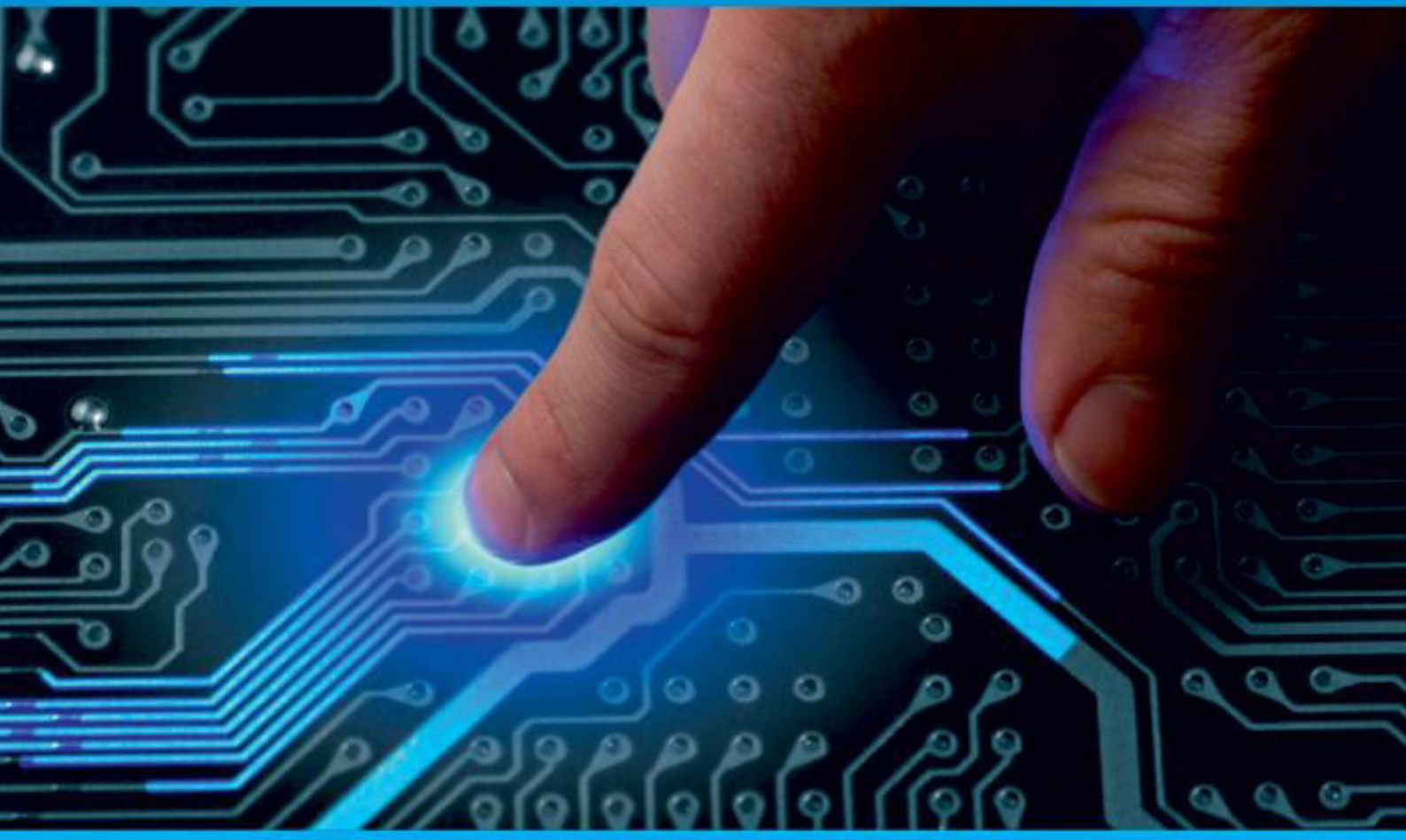
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 9, September 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009008 |

A Systematic Study of Blockchain and It's Application Domain

[1]Shreyash Gupta, [2]Aman Kumar, [3]Anirban Bhar, [4]Shambhu Nath Saha

[1,2] B. Tech Student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

[3]Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

[4]Associate Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

ABSTRACT: The purpose of the research paper is to give an overview about Blockchain technology. Blockchain is a growing list of records, called blocks which are linked together with the help of cryptography. Each block in the blockchain consists of some data, hash memory of the previous block and timestamp. These blocks are chained to each other and hence the name blockchain. As each block contains information about the previous block thus it is impossible to modify any data in the block without altering all other blocks. Blockchain are decentralized, distributed and often public digital ledger. Due to these features Blockchain is used not only for crypto-currencies but also for smart contract, financial services, supply chain etc.

KEYWORDS: Blockchain, Cryptography, Hash memory, Cryptocurrency, Decentralized, Timestamp.

I. INTRODUCTION

A blockchain is an immutable ledger since once data has been added to the chain it cannot be changed. This process is based on cryptographic hashes that overlap the blocks and since they overlap, the data is chained together. That is why it is called blockchain (chain of blocks). These blocks can also contain additional information which also becomes immutable. Which is the primary property for which blockchain technology is used.

Each block contains data, a timestamp, hash of the previous block, a nonce and the hash of the block itself. Where the index and timestamp are only for the ordering. The data is the information that will be stored in the blockchain and will become immutable once the blocks are chained together. The previous hash is the key or link to the previous block. In the first block the previous hash is 0, otherwise it contains the hash of the previous block. The nonce is not mandatory for all types of blockchains, but it is used to adjust the difficulty of the hashing. Basically, the final hash should have a fixed number of leading zeroes so that it can be accepted as hash. Finally, the hash field is the hash of the entire block, including the index, data, previous hash, nonce, etc. And it is the hash and the previous hash that makes blocks into a chain. If any single piece of data is changed in any of the blocks, it can easily be detected as the chain becomes broken. For example, if a change is made in block 1 from "hi" to "hey", then the new hash will be created for the change and it would be completely different from the hash which was stored in block 2. In this way any changes can be detected easily by all other users and the edited block will be discarded. Thus, ensuring that no changes can be made in blockchain easily.

II. HISTORICAL BACKGROUND

In this analysis, we also looked at the history, definition, and media usage of the term "blockchain." Particularly in the context of Sweden and the media's use of the word "blockkedja". According to what we can tell, Nanok Bie used the phrase "bitcoin" for the first time in Swedish media in May2011. A series of articles on the operation of this new coin and its danger to the current financial systems have been published in SVT nyheter[1], [2]. As the editor-in-chief of the news section of the main bitcoin.com website, Nanok Bie continues to publish and participate in articles on Bitcoin today.Journalist Anders Lotsson at International Data Group (IDG) published a series of stories in May 2013 that introduced the terms "blockchain" and "blockkedja" to the Swedish media [3]. These pieces were originally written for the Computer Sweden newspaper, but they were also printed in other IDG publications and on several IDG websites. Numerous other articles on the subject have since been published in Swedish media. Divided into each year, from 2008 to the present It's important to note that despite the first Bitcoin paper being released in 2008, it wasn't until 2013 that Bitcoin and blockchain technologies began to receive attention in Swedish media.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009008 |

The European Union passed the General Data Protection Regulation (GDPR), which was created to safeguard the data of people residing in the EU. It went into effect on May 25, 2018, and among other things, it makes it illegal for businesses to retain personal information about EU residents after receiving a request to delete it. However, because blockchain systems are immutable, it is nearly hard to comply with these requirements. simply because data on blockchains cannot be deleted and is generally accessible to anybody with access to the chain [4], [5].Blockchains have been excluded from this legislation by the regulatory bodies due to their resistance and scepticism, hence the two are in direct opposition to one another. Blockchains and GDPR, however, have a similar mindset and style of thinking. Both have been developed as a means of moving forward when major corporations or banks cannot be relied upon to act improperly with the knowledge they have amassed or the influence they have. The two do not necessarily have to be adversaries. Additionally, blockchains might be viewed as a valuable tool for data protection efforts [6], [7].

Blockchain technology and the development of a blockchain variant with immutability and data forgetting capabilities are the solutions for making blockchains GDPR compliant [8], [9]. First, public and private blockchains differ from one another, particularly in terms of accountability. The public blockchains should never be used to hold personal data because no one has official authority over them. However, there are other choices for blockchains that are private or have authorization. The operations of conventional databases follow the Create-Read-Update-Delete (CRUD) model and include the typical features we anticipate from a database system. There have been some suggested GDPR-compliant blockchains, and they typically use a Create-Retrieve-Append-Burn paradigm instead [10].

III. OVERVIEW OF BLOCKCHAIN FRAMEWORK

A blockchain is a distributed database that stores information on different nodes of a computer network. On being a database, blockchain stores information in digital format. Blockchains are well known for their use in cryptocurrencies, like bitcoin and for maintaining a secure and decentralized documentation of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the intervention of trusted third party.

One key dissimilarity between a database and a blockchain is how the data is stored in a structured manner. A blockchain collects information together in groups, which are called blocks, these blocks hold sets of information. Blocks have certain storage capacities and when filled the blocks are closed and linked to the previous block, forming a chain of blocks known as the blockchain. Similarly, the rest of the data that follows the freshly added block is compiled into new blocks and are linked to the previous block once filled.

A database stores data in tables whereas a blockchain stores data in group known as blocks which are linked to each other. This process of storing data makes an irreversible timeline of data when used in a decentralized nature. When a block is filled, the information's are noted and is set as a milestone on the timeline. Each block when added to the in the chain is given an exact timestamp.

Operations often waste lots of effort in maintaining a duplicate record and keeping third-party validations and these systems can be vulnerable to fraud and cyberattacks. Limited transparency of these records makes data verification a slow process and with the arrival of IoT, transaction volumes have exploded. All of this slows down business, thus we need a faster way and blockchain helps us with these problems.

Blockchain make these process faster with the help of the following features:

- Enhanced security

Data is sensitive and crucial, and blockchain can notably change how your important data is viewed. By creating a record that can't be changed and there is also an end-to-end encryption, blockchain helps to prevent fraud and unauthorized activity. Privacy issues can also be addressed on blockchain by removing particular details from personal data and using permissions to prevent unauthorized access. The data is stored across different servers rather than a single server, making it difficult for hackers to access data.

- Greater transparency

Without blockchain organization has to keep a separate database but with the help of blockchain transactions and data are recorded identically in multiple locations. All network participants with permission can access and see the same information at the same time, providing full transparency. All transactions are immutability recorded, and the time and date are stamped. This enables members to view the entire history of the transaction and eliminate any opportunity of fraud.

- Instant traceability

Blockchain creates an audit trail which keeps a track of an asset at every moment of its journey. In industries where users are concerned about environmental or human rights issues surrounding a product or an industry troubled by

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009008 |

imposters and fraud then this helps to provide the proof. With blockchain, it is possible to share data about track record directly with customers. The tracking record can also expose weaknesses in supply chain such as when a goods are poised in landing dock awaiting transits.

- Increased efficiency and speed

Traditional paper processes are time-consuming, liable to human error and often requires third-party intervention. By excluding these processes with the help of blockchain, transactions can be completed faster and more efficiently. Documentation and transaction details can be stored on the blockchain eliminating the need to exchange papers. There's also no need to confirm multiple ledgers, thus clearing and settling a transaction can be done much faster.

- Automation

Transactions can even be automated with "smart contracts" which increase productivity and speed the process even further. Once pre-declared conditions are met, the next step in transaction process is automatically processed. Smart contracts not only reduce human intervention but also reduce reliance on third parties to verify the terms of a contract. For example, once a consumer has provided all necessary documentation for a claim, then the claim can automatically be settled.

Consensus and validation are two of the fundamental characteristics of blockchain technology. It is a novel technology because of this. It keeps the same structure across all nodes and is designed as a monetary system. A public blockchain system is really neutral in the sense that it does not depend on trust, in contrast to conventional ledgers managed by centralised organisations (such as banks). Anyone wishing to participate as a node has access to a public blockchain full node client.

Different consensus procedures exist, including Delegated Proof of Stake (DPoS), Proof of WorK (PoW), and Proof of Stake (PoS), to mention a few.

A blockchain consensus method called "Proof of Work" enables nodes to work and provide evidence of each legitimate transaction. New information is added to a block when each node in a pool has confirmed a transaction and reached consensus. Each element that contributes to the effectiveness of this system is included in the architecture. These complete client nodes are "worker" nodes that operate on a blockchain network.

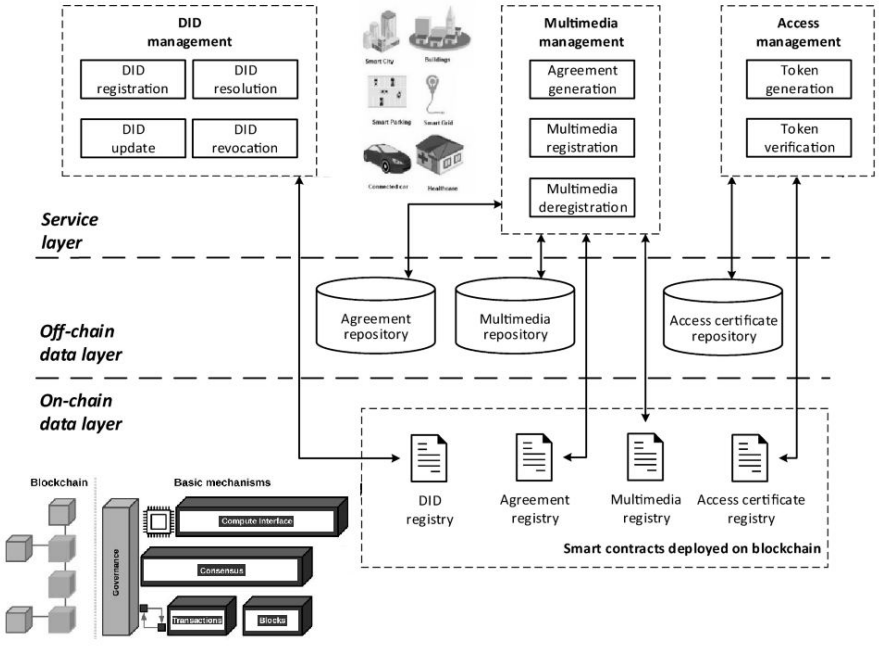


Fig.1.Architecture

A blockchain can be thought of as a distributed, append-only, timestamped data structure in theory. Blockchains enable us to build a dispersed peer-to-peer network where individuals who are not trustworthy can interact with each other in a verifiable manner without the need for a trusted third party (Christidis and Devetsikiotis, 2016). To do this, one might think of blockchain as a collection of interconnected mechanisms that give the infrastructure particular capabilities. We have the signed peer-to-peer transactions as the base of this system. These transactions signify a deal between two parties and could include the exchange of tangible or digital assets, the accomplishment of a task, etc. This transaction is distributed to the participants' neighbours after being signed by at least one of them.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009008 |

Any entity that connects to the blockchain is typically referred to as a node. Full nodes, on the other hand, are nodes that validate all of the blockchain's rules. These nodes organise the transactions into blocks and are in charge of deciding which transactions are legitimate and ought to be recorded in the blockchain and which ones shouldn't.

An example of a valid transaction would be Bob receiving one bitcoin from Alice. Nevertheless, given that bitcoin is a digital asset, Alice might have attempted to transmit Carol the same bitcoin. To ensure that there are no corrupt branches and divergences, nodes must agree on which transactions should be maintained in the blockchain (Vukoli, 2015; Christidis and Devetsikiotis, 2016).This makes the selection process more equitable and avoids having one participant dominate the network because of their money. Due to the huge reduction in power usage and enhanced scalability, many blockchains, including Ethereum (Dannen, 2017), are gradually switching to PoS. Other widely accepted methods include Byzantine Fault Tolerance (BFT) and its variations (Castro and Liskov, 2002). (Zheng et al., 2016).

Blockchains can now offer extra functionality thanks to a second layer called the Compute Interface. In practise, a blockchain retains a state that includes, for instance, all of the user transactions, allowing for the calculation of each user's balance. However, for more complicated applications, such as states that switch from one to another when certain conditions are satisfied, we need to store complex states that are updated dynamically using distributed computing. Due to this requirement, SCs have emerged, which leverage blockchain nodes to carry out a contract's conditions.

The Governance layer completes the blockchain architecture by extending it to include human interactions occurring in the real world. In spite of the fact that blockchain protocols are well stated, they are still impacted by the contributions of numerous groups of people that add new techniques, enhance the blockchain protocols, and repair the system. While essential to the development of each blockchain, these components are off-chain social processes. Blockchain governance therefore focuses on how these various parties collaborate to create, maintain, or modify the inputs that make up a blockchain.

Few of the features of Blockchain are

- Public ledger distributed ledger

The public distributed ledger is present in blockchains. The reason for this is that if only one person has access to all data, then he/she can tamper with the data without notice and because everyone has access to the data then any changes made can be notified easily.

Every user has access to the data on a blockchain, and they can see the whole record of transactions going back to the day the blockchain was created and any changes that are to be made in blockchains can be done after the consent of a majority of the network's members. Once a document has been changed, no changes can be done and once a transaction has been completed, it cannot be altered or modified.

- Hash inscriptions

A hash is a function that provides encryption requirement to a blockchain computation. Hashes are of predefined lengths, making it impossible for anyone to know the exact length of the hash value if they attempt to hack it because the hash values can’t be reversed to obtain the base text. Hash encryption is used as a key to protect confidential or sensitive data that is shared between two parties. Even the passwords are hashed so that even if a glitch occurs, the information can still be protected by PINs.

- Proof of work

Proof of work includes people competing with other people all over the world to be the first to add a block to the blockchain so that they can be awarded for their work. This helps them to invest in processing power. The people try to find the hash value that has certain predetermined criteria to receive this payment.

The hash value goal is set months in advance. The miners vary the nonce value to find an output that meets the desired criteria. If the miners find a value smaller than the hash value then the value is allowed otherwise, it is refused. This proof of work is easily verified by others people using hashing method.

- Mining

The process in which a block is added to a blockchain is called mining. The miners were the first to discover a nonce value that met the target criteria. For every block that is added the miners are rewarded with 12.5 Bitcoins but this reward is reduced every fourth year, resulting in a reward of 6.25 bitcoins currently. Blockchain Mining is an extremely costly process as mining consumes a lot of electricity, computing and other resources.

The working procedure may be implemented by the following steps

A blockchain is a distributed property that can be viewed by anyone but once the data is recorded on a blockchain, it cannot be changed. Blockchains dependent on three components: data, hash, and previous block hash.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009008 |

Step 1: Data

The type of data stored in a block can vary according to the purpose or type of the blockchain. If the blockchain is of Bitcoin, then the blocks contain transaction details such as sender receiver and transaction amount.

Step 2: hash

A hash is like a fingerprint, which is included in the block. When a block is created, its hash is also created at that moment and if any changes are made within the block, then the hash also changes. This also helps in finding out any changes that are made in the block. If a block's hash is changed then that block is no longer the same block.

Step 3: Previous data hash

The hash of the previous block is the last part of a blockchain. The hash of the prior block helps to create a chain and as a result of it the blockchains are extremely secure and trustworthy to use. In a blockchain, each block is linked to the previous block with the help of the hash data and if any changes are made in the blocks the hash data changes and similarly the other blocks recognize it and make changes in them accordingly.

Nowadays computers can sort thousands of hashes every second to make the block chain valid again. The hash tampered blocks is changed with the default blocks and similarly the hashes are also changed. This is completed with the help of proof of work.

The application domain of Block chain may be categorised as

- Asset Management

Blockchain plays a huge role in the financial world and it is no different in asset management. In simple terms, asset management includes the handling and exchange of different assets that an individual may own such as fixed income, real estate, equity, mutual funds, commodities, and other alternative investments. Normal trading processes in asset management can be very expensive, especially if the trading involves many countries and cross border payments. In these situations, Blockchain can be of great help as it removes the needs for any intermediaries such as the broker, custodians, brokers, settlement managers, etc. Instead, the blockchain ledge provides a simple and transparent process that eliminates the chances of error.

- Cross-Border Payments

Cross border payments can be a long-complicated process and it can take a lot of days for the money to arrive at its destination. Blockchain has assisted in simplifying these cross-border payments by equipping end-to-end remittance services without any intermediaries. There are multiple remittance companies that offer Blockchain services that can be used to make international remittances within 24 hours.

- Healthcare

Blockchain can have a huge impact on healthcare using smart contracts. Such smart contracts mean that a contract is made between 2 parties without needing any intermediary. All the parties involved in the contract know the contract details and the contract is applied automatically when the contract conditions are met. This can be very helpful in healthcare wearing personal health records can be encoded via Blockchain so they are only accessible to primary healthcare providers with a key. They also help in upholding the HIPAA Privacy Rule which guarantees that patient information is confidential and not accessible to all.

- Cryptocurrency

Perhaps one of the trendy applications of Blockchain is in Cryptocurrency. Who hasn't heard about bitcoin and its insane popularity. One of the many advantages of cryptocurrency using blockchain is that it has no geographical limitations. So crypto coins can be used for payments all over the world. The only important thing to remember is exchange rates and that people may lose some money in this process. However, this option is much better than regional payment apps that are only relevant in a particular country or geographical region and cannot be used to pay money to people in different countries.

- Blockchain in Cloud Storage

Centralized servers can lead to a high risk of data hacking, loss, or human errors. Cloud storage can be made more secure and vigorous against hacking with the execution of Blockchain technology, just like its application in cybersecurity.

- Supply Chain Management

The use of blockchain can eliminate time delays and human errors and monitor employment, costs, and releases at every step of the supply chain. Through traceability, Blockchain can also guarantee the fair-trade status and legitimacy of products. Blockchain has the potential to avoid the loss of revenue from black- or grey-market products and prevent reputational damage as well.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009008 |

- Internet of Things

Internet of things is a network of interconnected devices which communicate with each other's to gather information which can be useful in understanding different perceptions. Any system of things becomes an internet of things once it is connected with different devices. The most common examples are smart homes where all appliances can be connected and controlled together on a single platform. In massively distributed system blockchains are used to provide security. In IoT the security of systems is good but any least secured device could be the weak link. Here blockchain can help to store the data obtained from the IoT devices securely and makes it visible to trusted parties.

- NFT

A non-fungible token (NFT) is a record on a blockchain which is related to physical or digital asset. The possession of a NFT is stored in blockchain and can be transferred by the possessor to others, allowing the NFT's to be traded. NFT's can be created by anyone and no coding skills are required to create an NFT. NFT's usually contains references to the digital files such as photos videos and audio. As NFT's are identifiable assets they differ from cryptocurrencies which are fungible.

IV. CONCLUSION AND FUTURE WORK

Blockchain is a new technology that is still not widespread in all industries but it is slowly attaining more momentum. Once Blockchain becomes more widespread, it could become a powerful tool for the democratization of data that will help transparency and ethical business tactics and the uses of Blockchain would increase in the world with the result of faster transactions, more transparency, and security as well as reduced costs.

According to a theoretical analysis of the literature, Blockchain Technology offers high potential for solving issues with data integrity, increasing transparency, enhancing security, reducing fraud, and establishing trust and privacy. Blockchain technology has the potential to revolutionise a variety of industries, including finance, accounting, e-government, business process management, insurance, entertainment, trading platforms, healthcare, the internet of things, law firms, and others. Because technical innovation and applications can be used to achieve economic efficiency and societal benefits, Blockchain Technology has a significant potential to introduce novel solutions, depending on the field or industry in which it is used.

As a result, existing systems and outdated applications may not be quickly replaced by blockchain technology. Blockchain can, however, be used in conjunction with existing systems and, in the near future, might even inspire the creation of new ones.

REFERENCES

1. N. Bie, "Ny piratvaluta kan hota finanssystemen," May 2011. [Online]. Available:https://www.svt.se/2.22584/1.2439316/ny piratvaluta kan hota finanssystemen.
2. "Hr kan man spendera piratpengar," May 2011. [Online]. Available: https://www.svt.se/2.22584/1.2439344/har kan man spendera piratpengar.
3. A. Lotsson, "Bitcoin-valutan blir notarie," May 2013. [Online]. Available: https://computersweden.idg.se/2.2683/1.509172/bitcoin-valutan-blir-notarie.
4. D. Pollock, "How can blockchain thrive in the face of european gdpr blockade?" Oct 2018. [Online]. Available:https://www.forbes.com/sites/darrynpollock/2018/10/03/how-can-blockchain-thrive-in-the-face-of-european-gdpr-blockade/#66b754f861df.
5. "The gdpr and blockchain," Aug 2018. [Online]. Available: https://www.insideprivacy.com/international/european-union/the-gdpr-and-blockchain.
6. L. Mearian, "Will blockchain run afoul of gdpr? (yes and no)," May 2018. [Online]. Available:https://www.computerworld.com/article/3269750/blockchain/will-blockchain-run-afoul-of-gdpr-yes-and-no.html.
7. C. Sweden, "Krockar blockkedjan med gdpr? ja och nej," May 2018. [Online]. Available: https://computersweden.idg.se/2.2683/1.702061/blockkedjangdpr.
8. "Tre nycklar till framgng i blockchain-revolutionen." [Online]. Available:https://computersweden.idg.se/2.2683/1.697424/blockchain-framgang.
9. B. D. Journal, "Here's how gdpr and the blockchain can coexist," Jul 2018. [Online]. Available: https://thenextweb.com/syndication/2018/07/26/gdprblockchain-cryptocurrency/
10. A. V. Humbeeck, "The blockchain-gdpr paradox wearetheledger medium," Nov 2017. [Online]. Available: https://medium.com/wearetheledger/theblockchain-gdpr-paradox-fc51e663d047.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details