Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

A survey on applications and security issues of blockchain technology in business sectors

S. Gomathi [a], Mukesh Soni [b], Gaurav Dhiman [c,*], Ramya Govindaraj [d], Pankaj Kumar [e]

[a] UK International Qualifications, Ltd., Middle East, Asia & Africa Regional Office, Sharjah 62192, United Arab Emirates
[b] Department of Computer Science and Engineering, Jagran Lakecity University, Bhopal, India
[c] Department of Computer Science, Government Bikram College of Commerce, Punjabi University, Patiala, Punjab 147001, India
[d] School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India
[e] Department of Computer Science & Engineering, Noida Institute of Engineering & Technology, Greater Noida, Uttar Pradesh, India

ARTICLE INFO

Article history:
Received 9 January 2021
Received in revised form 9 January 2021
Accepted 3 February 2021
Available online xxxx

Keywords:
Blockchain
Business
Cryptocurrency
Banking
Security issues
Blockchain security attack

ABSTRACT

A measured structure to hold all kinds of valuable data in a way which is impossible to forge is called a blockchain. It is fundamentally some blocks connected as a chain which contains evidence of information. This blockchain is initially used to time-stamp the documents to get rid of backdating. The most important thing is once the data is recorded can't be changed further. Each block consists of a hash, information and a hash of the block which is available previously. The data which is stored inside the block depends on the type of blockchain. A Hash distinguishes a block and every one of its substance and which is extraordinary consistently like an iris or unique finger impression. When the block is made, then the Hash is determined. Hash will change if something is changed in the block. Along these lines, hashes are utilized to identify the adjustments in the squares. The chain of the block is created with the previous block's Hash. The principal block is known as the beginning block, which doesn't hold the location of the past block. Verification of-work is to the uncommon method in the blockchain, which is utilized to moderate the gatecrashers who are changing the messages and hashes.

The main aim of this chapter is to introduce and present the concept of blockchain, its current applications in the business sector and the various threats and security issues of blockchain technology. Blockchain is emerging technology which promises uncontrollable trust issues by allowing secure and authenticated system for many fields.

Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

1. Introduction

The basic objective of blockchain is to work out a creditworthy environment amongst independent contestants during an untrustable scattered environment [5]. A blockchain system is autonomous and secure, which is used to support its peer to peer nodes, chained blocks, consensus-based ledger mechanism, self-regulated data ownership, anonymous accounts, and smart contracts [8]. Additionally, the dedicated credit procedures are required to develop blockchain systems to be creditworthy even though blockchains will provide a creditworthy environment for data-level storage operations [4].

Fig. 1 shows the blockchain architecture. Blockchains are pertinent in numerous business zones. A sensible application situation is significant for a plausible blockchain application. The application ought to be extended to investigate the restrictive blockchain includes, including and keep concocted business manages inside the advanced rather than the traditional business situations. It is empowering that various endeavours and adventures are being worked on around the globe [7,46,47].

In 2008, Nakamoto wrote a paper about accomplishing non-reversible and money based exchanges without including any outsider. Blockchain was first to use for money based exchange without outsider mediation which is behind bitcoin cryptographic money [48]. The idea was very straightforward [11]. Assume that client A needs to move cash or information to client B, the exchange is spoken to as a square which is transmitted to each hub/client of the system. At that point, the clients will confirm if

* Corresponding author.
E-mail addresses: gomathis@uk-iq.co.uk (S. Gomathi), ramya.g@vit.ac.in (R. Govindaraj).

https://doi.org/10.1016/j.matpr.2021.02.088
2214-7853/
Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

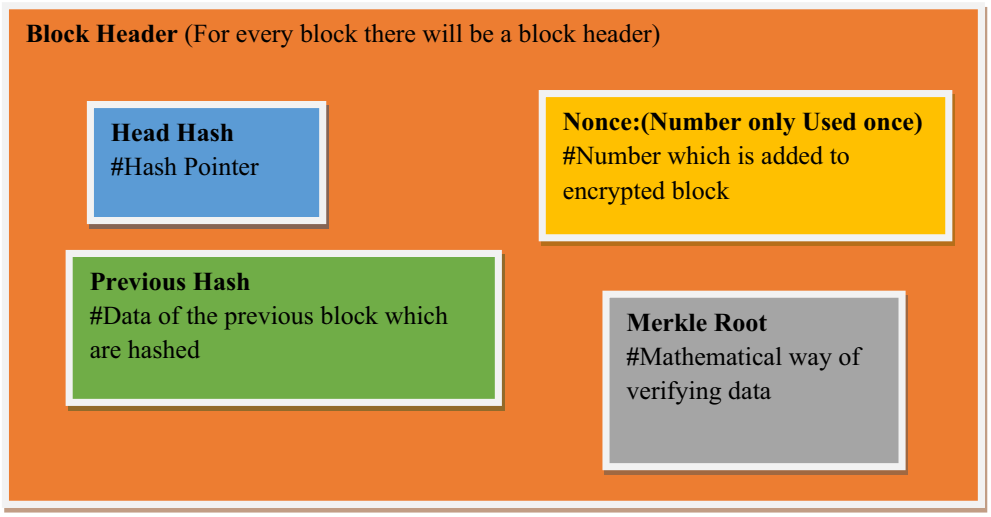

Fig. 1. Blockchain architecture.

the exchange is substantial [13]. The blockchain architecture is shown in Fig. 1.

1.1. Blockchain classification

Blockchains are ordered into Public Blockchain, Consortium Blockchain, and Private Blockchain, as shown in Fig. 2. Further, it tends to be ordered into primary chains and side chains dependent on the relationship of chains. In excess of a couple of blockchains can frame a system, and the chains in the system are interrelated so as to make the interchain [4].

1.1.1. Public blockchain

An agreement blockchain where everybody can get to it. Anyone in the blockchain topology can send exchanges and approved them. Everyone can vie for charging rights [44]. These blockchains are normally viewed as "totally decentralized", which ordinarily can utilize like the bitcoin blockchain, in which the data is totally unveiling [13].

1.1.2. Private blockchain

A blockchain in which the authorization to compose stays in a single association. The consent to peruse can be open or restricted somewhat. Inside an organization, there are extra alternatives; for

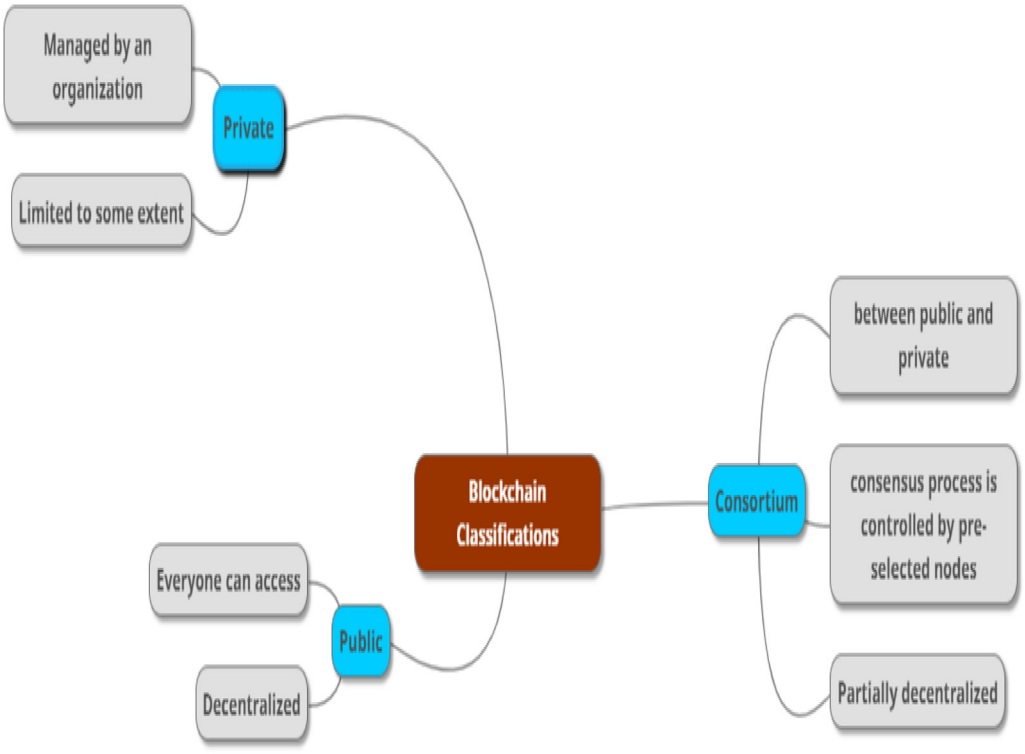

Fig. 2. Blockchain classifications.

example, database the board, review, etc. As a rule, the community isn't essential.

1.1.3. Consortium blockchain

Acts in the middle of Public Chain and Private Chain, it alludes to the blockchain whose accord procedure is constrained by prechosen hubs [8]. For instance, there is an arrangement of 15 money related organizations, every one of which oversees one hub, and at any rate 10 of which must affirm each square to be perceived as substantial and added to the chain. The option to peruse the blockchain can be available to the general population or restricted by members, or "crossbreed". Such chains can be designated "somewhat decentralized".

1.2. Components of a blockchain

Two primary segments that make up a blockchain are decentralized systems and undeniable records. The principal segment is the decentralized system. The decentralized system encourages and checks all exchanges. The decentralized blockchain arranges that the product isn't constrained to one PC framework and which can be controlled on various PC frameworks and not constrained by the administration [29].

The subsequent segment is the undeniable record in which the exchanges are overseen and recorded in a made sure about area. Unquestionable methods, if the data is entered once, can't be tinkered with similar data. The record is available just to people who are a piece of the chain. This sort of security sort is practically horrible for somebody who isn't associated with the chain to make changes or cut the data [18].

Then, there can be numerous donors associated with any blockchain; any of the supporters can administer the data that is gone into the record. Therefore, every exchange is prepared safely, with a perpetual time-stamp, which can get trying for another supporter to adjusting the record in any capacity.

2. Theoretical approach

Associations nonappearance a comprehension of how blockchain innovation can make business esteem for their separate plan of action. Besides, different security issues will be there while actualizing blockchain innovation. Concentrating on those confinements, this paper centres around the accompanying examination inquiries:

Research Query 1 (RQ1): How blockchain innovation is utilized in the business segment?

Research Query 2 (RQ2): What are the different security issues in utilizing blockchain innovation in the business segment?

A huge essential for assorted businesses assigning blockchain for the business applications is the effectiveness of the blockchain. If a business industry directs a blockchain hub to be involved with a blockchain, it is important to give the important administration abilities to the accessibility and availability of this hub.

Certain tasks begin to depend on the accessibility of a blockchain organize; these activities can be influenced by the end goal which may adversely corrupt the notoriety, authenticity and the believability of the business and its business. The hub of blockchain and the blockchain availability to the blockchain system ought to be solid and exceptionally accessible in such cases. Accordingly, it is imperative to deal with the exhibition, versatility, security, nature of-administration, and adaptation to internal failure issues in the systems. This requires the accessibility of compelling checking, configuration and adjustment capacities inside the system. What's more, the assets utilized for blockchain ought to give great adaptability capacities to help the necessary burdens. Moreover, it is essential to oversee future adaptability and execution prerequisites through appropriate and precise scope organization forms. What's more, it is critical to recognize and deal with the related dangers and give elective answers to handle issues and proceed with activities without interferences.

As each mechanical association has various sorts of organizations, activities, and accomplices, creating ad conveying blockchain arrangements is not valuable for open benchmarks which will include great flexibility for keeping up, updating, and including added application highpoints for business. Also, this will require even the fusion among blockchain chunks and other exertion applications segments inside the solitary mechanical undertaking and between shared different modern ventures. Moreover, setting the measures, protocols, and rules for novel applications to complete simple joining amid the accessible venture frameworks and the presented blockchain applications is essential.

3. Methods and materials

3.1. Goal and research questions

The key objective of this chapter to showcase the various viewpoint of blockchain used in the business industry. Blockchain has been widely used in many areas like logistic, banking, Government, etc.. This appropriate experience provides us with the wonderful opportunity to discuss the security issues that emerged over the last few years. To carry out this properly, we framed research queries,

RQ1: How blockchain innovation is utilized in the business segment? and

RQ2: What are the different security issues in utilizing blockchain innovation in the business segment?

For the principal inquire about the query, we found through writing, uses of blockchain innovation that is now utilized just as research results for other potential employments. For the subsequent inquiry, we attempted to feature security issues identified with the utilization of blockchain innovation in the business area.

3.2. Search process

Right now, sorted out writing audit technique was followed by the systems proposed by Kitchenham [8].

To cover a wide assortment of enormous related productions, we chose to look through the accompanying in the perceived and broadly utilized electronic libraries, from IEEE Xplore Digital Library, ACM Digital Library, and Springer Link. The catchphrases we attempted to look at are: "BLOCKCHAIN APPLICATIONS IN BUSINESS SECTOR", "BLOCKCHAIN SECURITY ISSUES".

The further advance is the thing that we recognized the different application fields of the papers we would apply the hunt terms. To acquire a superior and sensible inquiry of results, we checked for the catchphrase strings in the paper title, applied, and watchwords and end. We confined our interest to disseminations written in the English language and picked as a substance type simply meeting papers and journals, by excusing site pages and book parts. The standard papers were considered for this work.

The final number of papers that we assembled in the wake of evacuating copies is 250. At that point, we physically prohibited papers that their title appeared to be unessential to our examination, decreasing the papers to 100. The above method was rehashed by checking the papers' digests, arriving at 50 papers. We read the entire content of these papers, coming full circle in 25 of them so as to separate data and answer our examination addresses which are appeared in the Fig. 3.

Fig. 3. Workflow for identifying primary studies.

4. Results & discussion

The literature review which has been used is presented in this section. The results are organized by research queries. The RQ1 is tabulated in Table 1, and RQ2 in Table 2.

4.1. Research Query 1

We focused on eight various domains where blockchain is and can be applied, i.e. Healthcare, insurance, supply chain, Government, banking, personal identity, Internet of Things, cryptocurrencies, and other business sectors, which we extensively describe below. There are more domains where the blockchain can be used for efficient and secured transactions. The fields which are mentioned in table 1 is the most widely used.

4.1.1. Healthcare

One of the most touchy and basic parts of human services is the patients' information. A patient's clinical record is normally dis-

Table 1
Literature reviewed for RQ1.

Business sectors	Total number of papers
Healthcare	3
Insurance	5
Supply chain	6
Government	8
Banking	8
Personal identity	3
Internet of Things	3
Cryptocurrency	10
Other business sectors	15

Table 2
RQ2: The paper referring to the different security issues in utilizing blockchain innovation in the business segment.

Type of attack	Attack	Total number of papers
Peer-peer network-based attacks	Eclipse attack	3
	Sybil attack	1
Consensus & Ledger-based attacks	Selfish mining	3
	Mining malware	3
	51% attack	3
	Time jack attack	2
	Finney attack	3
	Race attack	1
Smart Contract-based attacks	DOA attack	3
Wallet-based attacks	Parity multisig wallet attack	1

persed over different frameworks possessed and worked by at least one social insurance suppliers. The advanced development has made the capacity to digitize understanding data into what is typically alluded to as the Electronic Medical Record (EMR)/Electronic Health Record (EHR) [1,55].

There are numerous snags in sharing EMRs among various human services suppliers and social insurance related associations because of numerous issues, including security and protection [2,50,51,53,54]. Blockchain can be utilized to empower secure EMRs and other human services data sharing among different suppliers. A new business called Gem built up a blockchain-based system for creating human services applications and a widespread social insurance information framework [27,56]. The various applications of blockchain are shown in Fig. 4.

Moreover, another new business Tierion built up a stage for human services information stockpiling. This stage additionally bolsters the verification and review procedures of human services records and procedures.

Human services is another segment where blockchain innovation could be effective. Utilizing blockchain innovation, human services associations could achieve high-information volume and high-throughput exchange handling. The creators of [3,26,34] give an answer by means of blockchain to oversee Electronic Medical Records, so that information treatment of the patients turns out to be progressively secure, private and basic. Specifically, in [34] MedRec, the main working model where the patients can allow access of their own clinical information to specialists and social insurance suppliers, ARIA, a stage which consolidates radiation, clinical and careful oncology data which can help clinicians to oversee different sorts of clinical information, create oncology-specific care plans, and screen radiation portion got by patients, and another model made by the creators are introduced as utilization of Blockchain in Healthcare.

4.1.2. Insurance

Blockchain can be utilized to help the protection of commercial centre exchanges between various customers, policyholders, and insurance agencies. Blockchain can be utilized to arrange, purchase and register protection strategies; submit and process claims, and bolster reinsurance exercises among insurance agencies. Distinctive protection arrangements can be computerized, utilizing brilliant agreements [37] which can significantly decrease organization costs. For instance, there is a high organization cost related to handling protection claims. By and large, the organization of cases can be exceptionally mind boggling forms because of contradictions and misinterpretations of the terms. Shrewd agreements can sidestep these issues by organizing protection arrangements in increasingly exact "assuming at that point" connections [41].

This takes into account the computerization of executing the terms by advanced conventions that precisely actualize the settled upon protection approaches, along these lines diminishing the exertion required and the expenses of execution. With this decrease, insurance agencies can likewise diminish the expense of their protection items and be increasingly serious about drawing in more clients. Simultaneously, it permits insurance agencies to dispatch new computerized protection items for their customers without stressing a lot over their organization's overhead and expenses. Moreover, blockchain empowers insurance agencies to be extended universally [32].

4.1.3. Supply chain

Blockchain innovation guarantees the identification of item provenance [6] and encourages the following of procedures [40]. Moreover, in [33] an item proprietorship the executives' framework is exhibited to forestall fakes once the items arrive at the end in the inventory network. Right now, of birthplace can be executed subsequent to buying and procuring an item.

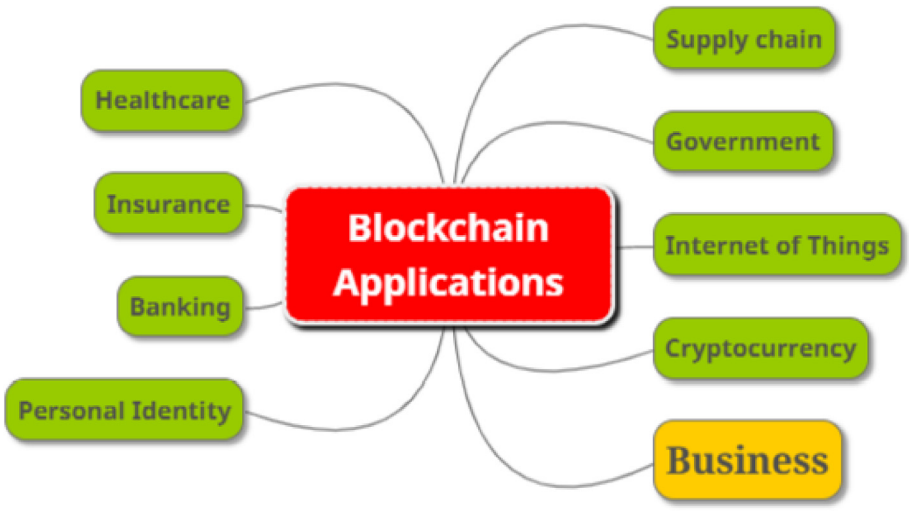

Fig. 4. Blockchain applications.

In [20] it is contended that blockchain innovation gives the security of the production network. It can pinpoint the wellspring of hazardous parts and can guarantee the reliability between store network accomplices.

Another production network based blockchain use case is Everledger [40]. Everledger utilizes blockchain innovation, which sets up an overall record for precious stones. The creators in [42] talked about that blockchain can be utilized to advance the nourishment production network. All the more specifically, they show Eaterra, a decentralized market that ties makers and customers by affirming nourishment recognizability.

4.1.4. Government

As of late, there is a monstrous development of e-taxpayer supported organizations to residents, organizations and open bodies. In [29,38,45] the utilization of blockchain innovation helps bolster framework in open part techniques, for example, Digital ID the board and secure record dealing with are talked about. The creators of [39,41] additionally suggest the development of a Blockchain for Business Applications personality the board framework based on the Ethereum blockchain and Bitcoin individually.

In [29,31,36] the creators propose a novel dispersed online lottery convention that applies systems produced for casting ballot applications to lessen security dangers while keeping away from the confided in an outsider. At long last, the utilization of blockchain is referred to in [27,30,45] where the blockchain innovation is utilized to follow lawmakers' exercises and fill in as a straightforwardness instrument to residents' hands.

4.1.5. Banking

Various financial establishments are at present testing exchanges on blockchain stages. In [19] likewise gives a careful examination of how blockchain can accomplish resource digitization, highlight point esteem move, in this way modifying the financial framework.

All the more explicitly, blockchain application could assist keeps money with encouraging remote trades and ongoing instalments by social occasion hubs in a blockchain, as opposed to having a national bank to manage instalments [4,17]. Blockchain's interruption in the financial area is featured by IBM's forecast that, "in 4 years, 66% of banks, will have business blockchain scale" [20].

4.1.6. Personal identity

Personal identity is one of the fundamental human rights as per Article 8 of the UN's convention on the Rights of the Child [44]. At its most basic level, personal identity consists of:

- First and last name.
- Date of birth.
- Nationality.
- Phone number
- Mail id
- Address
- Fingerprint
- Iris
- Other personal information.

Some form of a national identifier such as

- passport number.
- social security number (SSN)
- driving license
- PAN number
- Aadhar number
- Voter identity
- Ration card number
- Bank account number, etc.,

The significance of character can't be over-expand. Without a substantial type of ID, one can't claim property, appreciate taxpayer driven organizations, vote [49] open a financial balance, discover a house to remain or discover all-day business. Without power over one's character, it is anything but difficult to get undetectable and be not able to take an interest in the public eye essentially on the grounds that one can't demonstrate that they are who they state they are.

In any case, there is a major issue tormenting this space. This information, for example, identification number, SSN, driving permit, PAN, voter character [52] and so on., are put away in brought together servers and databases. This prompts three significant issues:

- Only these concentrated substances can give out personalities.
- These concentrated substances can misuse your own information.
- Identity burglary.
- Possibility of information misfortune

4.1.7. Internet of Things

Blockchain innovation is a kind of Distributed Ledger Technology, has been familiarizing enormous thought in territories past its digital currency roots since pretty much 2014: Blockchain and along these lines the Blockchain & account, Internet of Things (IoT), Blockchain & cybersecurity, coordinations and Blockchain, and so forth., The innovation behind sensors and savvy chips is developing quickly, making them continuously convenient and relevant for constant correspondences with blockchain ledgers [10].

The mix of IoT and blockchain innovation has wide potential for the production of a commercial centre of administrations among gadgets and gives organizations the opportunity to make an incentive from gathered information. The developing number of rising blockchain conventions, associations, and IoT gadget suppliers as of now demonstrates that there's a genuine fit blockchain inside the IoT division [21,63,64].

Moreover, blockchain is frequently wont to empower vitality exchanging inside the Industrial Internet of Things [23]. Blockchain empowers for improved force supply dealings and understandings between customers and suppliers in diverse ventures. This may help diminish the whole creation expenses of those businesses, along these lines, making them progressively flexible and serious inside testing market situations. For the most part, using blockchain for vitality related applications can possibly downsize vitality costs [23] likewise as increment flexibility. Researchers are doing various optimization algorithms for different datasets and applications[57-61,66-68]

4.1.8. Cryptocurrency

Digital currencies establish a significant application region for blockchain innovation. Here, we predominantly centred around the utilization of cryptographic forms of money as an instalment arrangement. In [2] the creators break down the way that probably the most well known cryptographic forms of money, for example, Bitcoin, Ethereum, Litecoin work. The creators additionally demonstrated an evaluation among these advanced monetary standards, calculations, in regards to their coin limit, beginning and current square rewards and meant square time.

Cryptographic forms of money could likewise be utilized as an impetus instrument for proposing thoughts in cross-utilitarian gathering ventures. Towards this, everything that produces a data thing may make a savvy contract which will acknowledge as an info a measure of virtual, computerized coins and will yield an instalment receipt.

The execution of a bitcoin-based network cryptographic money is assigned in [33]. The proposed model incorporates network subsidize, and the individuals may take credits that are endorsed by the vote of the network individuals.

4.1.9. Other business sectors

Notwithstanding the applications talked about before, there are other helpful applications in areas like development and media transmission enterprises. In the development business, blockchain can be utilized for developing executives by upgrading the present procedures of agreement creation, enrollment, checking, control, and executives.

Likewise, blockchain administrations can bolster better development inventory networks the executives, and development hardware renting [35]. In the media transmission industry, blockchain can improve media transmission administrations on the board [36].

Blockchain applications can progress contract the board, recognizability, and administration forms in the media transmission industry. Besides, applying blockchain will be a great support to Industry 4.0 claims [39] as they, as a rule, need to incorporate a few frameworks and segments that may not generally be possessed by a solitary substance. Secured, controlled, and trusted procedure for industries can be achieved through blockchain. [28,62].

5. Security issues in blockchain

Fig. 5 shows the blockchain security attacks which are classified into four: Consensus & ledger-based attacks, wallet based attacks, peer-to-peer network-based attack and smart contract-based attacks [50,65].

5.1. Peer-to-Peer Network-based attacks

5.1.1. Eclipse assault

A hub will rely upon the "x" number of hubs chose to utilize a Peer determination methodology to have its perspective on the disseminated record [14].

5.1.2. Sybil assault

While the Eclipse assault is tied in with obscuring a client's perspective on truth record, the Sybil assault focuses on the whole system. In a Sybil assault, an aggressor will flood the system with countless hubs with a pseudonymous personality and attempt to impact the system [17]. These hubs, however seeming like random people, are worked by one administrator at the back. Right now, the objective isn't to target one client, however various hubs or systems overall, and create a fork in the record if conceivable, permitting the aggressor to shape twofold spending and different assaults [15,16].

5.2. Consensus mechanism and Mining-based attacks

5.2.1. Selfish mining assault

Several blockchains believe the lengthiest chain to be the cutting-edge adaptation of the record. [44]

5.2.2. Mining malware

Malware utilizes the registering intensity of clueless casualties' PCs to dig digital currencies for programmers. China revealed that more than 1,000,000 PCs were contaminated through mining malware and facilitated aggressors mine very 28 million tokens of changed cryptographic forms of money.

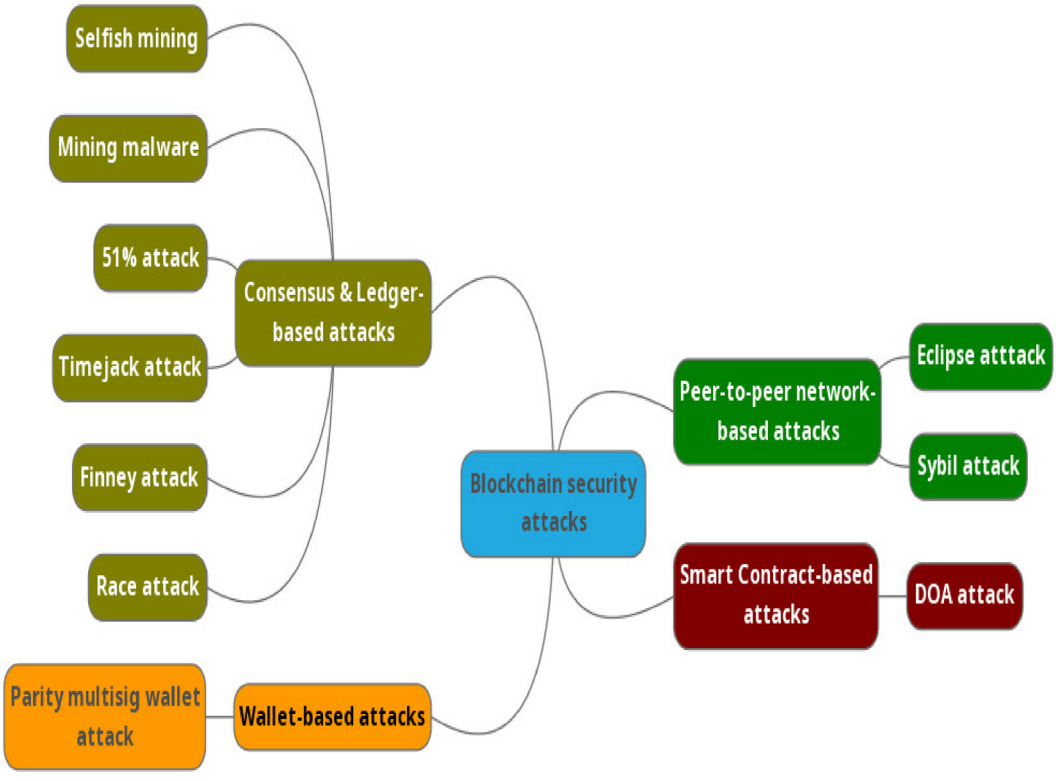

Fig. 5. Blockchain security attacks.

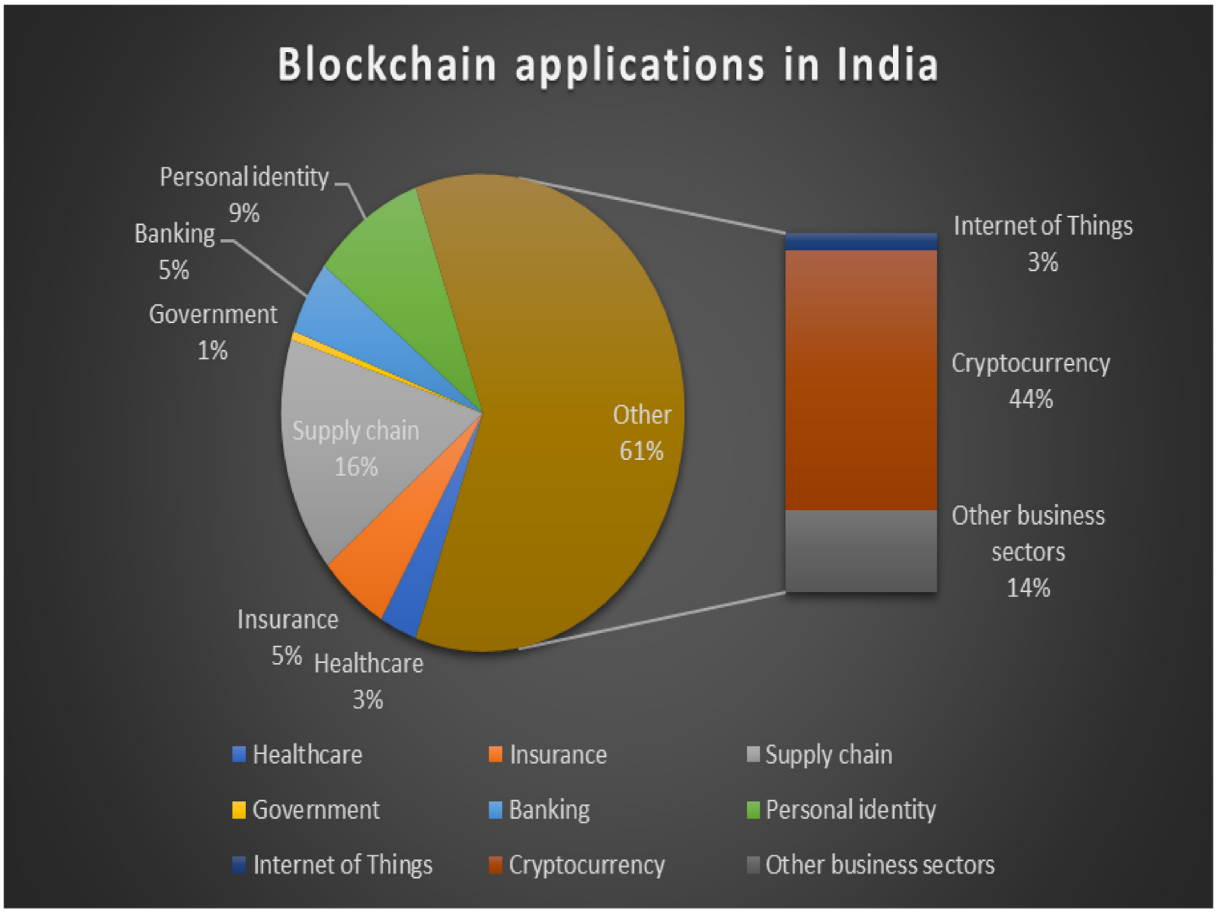

Fig. 6. Bar of the pie chart to depict the blockchain applications in India.

5.2.3. 51% assault

This assault is attainable when an excavator or a gaggle of digger's controls 51% or a greater amount of the mining intensity of the blockchain organize. In spite of the fact that it's extremely hard to occur for monster organizes, the probability of a 51% assault is higher in little systems. When a gathering has greater part authority over exchanges on a blockchain arrange, it can forestall explicit transactions or even converse more established exchanges.

5.2.4. Time jack assault

Nodes in specific blockchain systems like Bitcoin rely upon interior planning got from the average time announced by its companion hubs. For instance, you rely upon your companions to know the time. Let us state an aggressor figure out how to place a lot of vindictive individuals in your companions' rundown; at that point, he can control your time [35].

The initial step to the current assaults is regularly an Eclipse assault on the real hub. When this assault is finished on a real centre, at that point, the real hub won't acknowledge hinders from the specific system because the time-stamp of the squares won't be in accordance with its time-stamp [39].

5.2.5. Finney attack

A Finney attack is a duplicitous double-spend outbreak that entails the involvement of a miner once a block has been extracted. The risk in Finney attack cannot be eradicated irrespective of the protections engaged by the business, but the involvement of a miner is compulsory and a definite order of actions essential to occur. [35].

5.2.6. Race assault

This assault is a minor variety of the Finney assault. It is simpler for the assailant to dispatch the assault in the event that he is straightforwardly associated with the dealer's hub. This would give the trader a figment that his exchange is the first, yet that is never submitted to the blockchain arrange by the aggressor [39].

5.3. Smart Contract-based attacks

Brilliant agreements are mechanized agreements, which execute exchanges in a settled upon route between members, with contributions from this present reality and without intercession from any agents [21]. So once began, a reasonable agreement can't be halted. When the exchange is finished and composed into the blockchain, it gets total. This gives an assurance to members of profits dependent on their exhibition, as settled upon while entering the agreement [22,36].

5.3.1. The DAO assault

The most significant misuse inside the historical backdrop of cryptographic forms of money is that the Decentralized Autonomous Organization hack. DAO was a deciding element of an Ethereum. Was predestined to function like an undertaking capital fund for the decentralized and crypto space. The deficiency of a centralized specialist reduced costs, and it offers more control and entree to the investors.

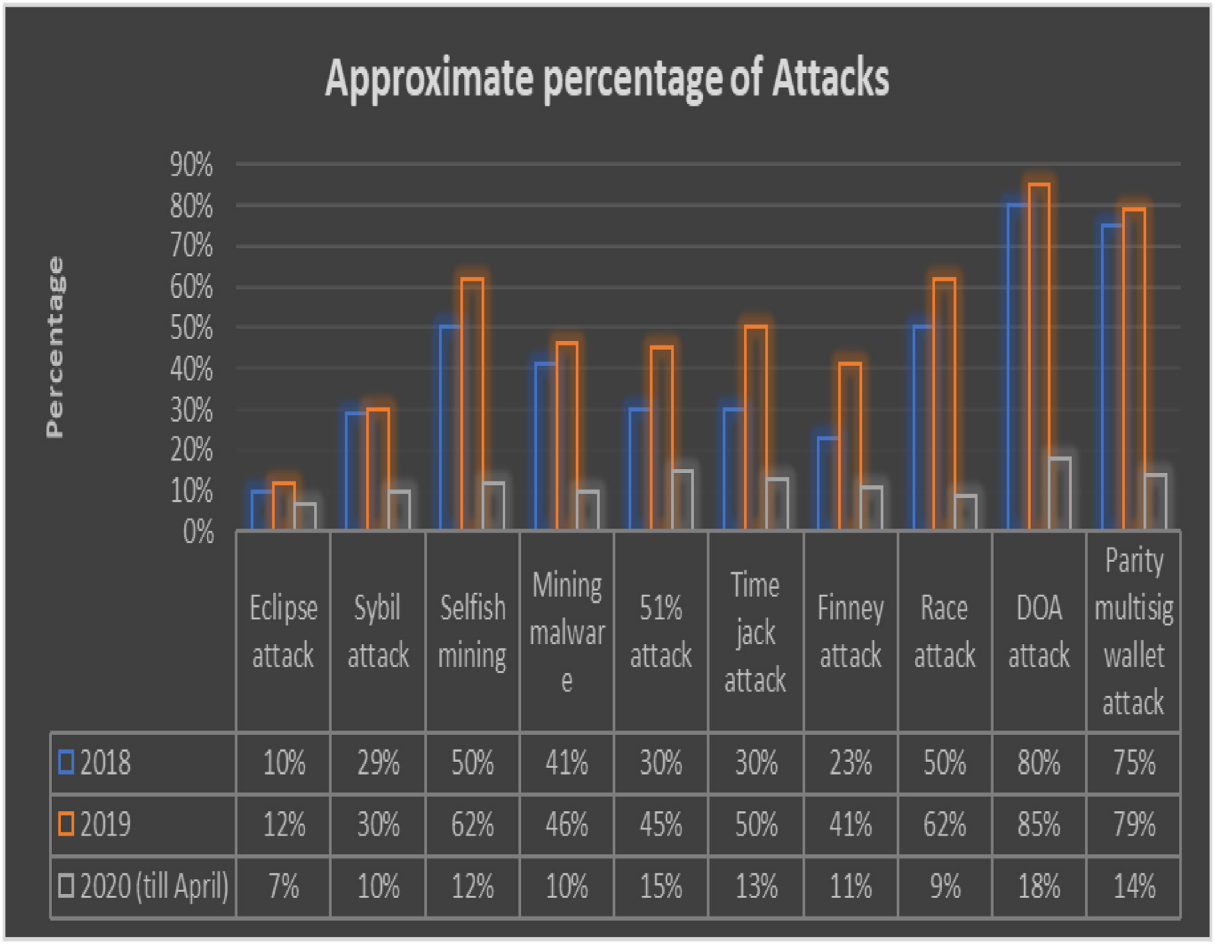

Fig. 7. The bar graph to show the approximate percentage of attacks happened from 2018 till 2020 (till April).

5.4. Wallet-based attack

5.4.1. Parity Multisig wallet attack

A weakness assault with the equality customer wallet hacked by a trespasser prompting holding from 600,000 Ether ($77 million today). Wallet contracts are extra rationale than can be based on client wallets for standard computerized instalments. To decrease the gas or exchange charges, the equality Multisig wallet usefulness (Multisig wallet resembles a shared service in the keeping money with different proprietors) utilized a brought together Library contract. Yet, they left some basic capacities open, prompting a weakness, which was abused by the aggressor [28].

6. Results & discussion

Blockchain technology is engendering substantial attention transversely an extensive range of businesses in India. As the blockchain field and its applications grow, industry privileged leaders are modifying and adapting the technology to suits the blockchain's multiple use cases. In India, Blockchain adoption has seen since 2016.

The monetary effect of blockchain is developing exponentially with time no matter the business is mentioned. It is not only the setup organizations and endeavours. However, even startups are concentrating on turning into a bit of Blockchain economy - a symbol of which are the bits of data recorded in Fig. 6, which shows the blockchain applications in India.

The applications of blockchain have been obtained and analyzed from the various works of literature and findings. A small survey has been undergone to draw the graph of the major applications of Blockchain in India, and the attacks happened over two years.

In this Fig. 6, it is clear that Cryptocurrency and other business sectors are using blockchain for the transactions than other various fields. The purpose of the blockchain is the safe and secured transfer of digital money.

Fig. 7 shows that a DOA attack is having the highest percentage than other attacks. Most of the transactions are tend to hack by a hacker or hacktivist to deny the service. The data is obtained from various sources and survey. The types of attacks are already discussed in the previous sections.

Even though India is silent at the budding stage in discovering Blockchain technology and its various applications, many startups are ready to adopt the blockchain technology, and few startup businesses are stepping backwards in fear of facing the risks and security factors involved in blockchain technology.

Need is more but the supply is less, is suited for blockchain technology and its adoption. Every new technology has to face the risks and threats is also true for blockchain too.

7. Conclusion

Blockchain exhibited its convenience through the broad utilization of cryptographic forms of money and its help for the tasks expected to accomplish computerized cash. In any case, similar

highlights are capable of empowering and bolstering further recent applications in numerous spaces. A wide scope of modern spaces is beginning to embrace or consider receiving blockchain to encourage their activities in order to streamline forms, improving security and information sharing, expanding efficiency and eventually diminishing expenses to increase an upper hand.

The fundamental empowering agents for utilizing blockchain in the fields like healthcare, supply chain and the fields which are discussed in this chapter are the arrangement of disseminated security, advanced characters, savvy contracts, and reduced scale metering through the conveyed blockchain records. Therefore, applications in the financial, vitality, coordination, social insurance, and assembling spaces are developing and ending up being extremely helpful. Right now, it showed the conceivable outcomes and benefits of blockchain by looking over changed modern areas and the applications utilized in these spaces. We additionally featured the principle benefits of these applications.

Numerous articles have been overviewed through which we comprehend that most analysts and clients focused on the blockchain innovation application and its uses and which demonstrates less significance to the blockchain security dangers. The eight application zones and the conceivable programming which can be utilized are focussed alongside the security gives that have been examined—crafted by this paper can mindful of the specialist and the designers on blockchain security assaults and dangers.

CRediT authorship contribution statement

S. Gomathi: conceptualize the work. **Mukesh Soni:** wrote the paper. **Gaurav Dhiman:** validated the work. **Ramya Govindaraj:** suggested the methodology. **Pankaj Kumar:** formal analyzed the work.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. Al Omar, M.S. Rahman, A. Basu, S. Kiyomoto, December). Medibchain: A blockchain-based privacy-preserving platform for healthcare data, in: International conference on security, privacy and anonymity in computation, communication and storage, Springer, Cham, 2017, pp. 534–543.

[2] Alboaie, S., Kosovan, D.: Private data system enabling self-sovereign storage managed by executable choreographies. In: Chen, L.Y., Reiser, H.P. (eds.) DAIS 2017. LNCS, vol. 10320, pp. 83–98. Springer, Cham (2017). 10.1007/978-3-319-59665-5_6

[3] G. Baralla et al., A blockchain-based system to ensure transparency and reliability in the food supply chain, European conference on parallel processing, Springer, Cham, 2018.

[4] Bashir, M., Strickland, B., Bohr, J.: What motivates people to use bitcoin? In: Spiro, E., Ahn, Y.-Y. (eds.) Soc. Info 2016. LNCS, vol. 10047, pp. 347–367. Springer, Cham (2016). 10.1007/978-3-319-47874-6_25

[5] O. Bermeo-Almeida et al., Blockchain in agriculture: A systematic literature review, Springer, Cham, 2018.

[6] Bettín-Díaz, Rafael, Alix E. Rojas, and Camilo Mejía-Moncayo. "Methodological approach to the definition of a blockchain system for the food industry supply chain traceability." International Conference on Computational Science and Its Applications. Springer, Cham, 2018.

[7] Bhardwaj, S., Kaushik, M.: Blockchain—technology to drive the future. In: Satapathy, S.C., Bhateja, V., Das, S. (eds.) Smart Computing and Informatics. SIST, vol. 78, pp. 263–271. Springer, Singapore (2018). 10.1007/978-3-319-59427-9_76.

[8] D.Mingxiao, M.Xiaofeng, Z.Zhe, W.Xiangwei, and C.Qijun, "A review on consensus algorithm of blockchain," in Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC), Oct. 2017, pp. 2567–2572.

[10] E. C. Ferrer, "The blockchain: A new framework for robotic swarm systems," in Proc. Future Technol. Conf. Cham, Switzerland: Springer, 2018, pp. 1037–1058.

[11] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in Proc. 17th Int. Conf. Smart Technol. (IEEE EUROCON) Jul. 2017, pp. 763–768.

[13] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Commun. Surveys Tuts. 18 (3) (2016) 2084–2123.

[14] G. Karame, "On the security and scalability of bitcoin's blockchain," in Proc. ACM SIGSAC Conf. Comput. Commun. Security. (CCS), New York, NY, USA, 2016, pp. 1861–1862.

[15] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing Privacy: Using blockchain to protect personal data," inProc. IEEESecur. Privacy Workshops (SPW), May 2015, pp. 180–184.

[16] M. Soni and A. Jain, "Secure Communication and Implementation Technique for Sybil Attack in Vehicular Ad-Hoc Networks," 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2018, pp. 539-543, doi: 10.1109/ICCMC.2018.8487887.

[17] Grumbach, S., Riemann, R.: Distributed random process for a large-scale peer-to-peer lottery. In: Chen, L.Y., Reiser, H.P. (eds.) DAIS 2017. LNCS, vol. 10320, pp. 34–48. Springer, Cham (2017). 10.1007/978-3-319-59665-5_3 29.

[18] J. Liu, P. Jiang, and J. Leng, "A framework of credit assurance mechanism for manufacturing services under social manufacturing context," in Proc. 13th IEEE Conf. Autom. Sci. Eng. (CASE), Aug. 2017, pp. 36–40.

[19] J. Wang, P. Wu, X. Wang, W. Shou, The outlook of blockchain technology for construction engineering management, Front. Eng. Manage. 4 (1) (2017) 67–75.

[20] Jaoude, Joe Abou, and Raafat George Saade. "Blockchain applications–usage in different domains." IEEE Access 7 (2019): 45360-45381.

[21] K. Christidisand M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[22] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contract smarter," inProc.ACM SIGSAC Conf. Comput. Commun. Secur., 2016, pp. 254–269.

[23] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA), Nov./Dec. 2016, pp. 1–6.

[26] Mettler, M.: Blockchain technology in healthcare: the revolution starts here. In: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (2016).

[27] Munsing, E., Mather, J., Moura, S.: Blockchains for decentralized optimization of energy resources in microgrid networks. In: 2017 IEEE Conference on Control Technology and Applications (CCTA) (2017). 10.1109/CCTA.2017.8062773

[28] N. Mohamed and J. Al-Jaroodi, "Applying blockchain in industry 4.0 applications," in Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC), Las Vegas, NV, USA, 2019, pp. 852–858. DOI: 10.1109/CCWC.2019.8666558.

[29] Ølnes, S.: Beyond bitcoin enabling smart Government using blockchain technology. In: Scholl, H.J., Glassey, O., Janssen, M., Klievink, B., Lindgren, I., Parycek, P., Tambouris, E., Wimmer, Maria A., Janowski, T., Sá Soares, D. (eds.) EGOVIS 2016. LNCS, vol. 9820, pp. 253–264. Springer, Cham (2016). 10.1007/978-3-319-44421-5_20 27.

[30] P. Chakraborty, R. Shahriyar, A. Iqbal, and A. Bosu, "Understanding the software development practices of blockchain projects: A survey," in Proc.12thACM/IEEE Int. Symp. Empirical Softw. Eng. Meas. NewYork, NY, USA: ACM, 2018, p. 28.

[31] Pass, Rafael, Lior Seeman, and Abhi Shelat. "Analysis of the blockchain protocol in asynchronous networks." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2017.

[32] Rimba, P., Tran, A., Weber, I., Staples, M., Ponomarev, A., Xu, X.: Comparing blockchain and cloud services for business process execution. In: 2017 IEEE International Conference on Software Architecture (ICSA) (2017). 10.1109/ICSA.2017.44

[33] S. Underwood, Blockchain beyond Bitcoin, Commun. ACM 59 (11) (2016) 15–17.

[34] Shae, Z., Tsai, J.: On the design of a blockchain platform for clinical trial and precision medicine. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (2017). 10.1109/ICDCS.2017.61

[35] Suhaliana bt Abd Halim, N., Rahman, M.A., Azad, S., Kabir, M.N.: Blockchain security hole: issues and solutions. In: Saeed, F., Gazem, N., Patnaik, S., Saed Balaid, A.S., Mohammed, F. (eds.) IRICT 2017. LNDECT, vol. 5, pp. 739–746. Springer, Cham (2018). 10.1007/978-3-319-59427-9_76

[36] V. Morabito, Smart contracts and licensing, in: B.I.T. Blockchain (Ed.), Cham, Springer, Switzerland, 2017, pp. 101–124.

[37] Vo, H., Mehedy, L., Mohania, M., Abebe, E.: Blockchain-based data management and analytics for micro-insurance applications. In: Proceedings of the 2017 ACM on Conference on Information and Knowledge Management - CIKM 2017 (2017).

[38] Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs BFT replication." International workshop on open problems in network security. Springer, Cham, 2015.

[39] W. Meng, E.W. Tischhauser, Q. Wang, Y. Wang, J. Han, When intrusion detection meets blockchain technology: a review, IEEE Access 6 (2018) 10179–10188.

[40] Wang, Shuaian, and Xiaobo Qu. "Blockchain applications in shipping, transportation, logistics, and supply chain." Smart Transportation Systems, 2019. Springer, Singapore, 2019. 225-231.

[41] Weber, Ingo, et al. "Untrusted business process monitoring and execution using blockchain." International Conference on Business Process Management. Springer, Cham, 2016.
[42] Wijaya, D.A., Liu, J.K., Suwarsono, D.A., Zhang, P.: A new blockchain-based value-added tax system. In: Okamoto, T., Yu, Y., Au, M.H., Li, Y. (eds.) ProvSec 2017. LNCS, vol. 10592, pp. 471–486. Springer, Cham (2017). 10.1007/978-3-319-68637-0_28 30.
[44] Xu, Y., Li, Q., Min, X., Cui, L., Xiao, Z., Kong, L.: E-commerce blockchain consensus mechanism for supporting the high-throughput and real-time transaction. In: Wang, S., Zhou, A. (eds.) CollaborateCom 2016. LNICST, vol. 201, pp. 490–496. Springer, Cham (2017). 10.1007/978-3-319-59288-6_46.
[45] X. Xu, I. Weber, M. Staples, Model-Driven Engineering for Blockchain Applications, in: Architecture for Blockchain Applications, Springer, Cham, 2019, pp. 149–172.
[46] X. Xu, I. Weber, M. Staples, Design process for applications on blockchain, in: Architecture for Blockchain Applications, Springer, Cham, 2019, pp. 93–111.
[47] Rajit Nair, Sweta Gupta, Mukesh Soni, Piyush Kumar Shukla, Gaurav Dhiman, "An approach to minimize the energy consumption during blockchain transaction",Materials Today: Proceedings,2020,ISSN 2214-7853, 10.1016/j.matpr.2020.10.361.
[48] Y. Yuan, F.Y. Wang, Blockchain and cryptocurrencies: model, techniques, and applications, IEEE Trans. Syst. Man Cybernet. Syst. 48 (9) (2018) 1421–1428.
[49] Zhao, Z., Chan, T.-H.H.: How to vote privately using bitcoin. In: Qing, S., Okamoto, E., Kim, K., Liu, D. (eds.) ICICS 2015. LNCS, vol. 9543, pp. 82–96. Springer, Cham (2016). 10.1007/978-3-319-29814-6_8.
[50] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE.
[51] M. Soni and D. Kumar, "Wavelet Based Digital Watermarking Scheme for Medical Images," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 2020, pp. 403-407, doi: 10.1109/CICN49253.2020.9242626.
[52] Y. Zhu, Z. Zeng, C. Lv, Anonymous Voting Scheme for Boardroom with Blockchain, Int. J. Perform. Eng. 14 (2018) 2414.
[53] G. Arora, P. L. Pavani, R. Kohli and V. Bibhu, "Multimodal biometrics for improvised security," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 1-5, doi: 10.1109/ICICCS.2016.7542312.
[54] D. P. Jha, R. Kohli and A. Gupta, "Proposed encryption algorithm for data security using matrix properties," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 86-90, doi: 10.1109/ICICCS.2016.7542316.
[55] Mukesh Soni, Yash Barot, S. Gomathi "A review on Privacy-Preserving Data Preprocessing", Journal of Cybersecurity and Information Management, Volume 4, Issue 2, Page 16-30.
[56] Gaurav Dhiman, An Innovative Approach for Face Recognition Using Raspberry Pi, Artif. Intell. Evol. (2020) 103–108.
[57] Satnam Kaur, Lalit K. Awasthi, A.L. Sangal, Gaurav Dhiman, Tunicate Swarm Algorithm: A new bio-inspired based metaheuristic paradigm for global optimization, Eng. Appl. Artif. Intell. 90 (2020) 103541.
[58] Dehghani, Mohammad, Zeinab Montazeri, Gaurav Dhiman, O. P. Malik, Ruben Morales-Menendez, Ricardo A. Ramirez-Mendoza, Ali Dehghani, Josep M. Guerrero, and Lizeth Parra-Arroyo. "A Spring Search Algorithm Applied to Engineering Optimization Problems." Applied Sciences 10, no. 18 (2020): 6173.
[59] Gaurav Dhiman, Krishna Kant Singh, Mukesh Soni, Atulya Nagar, Mohammad Dehghani, Adam Slowik, Amandeep Kaur, Ashutosh Sharma, Essam H. Houssein, Korhan Cengiz, MOSOA: A new multi-objective seagull optimization algorithm, Expert Systems with Applications, 2020,114150,ISSN 0957-4174, 10.1016/j.eswa.2020.114150.
[60] Dhiman, Gaurav, Meenakshi Garg, Atulya K. Nagar, Vijay Kumar, and Mohammad Dehghani. "A novel algorithm for global optimization: rat swarm optimizer." Journal of Ambient Intelligence and Humanized Computing (2020): 1.
[61] Yuvaraj, N., K. Srihari, S. Chandragandhi, R. Arshath Raja, Gaurav Dhiman, and Amandeep Kaur. "Analysis of protein-ligand interactions of SARS-Cov-2 against selective drug using deep neural networks." Big Data Mining and Analytics (2020): 1.
[62] Sudhakar Sengan N.Satheesh , Ganga Rama Koteswara Rao , Subrata Chowdhury ,Kolla Bhanu Prakash4, " Blockchain - Facilitated IoT Built Cleverer Home with Unrestricted Validation Arrangement", International Journal of Advanced Trends in Computer Science and Engineering, volume-9, Page 5398 - 5405.
[63] Ramya Govindraj Subrata Chowdhury, P. Mayilvahananan, " Health Machine Sensors Network Controlling and Generating Trust Count in the Servers Platform through IoT", International Journal of Recent Technology and Engineering (IJRTE), Volume-7, page 880-884.
[64] Ramya Govindaraj, SubrataChowdhury, Dr.P.Mayilvahahnan, " Defiance and Contention braced in IoT for the TherapeuticSensor Systems Inquisitions", International Journal of Management, Technology And Engineering, Volume-8, page-12.
[65] A. Anand, A. Raj, R. Kohli and V. Bibhu, "Proposed symmetric key cryptography algorithm for data security," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 159-162, doi: 10.1109/ICICCS.2016.7542294.
[66] Gaurav Dhiman, Amandeep Kaur, HKn-RVEA: a novel many-objective evolutionary algorithm for car side impact bar crashworthiness problem, Int. J. Vehicle Design 80 (2–4) (2019) 257–284.
[67] Gaurav Dhiman, MOSHEPO: a hybrid multi-objective approach to solve economic load dispatch and micro grid problems, Appl. Intell. 50 (1) (2020) 119–137.
[68] Garg, Meenakshi, and Gaurav Dhiman. "A novel content based image retrieval approach for classification using glcm features and texture fused lbp variants." Neural Comput Appl (2020).

Further reading

[9] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F.: How blockchain could empower e-health: an application for radiation oncology. In: Begoli, E., Wang, F., Luo, G. (eds.) DMAH 2017. LNCS, vol. 10494, pp. 3–6. Springer, Cham (2017). 10.1007/978-3-319-67186-4_1 26.
[12] ElMessiry, Magdi, and Adel ElMessiry. "Blockchain framework for the textile supply chain management." International Conference on Blockchain. Springer, Cham, 2018.
[24] M. Conti, S. Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Commun. Surveys Tuts. 20 (4) (2018) 3416–3452.
[25] J. Mendling et al., Blockchains for business process management-challenges and opportunities, ACM Trans. Manage. Inform. Syst. (TMIS) 9 (1) (2018) 1–16.
[43] Wu, L., Meng, K., Xu, S., Li, S., Ding, M., Suo, Y.: Democratic centralism: a hybrid blockchain architecture and its applications in energy internet. In: 2017 IEEE International Conference on Energy Internet (ICEI) (2017). 10.1109/ICEI.2017.38.