Cluster Computing (2019) 22:S14743–S14757
https://doi.org/10.1007/s10586-018-2387-5

Analysis of Blockchain technology: pros, cons and SWOT

M. Niranjanamurthy[1] · B. N. Nithya[1] · S. Jagannatha[1]

Received: 30 January 2018 / Revised: 24 February 2018 / Accepted: 6 March 2018 / Published online: 19 March 2018

Abstract
Any online transaction that involves digital money is a bit of a challenge these days with the rising threats of hackers trying to steal bank details posted online. This leads to the invention of various kinds of crypto-currency, Bitcoin being one of them. The technology behind using the Bitcoin is popularly called as Blockchain. Blockchain is a digitized, de-centralized, public ledger of all crypto-currency transaction/s. Blockchain tries to create and share all the online transactions, stored in a distributed ledger, as a data structure on a network of computers. It validates the transactions using peer-to-peer network of computers. It allows users to make and verify transactions immediately without a central authority. Blockchain is a transaction database which contains information about all the transactions ever executed in the past and works on Bitcoin protocol. In this analysis paper we discussed what is Blockchain?, SWOT analysis of BC, Types of BC and how Blockchain works along with its advantages and disadvantages.

Keywords Blockchain · Structure of Blockchain · Types of Blockchain · SWOT analysis · Pros and cons of Blockchain

1 Introduction

Any crypto currency transaction that takes place in these days has to be transparent. There is a lot of private data in these transactions that can cause huge damage if fallen in the wrong hands. The technology both the hardware and software that is associated with these transactions also have to be taken care of as failure of any one of these components would lead to the failure of a transaction that involves money. A Blockchain can be considered as a digitalized public ledger that would record all the digital transactions in a chronological order or as "Completed Transaction Blocks" as a data structure and stores this in a distributed manner across a network. This ledger would be available for anyone to download who can connect with this network. The Blockchains are implemented using three major technologies: (1) Private Key Cryptography, (2) Peer to Peer Network (3) Program (the Blockchains protocol). The major advantage of a Blockchain is its usage to distributed computing technology that helps it overcome problems of load sharing. Distributed computing technology also supports graceful degradation that makes Blockchain technology very reliable to store sensitive information like medical records, management activities, transaction processing, documenting derivation, food traceability or voting.

Blockchain technologies contains Cryptography, mathematics, Algorithm and economic model, combining peer-to-peer networks and using distributed consensus algorithm to solve traditional distributed database synchronize problem, it's an integrated multi- field infrastructure construction. The Blockchain technologies are generally composed of six key elements.

(1) Decentralized
(2) Transparent
(3) Open Source
(4) Autonomy
(5) Immutable
(6) Anonymity

(1) *Decentralized* the basic feature of Blockchain, which means that Blockchain doesn't have to rely on centralized node anymore, the data can be recorded, stored and updated on multiple systems.
(2) *Transparent* the data's record by Blockchain system is transparent to each node, each of these nodes can

✉ M. Niranjanamurthy
niruhsd@gmail.com; mniruhsd@gmail.com

[1] Department of Computer Applications, M S Ramaiah Institute of Technology, Bangalore, Karnataka 560054, India

further update the data as well which makes it transparent and trustworthy.

(3) *Open source* most Blockchain system is open to everyone, record can be check publicly and people can also use Blockchain technologies to create any applications they want.

(4) *Autonomy* because of the base of consensus, every node on the Blockchain system can transfer or update data safely, the idea is to trust form single person to the whole system, and no one can intervene it.

(5) Immutable: Any records will be reserved forever, and can't be changed unless someone who has control more than 51% node in the same time.

(6) *Secrecy* Blockchain technologies solved the trust problem between node to node, so data transfer or even transaction can be anonymous, we only need to know the person's Blockchain address to do so [1].

The Structure of Blockchain: a block consists of the block header and the block body as shown in Fig. 1. In particular, the block header includes:

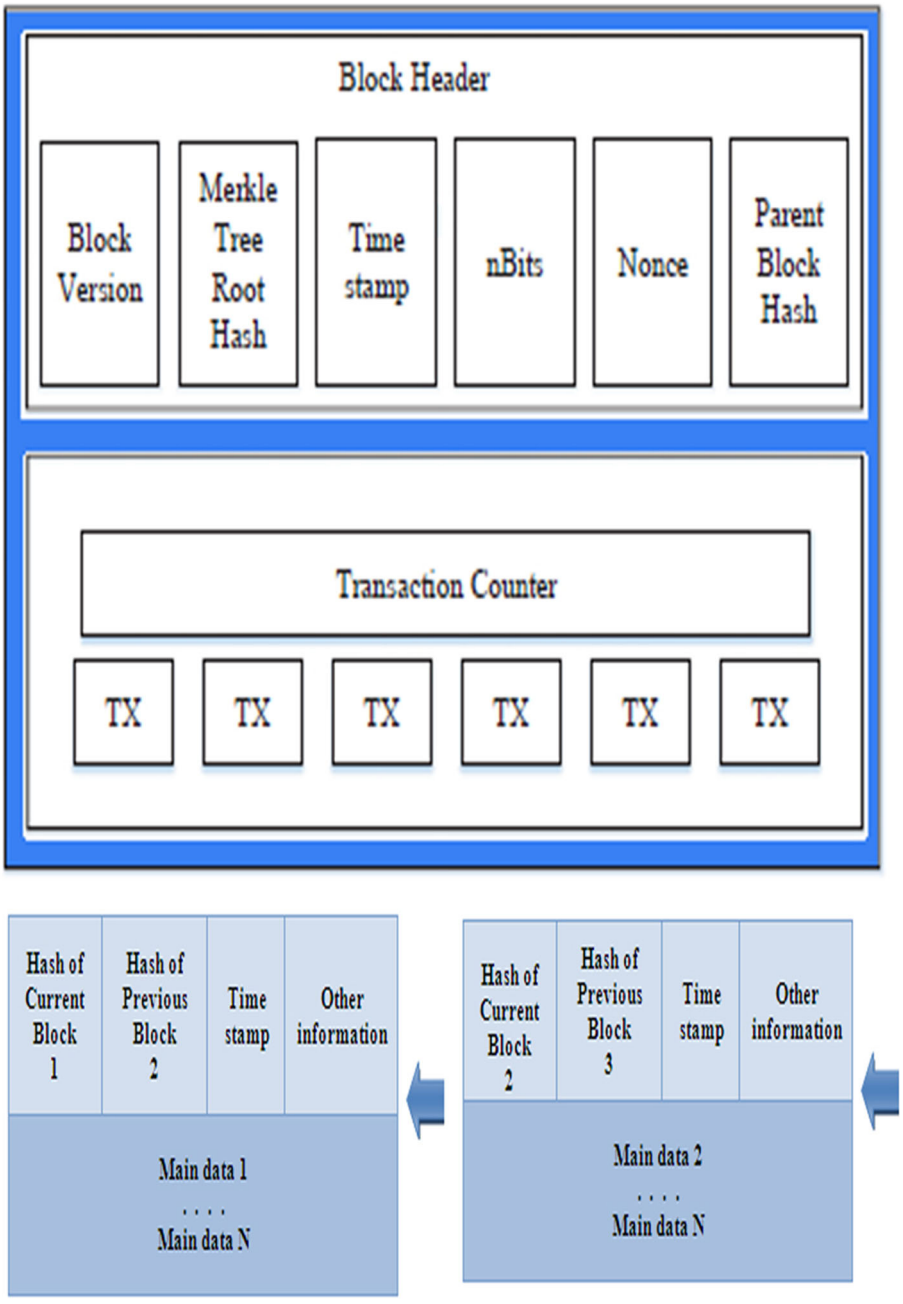


Fig. 1 Structure of Blockchain. **a** Blockchain which consists of a continuous sequence of blocks

(i) *Block version* indicates which set of block validation rules to follow.
(ii) *Merkle- tree root hash* the hash value of all the transactions in the block.
(iii) *Timestamp* current time as seconds in universal time since January 1, 1970.
(iv) *nBits* target threshold of a valid block hash.
(v) *Nonce* a 4-byte field, which usually starts with 0 and increases for every hash calculation.
(vi) *Parent block hash* a 256-bit hash values that point to the previous block.

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate and authenticate transactions. Digital signature based on asymmetric cryptography is used in an untrustworthy environment [2].

2 Related work

The Blockchain, originally implemented for the virtual crypto currency, Bitcoin, is a novel peer-to-peer approach which links a sequence of transactions or events together in a way that makes them immutable [3].

Blockchain is a transaction database which contains information about all the transactions ever executed in the past and works on Bitcoin protocol. It creates a digital ledger of transactions and allows all the participants on network to edit the ledger in a secured way which is shared over distributed network of the computers [4].

The amount of data in our world is rapidly increasing. According to a recent report, it is estimated that 20% of the world's data has been collected in past couple of years. Facebook, the largest online social network, collected 300 peta bytes of personal data since its inception. MIT Media Lab provided a mechanism called "Decentralizing Privacy" which could protect personal data. A Blockchain is something like a ledger in which all transactions have been recorded, and it is shared by the participants of a Bitcoin network [5].

Trust is the most important issue of the Blockchain. The interactions between the nodes within the network ensure that trust is achieved. The participants of Blockchain network rely on the Blockchain network itself rather than relying on trusted third-party organizations to facilitate transactions. These five properties (immutability, non-repudiation, integrity, transparency, and equal rights) are the main properties supported in existing Blockchains [6].

Research Questions (A) How to categorize the bugs that appear in Blockchain system? The answer to this question can help us understand the loopholes in the Blockchain systems. The categorization of the bugs should be done in such a way that the most frequent bugs should be put under one category so that more work and effort could be put in addressing that category. (B) How frequently are similar bugs coming up in different Blockchain projects? The various Blockchain projects are developed as solutions to different problems that work under different environments. Are there any bugs that come up under the different environments and technologies? If there is some frequent occurrence of the bugs and they show similar trends across projects then the categorization of these bugs becomes easy based on their characteristics [7].

Security and reliability "Software Security Guidelines span every phase of the software development lifecycle" and "Software Reliability Engineered Testing is a testing method encompassing the whole development process". A Blockchain must guarantee data integrity and uniqueness to ensure Blockchain based systems are trustworthy which, in the case of BOS, is that of security-critical systems. In particular, there is a need for testing suites for BOS. These suites should include: Smart Contract Testing (SCT), namely specific tests for checking that smart contracts (i) satisfy the contractors' specifications, (ii) comply with the laws of the legal systems involved, and (iii) do not include unfair contract terms. Blockchain Transaction Testing (BTT), such as tests against double spending and to ensure status integrity [8].

A Blockchain is simply a cryptographically verifiable list of data. One of the reasons for the enthusiasm around the Blockchain is that databases do not have any cryptographic guarantees of integrity, guarantees that are necessary for any database operating in an adversarial environment [9].

Information technology has become a critical innovation in almost every industry. Those institutions or teams that can use technology correctly and effectively play a major role in disrupting the status quo in a leadership position. Those that don't keep up with technology generally do not survive. The authors of this paper have identified the Blockchain technology as a catalyst for emerging use cases in the financial and nonfinancial industries such as industrial manufacturing, supply chain, and healthcare [10].

The architecture as shown in Fig. 2 contains two major parts: ULE (sensors and network) and the cloud platform based on BC. The system is composed of connected devices and sensors, and the collector that collect data. These elements are connected to the internet to transfer data securely to the Ubiquitous-IoT platform for analysis, and processing. It allows the groups of students to access securely to the services via integrated cloud platform based on BC. In a BC network, students use a consensus protocol to approve the ledger content. The cryptographic hashes are

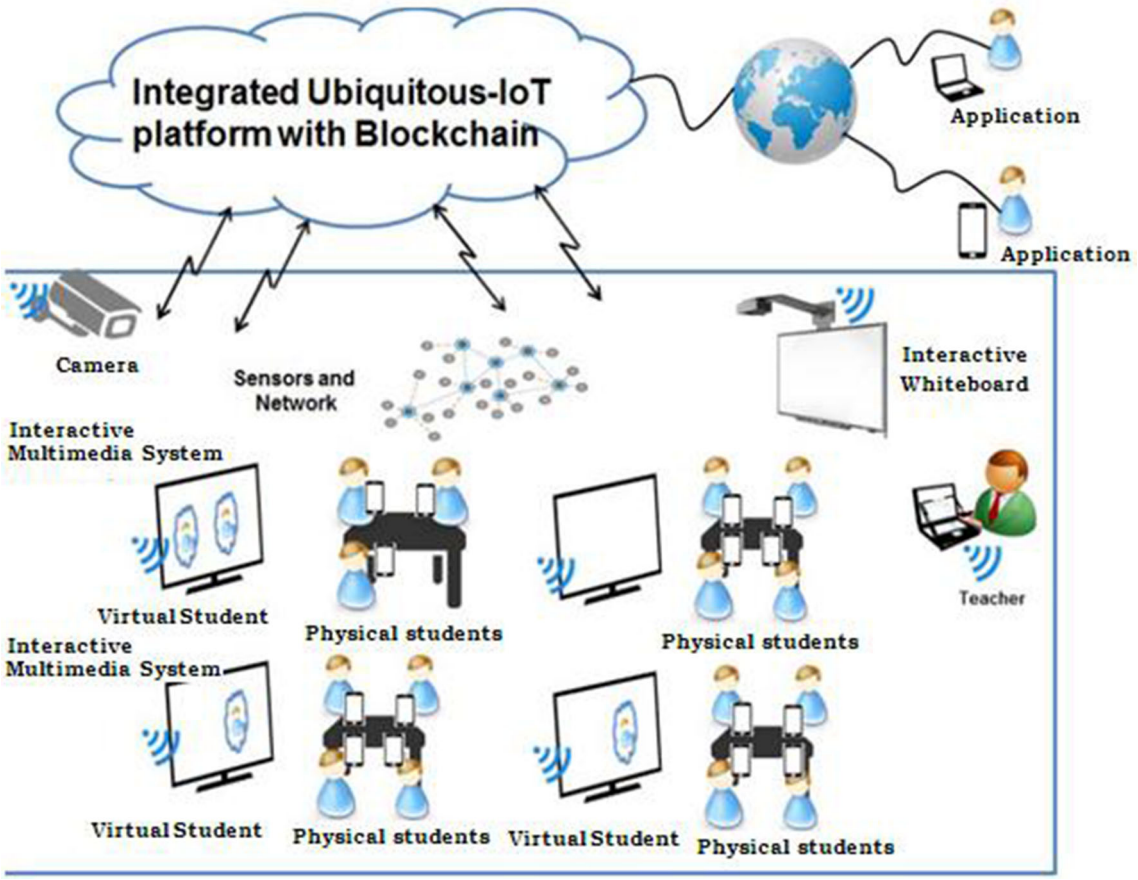


Fig. 2 ULE based on Blockchain technology

used to confirm the reliability of transactions. The consensus protocol verifies that the shared ledgers are duplicated, and eliminates the risk of unsecured transactions. Obviously, collected data from devices are integrated with the private BC ledgers and ensures shared transactions efficiently. The distributed architecture eliminates the requirement to centrally store data, and allows the decentralization way.

In the Fig. 2 The combination of ubiquitous computing, IoT and BC that can be effective. BC provides a resilient distributed P2P system considering the possibility to interact with peers in an effective manner. The connected devices in ULE ecosystem are the elements of contact with students and teacher. Indeed, we believe that the continuation of BC integration using ubiquitous computing and IoT will present a substantial transformation of current ecosystems. It enhances the next generation of IoT applications regarding the features of cryptographic, security, and decentralized model that can completely change the organization of our economic and scientific activities [11].

Transaction data should not be trusted in the hands of third-parties, where they are susceptible to steals and misuse. Instead, users should own and control their data without compromising security or limiting companies' and authorities' ability to provide encrypted transactions. Our platform enables this by combining a Blockchain with a holomorphic encryption solution. Users are not required to trust any third-party and are always aware of the data that is being collected about them and how it is used. In addition, the Blockchain recognizes the users as the owners of their encrypted data. Companies, in turn, can focus on utilizing data without being overly concerned about properly securing and compartmentalizing issues [12].

Author illustrated a novel approach of personal document management using Blockchain technology

PASS-Personal Archive Service System. Personal Archive Service System is exploiting the features from the Blockchain well. Whenever a subject would like to make a trace of achievement or new characteristics, the subject can archive it right away rather than waiting for an inquisitor later on. The opportunity for such application is pervasive. It can be used in online applications as well as other applications like employment and promotion. It eliminates a third party completely yet keeps its anonymity and accountability [13].

Fig. 3 Blockchain revenue by region, world markets: 2016–2025

Blockchain technology, as introduced with Bitcoin, offers an open, secure and distributed transaction ledger (ODL). As realizations of the technology focus on implementing currency systems and are based on cryptographic primitives, they are known as crypto-currencies. The basic idea behind the design is facilitating decentralized consensus, that is, making it possible for a network of unknown participants to jointly decide on a global view and ordering of transactions. Transactions are grouped in blocks and in each round, a participant is elected to propose a valid block [14].

The difficulties of adopting BC Technology to electronic government in China: The Cost of Establishing a New Blockchain-based Platform, The Long-term Preservation of Blockchain Platform Records, The Information Security of Blockchain Technology, Management Responsibility of the Blockchain Platform, The solution is: Standardization, Collaboration, Management System, and Security [15].

Blockchains have risen to prominence in recent years with the introduction of crypto currencies. As a technology, however, they support a wider range of use cases. A Blockchain system can be thought of as an append-only, public ledger that keeps track of transactions made by participants. In most cases, these transactions relate to some (virtual) asset, and often involve moving quantities of the asset from one account to another. Every participant in the Blockchain system holds a local copy of the ledger and runs a network client that relays transactions to the entire network. The client can also inject new transactions into the network [16].

A Blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The Blockchain contains a certain and verifiable record of every single transaction ever made. Beyond currency, the Blockchain can be used in smart contracts, record keeping, ID systems, cloud storage and many other areas [17].

The Blockchain technology is an enabler that makes many processes and transactions services more transparent, decentralized, secure and democratic without the need of a third-party organization in the middle. There is no doubt that the role that Blockchain plays to be implemented as a Digital Identity method, is crucial in the near future to authenticate citizens and prove their identities for the bunch of digital services that currently exist in this interconnected world. Blockchain in this area could help to improve the way that society views identity privacy and security. It will positively impact in different domains that a smart city environment interacts, such as; banking and payment, population growth forecasting, healthcare medical records, voting, digital services of governmental operations, financial services and many other scenarios [18].

In Fig. 3 it is clear that day by day in the market people moving towards Blockchain technology in 2016 Blockchain Revenue by Region below $5000 and in the expected year 2025 it will be $20,000.

The rise of big data age in the Internet has led to the explosive growth of data size. However, trust issue has become the biggest problem of big data, leading to the difficulty in data safe circulation and industry development. The Blockchain technology provides a new solution to this

problem by combining non-tampering, traceable features with smart contracts that automatically execute default instructions [19].

Bitcoin applies many technologies, they can be roughly divided into four blocks of the wallet address generation. These four blocks are Bitcoin transaction signature/broadcast, Blockchain technology and decentralized ledgers respectively. Bitcoin is one of the most typical applications applying Blockchain technology [20].

Many activities have been performed to improve the trust aspect in supply chains. The technologies used still have issues. The quality scandals recently reveal the importance of quality from a supply chain ideology. The traditional trust mechanism runs on three challenges because of which these trust issues occur. The challenges being self-interests of supply chain members, information asymmetry in production processes, costs and limitations of quality inspections. Blockchain is a promising technology to address these problems [21].

Potential benefits to South African public mHealth in implementing Blockchain: For Bitcoin implementers, Blockchain technology has provided technology that allows service providers to deliver: Secure peer to peer transactions with no need for a trusted third party. Digital signatures to safeguard content and thus the integrity of the data, Transactional chains that store history of ownership providing auditability, Blockchain that hold transactional order to prove authenticity of transactions [22].

Blockchain promises a secure distributed framework to facilitate sharing, exchanging, and the integration of information across all users and third parties, it is important for the planners and decision makers to analyze it in depth for its suitability in their industry and business applications. The blockchain should be deployed only if it is applicable and provides security with better opportunities for obtaining increased revenue and reductions in cost [23].

2.1 Blockchain applications

Finance Services:	Asset Management, Insurance Claims, Processing, Cross-Border Payments
Smart Property:	Money Lending, Smart Car, Smartphone
Smart Government:	Electronic Passport, Birth, … Wedding Certificates, Personal Identification, Smart Community
IoT	Smart Appliances, Supply- Chain Sensors
Smart Health Care:	Personal Health Record Keeping, Access Control, Health-Care Management, Insurance Processing

2.2 Blockchain characteristics

Decentralized, Distributed, Transparent and Verifiable, Cryptographically Secured, Immutable and Non-repudiable, Reduces Dependencies on Third Parties, "Trustless" Operation (Based on Consensus), Irrevocable and Auditable, Chronological and Time Stamped, Digital Ledger [24].

Specially, in the transaction authentication, the Blockchain technology is based on the elliptic curve digital signature algorithm (ECDSA), which cannot cope with the quantum attack in the actual network which will appear in the future. If anyone uses the Shor algorithm to derive a user's private key from a public key to sign a variety of unauthorized transactions, or an attacker forged a user signature, it means that the legitimate users will lose all their assets and privacy. In terms of resisting quantum attacks, the research of lattice cryptography is fruitful, which lays the foundation for the design of anti-quantum attack signature scheme which is suitable for blockchain [25].

2.3 Transactions not data

It is important to understand that in blockchain, you are out hundreds or even thousands of copies of the transaction records but not thousands of copies of the transaction data. It is like the difference between working in Microsoft Word and Google documents. When you collaborate on Microsoft Word, you typically create a document, make changes, and then send a full copy of the document to your colleague for editing. If you chose to make those changes without revisions turned on, it would be very difficult to tell exactly what changed from one version of the document to the other. And because you are sending out a full copy of the data, it would be pretty easy for somebody to intercept your email attachment and make a copy of it and steal your work. Additionally, you and your colleague must work one at a time. If you both work on the document at the same time, you may create conflicts that are difficult to resolve.(As per Jeanette DePatie)

Growing government regulatory requirements: The use of Blockchain technology to achieve multifaceted management of the food market is the government's demand, through the system of regulatory records of the food market transaction information. This can effectively solve the problem of food regulatory process. According to the understanding of the relevant government departments, there are some requirements of government regulatory authorities on the food supply chain:

(a) Precisely collect the information on all aspects of the food supply chain.

(b) Information gathering and storage of the food supply chain from planting (breeding) to the whole process of consumption.
(c) Can be transferred to the government regulatory platform through the block chain technology.

These requirements match with the technological characteristics of the blockchain which stores information on each transaction. Though each private key is produced and released by Information department of the Chinese Government, Ministry of Agriculture is given the access to the record of the data. This information would provide the basis for supervision, food recall and prior warning. Therefore, we can see that the application of Blockchain technology meets with the government's demand for food supply chain system [26, 27].

Electronic Health Records (EHRs) are entirely controlled by hospitals instead of patients, which complicates seeking medical advices from different hospitals. Patients face a critical need to focus on the details of their own healthcare and restore management of their own medical data. The rapid development of Blockchain technology promotes population healthcare, including medical records as well as patient-related data. This technology provides patients with comprehensive, immutable records and access to EHRs free from service providers and treatment websites [28, 29].

As an emerging technology, blockchains definitely will keep evolving, because of its disruptive capability across various industries and domains. The technology is expected to validate itself with more proof-of-concept implementations. In the field of intrusion detection, Blockchain technology can make positive impacts, but its major applications are more focused on the following aspects, in terms of a trade-off between benefit and cost.

- *Data sharing* by design nature, blockchains are suitable for handling the recording of events, medical records, and transaction processing. As data management is a big issue for a large distributed detection system or network, blockchains have a great potential to improve the performance through enforcing trust and data privacy among collaborating parties.
- *Alert exchange* Alexopoulos et al. already introduced how to use blockchains to secure the alerts generated by various nodes and ensure only truthful alerts would be exchanged. Due to the lack of real system applications, it is an interesting and important direction for future research studies.
- *Trust computation* as mentioned above, some collaborative detection approaches (e.g., challenge-based CIDN) utilize alerts to evaluate the trustiness of others, blockchains can thus provide a solution to enhance the process of trust computation. For instance, designing blockchain-based approaches to verify whether the received alert-information is unaltered or not.

As Blockchains were originally designed for crypto-currencies, we have to avoid the situation that "Blockchain is a solution looking for a problem". Indeed, we have to still focus on our traditional solutions to some issues and challenges, but keep an eye on such emerging technologies. It means that a balance should always be made in a case-by-case scenario [30].

One of the challenges in P2P design is a fair scheduling and a general protection of the whole cluster against abusive or malfunctioning nodes. Algorithms used in a single-master or multi-master clusters do not work anymore. We have designed a multi-level system based on one of the main principles of crypto-currencies to achieve. Blockchain is a key component of contemporary crypto-currencies such as Bitcoin, Lite-coin and Ethereum. Blockchain solves the main problem of digital assets—the double-spend problem. Each digital asset such as file, email or an array can be copied and a spectator can not determinate the origin and the copy without a 3rd party. In P2P networks there is no such authority. The ownership of an asset is recorded in a public ledger. This ledger is confirmed by the whole community of the system, so the trust is not needed between two parties, but between one party and the whole system. The basic principle is based on asymmetric cryptographic functions. Each transaction is signed by its owner. In order to be a valid transaction of the public ledger, the transaction must be hashed and the hash must be included in the next transaction [30].

Bitcoin is digital assets infrastructure powering the first worldwide decentralized cryptocurrency of the same name. All history of Bitcoins owning and transferring (addresses and Transactions) is available as a public ledger called Blockchain. But real-world owners of addresses are not known in general. That's why Bitcoin is called pseudo-anonymous. However, some addresses can be grouped by their ownership using behavior patterns and publicly available information from off-chain sources. Blockchain-based common behavior pattern analysis (common spending and one-time change heuristics) is widely used for Bitcoin clustering as votes for addresses association, while offchain information (tags) is mostly used to verify results. Here Represent's the use off-chain information as votes for address separation and to consider it together with Blockchain information during the clustering model construction step. Both Blockchain and off-chain information are not reliable, and our approach aims to filter out errors in input data. A new Bitcoin address clustering algorithm is proposed. Its difference from the existing ones is two-fold. Firstly, it uses for clustering not only Blockchain information but also off-chain information from the Internet.

Secondly, we treat certain off-chain data types as votes against address union in clustering process. Such approach allows avoiding significant part of erroneous cluster merges suggested by Blockchain based heuristics. Numerical experiments show that the proposed approach provides reasonable clustering results outperforming approaches based solely on Blockchain data in terms of cluster homogeneity [31].

3 Swot analysis of blockchain

SWOT analysis (or SWOTM matrix) is a short form for strengths, weaknesses, opportunities, and threats and is a structured planning method that evaluates those four elements of an association, project or commerce endeavor etc.

(a) *Strengths*

- 100% transparency
- Able to skip the intermediary
- Auditable trail
- Business process efficiency and productivity
- Decentralized approach
- High quality and fool proof data
- Higher efficiency
- Lower cost
- Lower risk
- More secure
- No reliance on third party
- Robustness (no SPOF)
- Speed
- Transparency
- Trust in trustless networks
- Unharmed privacy

(b) *Weaknesses*

- Access challenge
- Change Management
- Integration With Legacy Systems
- Lack Of Standards
- Low capacity and processing speed
- Ownership challenge
- Recent technology (not 100% developed)
- Scalability
- Security against cyber criminals
- Storage
- Technology Maturity

(c) *Opportunities*

- Automations
- Business Process Optimisation
- Elimination of trust necessity
- Faster (international) payment transfers
- Improved customer experience
- Increased quality of products and services
- Innovation In Almost Every Industry Especially Banking
- Instantaneous settlements
- KYC database
- New Intermediaries
- No reliance on rating agencies
- Opportunities In IoT
- Programmable control mechanisms
- Smart contracts in insurance
- Speedup bank processes

(d) *Threats*

- A lot of research needs to be done
- Disappearance of existing bank jobs
- Govt. willingness to adopt
- High investments for implementations
- Huge regulatory impact
- Hype
- Legal/regulatory and compliance
- Privacy and security
- Time—consuming negotiations
- Uncertainty about the impact

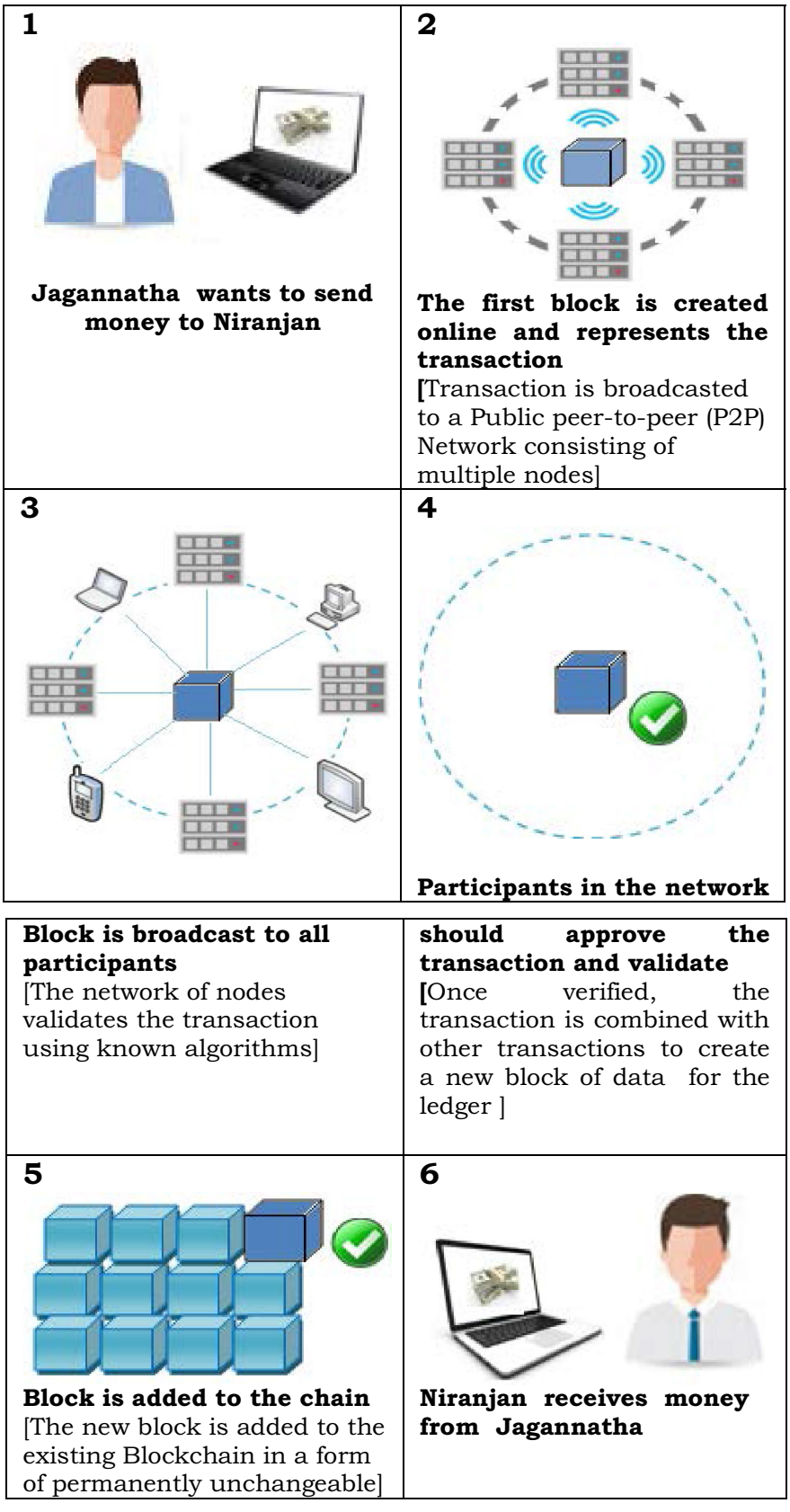
4 How Blockchain works?

Someone requests a transaction

(1) The requested transaction is broadcasted to P2P network consisted of computers known as nodes.
(2) Validation: the network of nodes validates the transaction and user's status using known algorithms.
(3) A verified transaction can include crypto currency, contracts, records or other information.
(4) Once verified, the transaction is linked to other transactions to create a new block of data for the ledger.
(5) The new block is then appended to the existing Blockchain, in a way that is permanent and unalterable.
(6) The transaction is finally complete.

Transactions are not valid until added to chain. Tampering is immediately evident. The Blockchain is regarded as safe as everyone in the network has a copy. The sources of any discrepancies are usually evident immediately (Fig. 4).

Fig. 4 Working nature of Blockchain



5 Types of Blockchain

Blockchain technologies can be divided into three types.

(1) Public Blockchain
(2) Consortium Blockchains
(3) Private Blockchain

(1) *Public Blockchain* everyone can check the transaction and verify it, and can also participate the process of getting consensus. Like Bitcoin and Ethereum are both Public Blockchain. Figure 5 shows public Blockchain.

(2) *Consortium Blockchains* it means the node that had authority can be choose in advance, usually has partnerships like business to business, the data in Blockchain can be open or private, can be seen as Partly Decentralized. Like Hyperledger and R3CEV are both consortium Blockchains. Figure 6 shows consortium Blockchains.

(3) *Private Blockchain* node will be restricted, not every node can participate this Blockchain, has strict authority management on data access. Figure 7 shows private Blockchain. No matter what types of Blockchain are, it both has advantage. Sometimes we need public Blockchain because its convenience, but sometimes we maybe need private control like consortium Blockchains or private Blockchain, depending on what service we offer or what place we use it [1].

6 Pros and cons of Blockchain

(1) Pros of Blockchain technology (advantages of Blockchain technology):

(a) *Disintermediation* the core value of a Blockchain is that it enables a database to be directly shared without a central administrator. Rather than having some centralized application logic, Blockchain transactions have their own proof of validity and authorization to enforce the constraints. Hence, with the Blockchain acting as a consensus mechanism to ensure the nodes stay in sync, transactions can be verified and processed independently. But why is disintermediation good for us? Because a database is still a tangible thing even though is just bits and bytes. If the contents of a database are stored in the memory and disk of a particular computer system run by a third party even if it is a trusted organization like banks and governments, anyone who somehow got access to that system can easily corrupt the data within. Thus the third-party organizations especially those who control important databases need to hire many people and design many processes to prevent that database being tampered with. Unavoidably, all this takes a great amount of time and money.

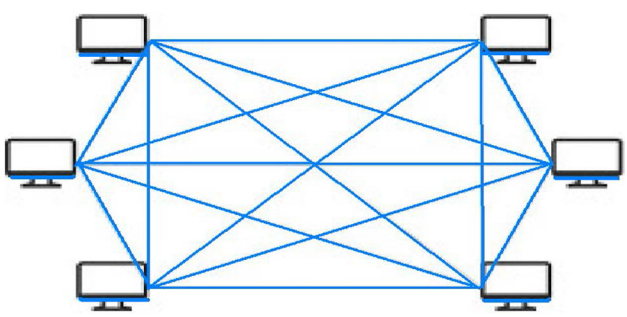


Fig. 5 Public Blockchain

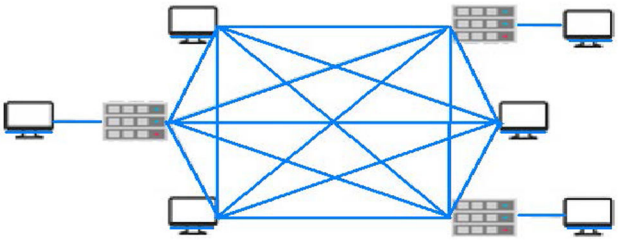


Fig. 6 Consortium Blockchain

(b) *Empowered users* users are in control of all their information and transactions.

(c) *High quality data* Blockchain data is complete, consistent, timely, accurate, and widely available

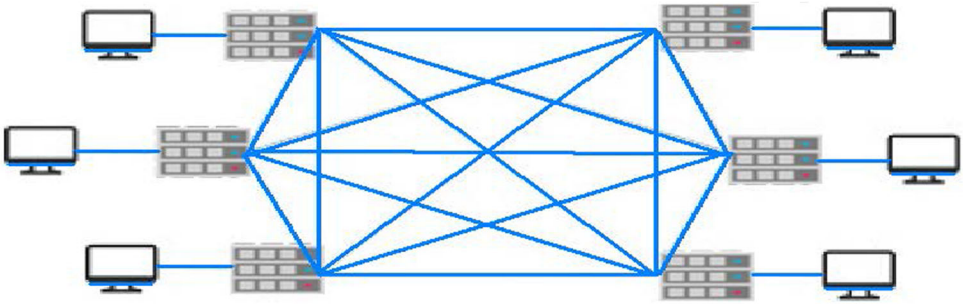
(d) *Durability reliability and longevity* due to the decentralized networks, Blockchain does not have a centralized point of failure and is better able to withstand malicious attacks.

(e) *Process integrity* users can trust that transactions will be executed exactly as per the protocol commands removing the need for a trusted third party

(f) *Transparency and immutability* changes to public Blockchains are publically viewable by all parties creating transparency, and all transactions are immutable, meaning they cannot be altered or deleted.

(g) *Ecosystem simplification* with all transactions being added to a single public ledger, it reduces the clutter and complications of multiple ledgers.

Fig. 7 Private Blockchain



(h) *Faster transactions* inter bank transactions can potentially take days for clearing and final settlement, especially outside of working hours. Blockchain transactions can reduce transaction times to minutes and are processed 24/7

(i) *Lower transaction costs* by eliminating third party, intermediaries and overhead costs for exchanging assets, Blockchains have the potential to greatly reduce transaction fees.

(j) *Blockchains can be used to*

- *Reduce total cost of ownership* Blockchain stacks offer a robust and verifiable alternative to traditional proprietary stacks at a fraction of the cost.
- *Manage system-of-record sharing* Blockchain technology makes it possible to give various parties (e.g., clients, custodians and regulators) access to their own live copies of a shared system of record.
- *Clear and settle transactions faster* Blockchain technology can facilitate the transition from overnight batch processing to intra-day clearing and settlement.
- *Create self-describing electronic transactions* smart contracts can use Blockchain's programming language to create context-aware transactions for complex arbitration. For example, a credit default swap could pay out automatically according to pre-agreed logic that watches market data feeds.

(k) *Business benefits* many businesses can actually utilize the Blockchain technology into the new trading platform and get benefited. There are numerous benefits of adopting this technology into business. The major six benefits are given below:

- *Efficiency* as in Blockchain technology, transactions are done directly in between the two parties without any involvement of the third party, so transactions take place quickly. In addition, the technology has the ability to manage smart contracts and commercial actions automatically. Therefore, this directly streamlines every process and remove the cost and time from the transaction. For more information about the same, you can read articles and blogs on reliable sites that how this technology is getting utilized in different industries.
- *Auditability* on the Blockchain network, each transaction detail is recorded subsequently and it provides an audibility for the asset in between two parties. It is especially beneficial for the businesses in which data source is needed in order to authenticate the assets. At present, the company Every ledger realized the benefit of Blockchain technology and used it to track the diamonds.
- *Traceability* in the Blockchain, tracking goods in a supply chain is pretty easy and advantageous too. The information related to component can communicated to and from the new owner required for the possible action.
- *Transparency* transparency is one of the major benefits of Blockchain to small, medium as well as large businesses. As lack of financial and commercial transparency might result in bad business relations and commerce delays. So, in order to provide transaction details against commercial construct, trust and transparency need to be maintained in the process for a stable relationship instead of negotiation.
- *Security* on the Blockchain technology, each transaction is recorded and verified in the network through complex cryptographic problems. The information

authenticity is assured through complex mathematical algorithms. The benefits of IoT—Internet of Things is assured information of the keys. This has already been used in the Defense industry for IP protection and verification of instructions.

- *Feedback* another benefit to businesses of Blockchain technology is feedback. As the technology has full traceability throughout the asset lifecycle, the manufacturers and designers of asset can easily track the assets and accommodate the asset management in products in order to make it more effective. Feedback allows information regarding installation, maintenance, shipping returns, and decommissioning.
- *The bottom line* while Blockchain has been designed to serve the digital currency; however, it can also help the businesses in serving their needs. Therefore, business owners should use this technology in their business and make a boom in the industry. In Fig. 8 it is clearly representing the main benefits of BC: Reduce operational costs 73%, Shorten settlement time is 69%, Reduce risk is 57%, Create revenue opportunities is 51%, Reduce cost of capital 46%, others is 10%, none is 2%.

(2) Cons of Blockchain technology (disadvantages of Blockchain technology):

(a) Performance because of the nature of Blockchains, it will always be slower than centralized databases. When a transaction is being processed, a Blockchain has to do all the same things just like a regular database does, but it carries three additional burdens as well:

(i) *Signature verification* every Blockchain transaction must be digitally signed using a public–private cryptography scheme. This is necessary because transactions propagate between nodes in a peer-to-peer fashion, so their source cannot otherwise be proven. The generation and verification of these signatures is computationally complex, and constitutes the primary bottleneck in products like ours. By contrast, in centralized databases, once a connection has been established, there is no need to individually verify every request that comes over it.

(ii) *Consensus mechanisms* in a distributed database such as a Blockchain, effort must be expended in ensuring that nodes in the network reach consensus. Depending on the consensus mechanism used, this might involve significant back-and-forth communication and/or dealing with forks and their consequent rollbacks. While it's true that centralized databases must also contend with conflicting and aborted transactions, these are far less likely where transactions

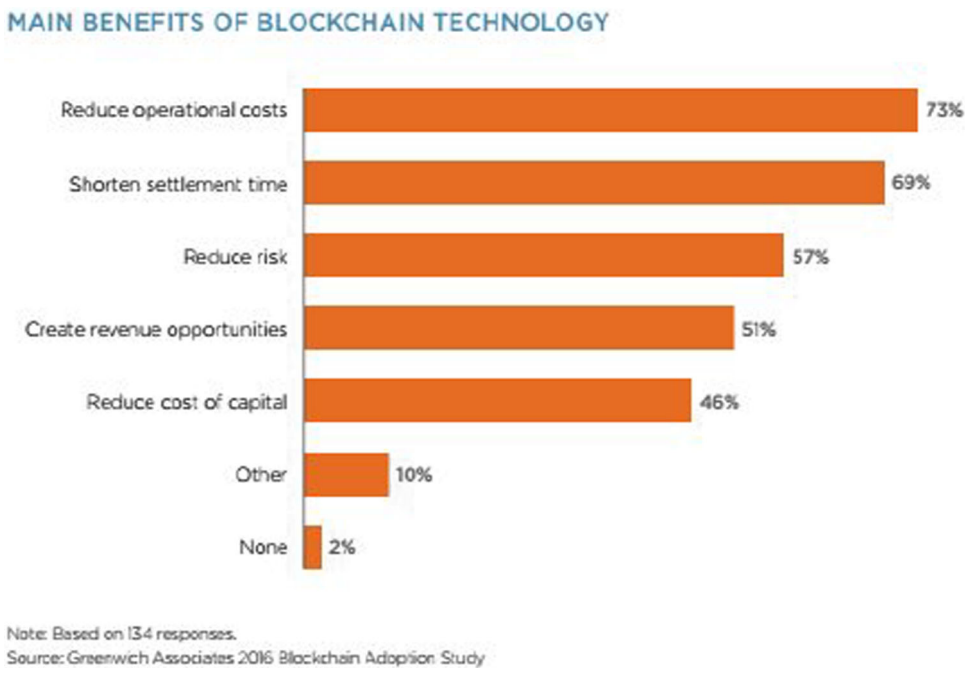


Fig. 8 Main benefits of BC

are queued and processed in a single location.

(iii) *Redundancy* this isn't about the performance of an individual node, but the total amount of computation that a Blockchain requires. Whereas centralized databases process transactions once (or twice), in a Blockchain they must be processed independently by every node in the network. So lots more work is being done for the same end result.

(b) *Nascent technology* resolving challenges such as transaction speed, the verification process, and data limits will be crucial in making Blockchain widely applicable

(c) *Uncertain regulatory status* because modern currencies have been created and regulated by national governments, Blockchain and Bitcoin face a hurdle in widespread adoption by pre—existing financial institutions if its government regulation status remains unsettled.

(d) *Large energy consumption* the Bitcoin Blockchain network's miners are attempting 450 thousand trillion solutions per second in efforts to validate transactions, using substantial amounts of computer power.

(e) *Control, security and privacy* while solutions exist, including private or permissioned Blockchains and strong encryption, there are still cyber security concerns that need to be addressed before the general public will entrust their personal data to a Blockchain solution.

(f) *Integration concerns* Blockchain applications offer solutions that require significant changes to, or complete replacements of, existing systems. In order to make the switch, companies must strategize the transaction.

(g) *Cultural adoption* Blockchain represents a complete shift to a decentralized network which requires the buy—in of its users and operators.

(h) *Cost* Blockchain offers tremendous savings in transaction costs and time but the high initial capital cost could be limit.

(3) BC attacks could be accomplished-through:

- User identify theft
- Fraudulent sender and receiver
- Asset/node theft or impersonation
- Targeting of Bitcoin miners
- Availability of distributed nodes
- Injection of malicious code into a distributed ledger
- Reputational risk
- Target reconnaissance
- Bypassing the onboarding and off boarding of nodes
- Fictitious Blockchain applications will appear to steal transaction details/personal information/behavior from nodes/individuals.

7 Conclusion

Blockchain is a data structure to create and share distributed ledger of transactions among a network of computers. It allows users to make and verify transactions immediately without a central authority. Blockchain is a transaction database which contains information about all the transactions ever executed in the past and works on Bitcoin protocol. Blockchain technologies is contains Cryptography, mathematics, Algorithm and economic model, combining peer-to-peer networks and using distributed consensus algorithm to solve traditional distributed database synchronize problem, it's an integrated multi-field infrastructure construction. The Blockchain technologies composed of six key elements. - Decentralized, Transparent, Open Source, Autonomy, Immutable, Anonymity. Blockchain technologies can be divided into three types. Public Blockchain, Consortium Blockchains, Private Blockchain. Advantages of Blockchain Technology-Disintermediation, Empowered users, High quality data, Durability, reliability and longevity, Process integrity, Transparency and immutability, Ecosystem simplification, Efficiency, Auditability, Traceability, Transparency, Faster transactions, Lower transaction costs.

Acknowledgments I thank Dr. T. V. Suresh Kumar, Registrar (Academic), Prof. and Head, Dept. of Computer Applications, RIT, Bangalore-54. He has provided his continuous support for the completion of this paper and my sincere gratitude to RIT management.

References

1. Lin, I.C., Liao, T.C.: A survey of Blockchain security issues and challenges. Int. J. Netw. Secur. **19**(5), 653–659 (2017). https://doi.org/10.6633/ijns.201709.19(5).01
2. Zheng, Z, Xie, S., Dai, HN., Chen, X., Wang, H.: An overview of Blockchain technology: architecture, consensus, and future Trends. In: 978-1-5386-1996-4/17 6th International Congress on Big Data PP557-564 IEEE (2017).
3. Dennis, R., Owenson, G., Aziz, B.: A temporal Blockchain: a formal analysis. In: 2016 International Conference on

Collaboration Technologies and Systems-978-1-5090-2300-4/16 PP 430-437 IEEE (2016)
4. Singh, S, Singh, N.: Blockchain: future of financial and cyber security. In: 978-1-5090-5256-1/16/PP463-467 IEEE (2016)
5. Fu, D., Fang, L.: Blockchain-based trusted computing in social network. In: 2nd International Conference on Computer and Communications-978-1-4673-9026-2/16/IEEE (2016)
6. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A taxonomy of Blockchain-based systems for architecture design. In: International Conference on Software Architecture 978-1-5090-5729-0/17 IEEE (2017)
7. Wan, Z., Lo, D., Xia, X., Cai, L.: Bug characteristics in Blockchain systems: alarge-scale empirical study. In: 14th International Conference on Mining Software Repositories (MSR) PP 423-424 IEEE/ACM (2017)
8. Porru, S., Pinna, A., Marchesi, M., Tonelli, R.: Blockchain-oriented software engineering: challenges and new directions. In: 39th IEEE International Conference on Software Engineering Companion PP169-179 IEEE/ACM (2017)
9. Halpin, H., Piekarska, M.: Introduction to security and privacy on the Blockchain. In: European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 1–3 IEEE (2017)
10. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., Amaba, B.: Blockchain technology innovations. In: 978-1-5090-1114-8/17/ Technology & Engineering Management Conference (TEMSCON) IEEE (2017)
11. Bdiwi, R., de Runz, C., Faiz, S., Cherif, A.A.: Towards a new ubiquitous learning environment based on Blockchain technology. In: 17th International Conference on Advanced Learning Technologies PP101-102 IEEE (2017)
12. Nakasumi, M.: Information sharing for supply chain management based on block chain technology. In: 19th Conference on Business Informatics 2378-1971/17 PP 140-149 IEEE (2017)
13. Chen, Z., Zhu, Y.: personal archive service system using Blockchain technology: case study, promising and challenging. In: International Conference on AI & Mobile Services (AIMS) 978-1-5386-1999-5/17, pp. 93–99 IEEE (2017)
14. Alexopoulos, N., Daubert, J., M̈uhlḧauser, M., Habib, S.M.: Beyond the hype: on using Blockchains in trust management for authentication. In: 2324-9013/17 Trustcom/BigDataSE/ICESS, pp. 546–553 IEEE (2017)
15. Hou, H.: The application of Blockchain technology in E-government in China. In: 978-1-5090-2991-4/17/IEEE (2017)
16. Weber, I., Gramoli, V., Ponomarev, A.: On availability for Blockchain-based systems. In: 36th Symposium on Reliable Distributed Systems 978-1-5386-1679-6/17, pp. 64–73 IEEE (2017)
17. Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V., Yalansky, L.: Ensuring data integrity using Blockchain technology. In: Proceeding of the 20th Conference of fruct Association ISSN 2305-7254 IEEE (2017)
18. Rivera, R., Robledo, J.S., Larios, V.M., Avalos, J.M.: How digital identity on Blockchain can contribute in a smart city environment. In: 978-1-5386-2524-8/17/IEEE (2017)
19. Li, Y, Huang, J., Qin, S., Wang, R.: Big data model of security sharing based on Blockchain. In: 3rd International Conference on Big Data Computing and Communications 978-1-5386-3349-6/17, pp. 117–121 IEEE (2017)
20. Chen, P.W., Jiang, B.S., Wang, C. H.: Blockchain-based payment collection supervision system using pervasive bitcoin digital wallet. In: 5th International Workshop on Pervasive and Context-Aware Middleware-978-1-5386-3839-2/17 IEEE (2017)
21. Chen, S., Shi, R., Ren, Z., Yan, J., Shi, Y., Zhang, J.: A Blockchain-based supply chain quality management framework. In: The 14th IEEE International Conference on e-Business Engineering 978-1-5386-1412-9/17, pp. 172–176 IEEE (2017)
22. Weiss, M., Botha, A., Herselman, M., Loots, G.: Blockchain as an enabler for PublicmHealth solutions in South Africa. In: IST-Africa 2017 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds)IIMC International Information Management Corporation, ISBN: 978-1-905824-57-1 (2017)
23. Hamida, E.B., Brousmiche, K.L., Levard, H., Thea, E.: Blockchain for enterprise: overview, opportunities and challenges. In: The Thirteenth International Conference on Wireless and Mobile Communications-IEEE ICWMC (2017)
24. Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E., Yang, C.: The Blockchain as a decentralized security framework [Future Directions]. IEEE Consum. Electron. Mag. **7**(2), 18–21 (2018)
25. Yin, W., Wen, Q., Li, Q., Zhang, H., Jin, Z.: An anti-quantum transaction authentication approach in Blockchain. IEEE Access. **6**, 5393–5401 (2018)
26. Tse, D., Zhang, B., Yang, Y., Cheng, C., Mu, H.: Blockchain application in food supply information security. In: IEEE International Conference on Industrial Engineering and Engineering Management (IEEM),ISSN: 2157-362X, pp. 1357–1361 (2018)
27. Chinnasamy, A., Sivakumar, B., Selvakumari, P., Suresh, A.: Minimum connected dominating set based RSU allocation for smartCloud vehicles in VANET. Clust. Comput. (2018). https://doi.org/10.1007/s10586-018-1760-8
28. Guo, R., Shi, H., Zhao, Q., Zheng, D.: Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems. IEEE Access. **776**(99), 1–12 (2018)
29. Suresh, A., Varatharajan, R.: Competent resource provisioning and distribution techniques for cloud computing environment. Clust. Comput. (2017). https://doi.org/10.1007/s10586-017-1293-6
30. Gattermayer, J., Tvrdik, P.: Blockchain-based multi-level scoring system for P2P clusters. In: 46th International Conference onParallel Processing Workshops (ICPPW), ISSN: 1530-2016, pp. 301–308 IEEE (2017)
31. Ermilov, D., Panov, M., Yanovich, Y.: Automatic bitcoin address clustering. In: 16th IEEE International Conference on Machine Learning and Applications. pp. 461–466 IEEE (2018). https://doi.org/10.1109/icmla.2017.0-118

M. Niranjanamurthy received Ph.D. Computer Science degree from JJT University, Rajasthan, INDIA in the year 2016, M.Phil-Computer Science degree from VM University, Tamil Nadu in the year 2009. MCA degree from VT University, Karnataka in the year 2007 and BCA Degree from Kuvempu University in the year 2004. He is a Assistant Professor in the department of Computer Applications, M S Ramaiah Institute of Technology, Bangalore. His areas of interests are software testing, e-commerce and m-commerce, software engineering, web technologies, Cloud Computing, Big data analytics. He has been participating in National and International workshops/Conferences on different aspects related to Computer Applications. Guiding Research Scholars, Recognized Ph.D. research examiner National and International. Published many research Articles related to Computer Science.

B. N. Nithya received MCA degree from SPMVV University, Tirupati, Andhra Pradesh in the year 2005 and BCA SV University, Tirupati, Andhra Pradesh in the year 2002. She is a Assistant Professor in the department of Computer Applications, M S Ramaiah Institute of Technology, Bangalore. She is currently doing a Ph.D. degree in VT University, Karnataka INDIA. Her areas of interests are Cloud Computing, Social Network Analysis, Data Analytics using Python. She also has the experience of being a Life Skills Trainer.

S. Jagannatha Ph.D. Computer Applications degree from VT University, Karnataka INDIA in the year 2014, Mhil-Computer Science degree from M S University, Tirunelveli, Tamil Nadu in the year 2013. MCA degree from Bangalore University in the year 1993 and BSc Degree from Bangalore University in the year 1990. He is a Associate Professor in the department of Computer Application, M S Ramaiah Institute of Technology, Bangalore. He has been participating in national and international workshops/ Conferences on different aspects related to Computer Applications. Guiding Research Scholars, His areas of interests are distributed database, object technology, and software engineering.